|  |  |
| --- | --- |
|  | **CyberCrime@IPA**  **Projekt i Përbashkët BE/KiE për Bashkëpunimin Rajonal kundër Krimit Kibernetik**    **Trajnimi Gjyqësor**  **Kurs bazë për krimin kibernetik dhe provat elektronike për gjyqtarët dhe prokurorët**  Manuali i Trajnimit dhe Guida për Trajnerët – Versioni 1.0  Departamenti për Mbrojtjen e të Dhënave dhe Krimin Kibernetik  Drejtoria e Përgjithshme për të Drejtat e Njeriut dhe Shtetin e së Drejtës  Strasburg, Francë  5 Prill 2013 |
| **www.coe.int/cybercrime**  eu_coe_JP1 |

|  |  |
| --- | --- |
| **Kontakt:**  Departamenti për Mbrojtjen e të Dhënave dhe Krimin Kibernetik  Drejtoria e Përgjithshme për të Drejtat e Njeriut dhe Shtetin e së Drejtës  Këshilli i Evropës,  Strasburg, Francë  Tel: +33-3-9021-4506 Fax: +33-3-9021-5650 Email: [alexander.seger@coe.int](mailto:alexander.seger@coe.int) | **Përjashtimi nga përgjegjësia:**  Ky raport teknik nuk reflekton domosdoshmërisht pozicionin zyrtar të Këshillit të Evropës, të donatorit financues të këtij projekti apo të Palëve të traktateve të përmendura në të. |

**Përmbajtja**

[1 Hyrje 4](#_Toc352944220)

[2 Vështrim i Përgjithshëm 5](#_Toc352944221)

[2.1 Qëllimi i Kursit 5](#_Toc352944222)

[2.2 Pse është i domosdoshëm ky trajnim 5](#_Toc352944223)

[2.3 Programi mësimor 6](#_Toc352944224)

[3 Si përdoret guida për trainerët 6](#_Toc352944225)

[4 Vështrim i përgjithshëm i kursit 7](#_Toc352944226)

[4.1 Sa i gjatë është kursi dhe për kë është 7](#_Toc352944227)

[4.2 Kush do ta japë kursin](#_Toc352944228) 8

[4.3 Si do të jepet kursi 8](#_Toc352944229)

[4.4 Objektivat 8](#_Toc352944230)

[4.5 Grupi i trainerëve dhe pjesëmarrësit e synuar 8](#_Toc352944231)

[4.5.1 Pjesëmarrësit 8](#_Toc352944232)

[4.5.2 Kriteret e përvojës 8](#_Toc352944233)

[4.5.3 Trainerët](#_Toc352944234) 8

[4.5.4 Kriteret e përvojës](#_Toc352944235) 9

[4.6 Burimet 9](#_Toc352944236)

[4.6.1 Kriteret për Burimet e Kursit 9](#_Toc352944237)

[4.7 Vlerësimi 9](#_Toc352944238)

[4.8 Objektivat e mësimit dhe kursit 9](#_Toc352944239)

[5 Kontaktet kryesore 1](#_Toc352944240)4

[6 Planet mësimore 1](#_Toc352944241)5

[6.1 Mësimi 1.1.1 Hyrja në kurs 1](#_Toc352944242)5

[6.2 Mësimi 1.1.2 Hyrje në krimin kibernetik 1](#_Toc352944243)8

[6.3 Mësimi 1.1.3, 1.2.2 & 1.2.5 - Teknologjia 31](#_Toc352944244)

[6.4 Mësimi 1.3.1 – Rishikimi Ditor 60](#_Toc352944245)

[6.5 Mësimi 1.2.3 Krimi kibernetik si vepër penale – legjislacioni i brendshëm 61](#_Toc352944246)

[6.6 Mësimi 1.2.4 Ligji procedural i brendshëm 8](#_Toc352944247)7

[6.7 Mësimi 1.3.1 Rishikimi Ditor 93](#_Toc352944248)

[6.8 Mësimet 1.3.2 & 1.3.3 Provat Elektronike 94](#_Toc352944249)

[6.9 Mësimi 1.3.4 Bashkëpunimi Ndërkombëtar 121](#_Toc352944250)

[6.10 Mësimi 1.3.5 Mbyllja e kursit 132](#_Toc352944251)

[7 Vlerësimi 134](#_Toc352944252)

[8 Vlerësimi 134](#_Toc352944253)

# Hyrje

Me mbështetjen e shoqërive në të gjithë botën në teknologjitë e informacionit dhe komunikimit, gjyqtarët dhe prokurorët duhet të jenë të përgatitur për të gjykuar krimin kibernetik dhe shqyrtuar provat elektronike. Megjithëse në shumë vende, autoritetet e zbatimit të ligjit i kanë forcuar kapacitetet e tyre për hetimin e krimit kibernetik dhe sigurimin e provave elektronike, kjo gjë nuk ndodh me gjyqtarët dhe prokurorët. Përvoja të sugjeron se në shumicën e rasteve, gjyqtarët dhe prokurorët hasin vështirësi në përballjen me realitetet e reja të botës kibernetike. Për këtë arsye, kërkohen përpjekje të posaçme për të aftësuar gjyqtarët dhe prokurorët që të mund të ndjekin ligjërisht dhe gjykojnë krimin kibernetik dhe të shfrytëzojnë provat elektronike nëpërmjet trajnimit, lidhjes në rrjet dhe specializimit.

Gjatë vitit 2009 u zhvillua një koncept për mbështetjen e këtyre përpjekjeve nga Këshilli i Evropës në kuadër të Projektit për Krimin Kibernetik në bashkëpunim me Rrjetin e Lisbonës të institucioneve të trajnimit gjyqësor në bashkëpunim me një grup pune me shumë anëtarë.

Qëllimi i këtij koncepti ishte të ndihmoheshin institucionet e trajnimit gjyqësor në zhvillimin e programeve të trajnimit për krimin kibernetik dhe provat elektronike për gjyqtarët dhe prokurorët dhe integrimin e një trajnimi të tillë në programet e tyre të rregullta të formimit fillestar dhe atij të vazhduar.

Objektivat e konceptit të trajnimit për gjyqtarët dhe prokurorët janë:

* Aftësimi i institucioneve trajnuese për ofrimin e trajnimit fillestar dhe të vazhduar për krimin kibernetik bazuar në standardet ndërkombëtare
* Pajisje e një numri sa më të madh gjyqtarësh dhe prokurorësh të ardhshëm dhe atyre në detyrë me njohuri bazë për krimin kibernetik dhe provat elektronike
* Ofrimi i trajnimit të avancuar për një numër të konsiderueshëm gjyqtarësh dhe prokurorësh
* Mbështetja për specializimin e vazhdueshëm dhe trajnimin teknik të gjyqtarëve dhe prokurorëve
* Kontributi për rritjen e njohurive nëpërmjet lidhjes në rrjet të gjyqtarëve dhe prokurorëve
* Lehtësimi i aksesit në rrjete dhe iniciativa të ndryshme të trajnimit.

Nëpërmjet Projektit Rajonal të Përbashkët ndërmjet Bashkimit Evropian dhe Këshillit të Evropës për Krimin Kibernetik @IPA (Bashkëpunimi Rajonal në Drejtësinë Penale: Forcimi i kapaciteteve në luftën kundër krimit kibernetik)[[1]](#footnote-2), jepet mbështetje që institucionet e trajnimit në zonat e projektit (Shqipëria, Bosnja dhe Hercegovina, Kroacia, Mali i Zi, Serbia, “Ish-Republika Jugosllave e Maqedonisë”, Turqia dhe Kosova[[2]](#footnote-3)\*) të mund të zbatojnë këtë koncept trajnimi.

Në këtë kontekst, janë hartuar materialet e trajnimit për tu përdorur nga institucionet trajnuese dhe është realizuar një “Program për Trajnimin e Trajnerëve”. Ky version final i paketës së trajnimit merr në konsideratë informacionin e marrë nga gjyqtarët dhe prokurorët, të cilët morën pjesë në “Programin e Trajnimit të Trajnerëve” dhe e zhvilluan më pas kursin në institucionet e tyre të trajnimit. Krahas kësaj, versioni final është diskutuar me anëtarët e grupeve të punës në trajnimin gjyqësor dhe trajnerët në një aktivitet të organizuar për këtë qëllim.

# Vështrim i Përgjithshëm

## Qëllimi i Kursit

Ky kurs është hartuar për t’i pajisur gjyqtarët dhe prokurorët me një nivel bazë të njohurive në lidhje me krimin kibernetik dhe provat elektronike. Kursi do të ofrojë informacion praktik po ashtu edhe ligjor në lidhje me temën dhe do të përqendrohet sesi këto çështje ndikojnë në punën e përditshme të gjyqtarëve dhe të prokurorëve.

Në fund të kursit gjyqtarët dhe prokurorët do të kenë njohuri bazë për:

* Krimin kibernetik dhe provat elektronike
* Si të trajtohen këto çështje
* Cilat ligje materiale apo procedurale si dhe cilat teknologji mund të zbatohen, dhe
* Si mund të ndërmerren masa urgjente dhe efiçente si dhe si të realizohet një bashkëpunim i gjerë ndërkombëtar.

Kursi do të mbulojë temat e mëposhtme:

* Hyrje në fushën e krimit kibernetik – tendencat dhe instrumentet
* Teknologjia e përfshirë në krimin kibernetik
* Krimi kibernetik si vepër penale në legjislacionin e brendshëm
* Legjislacioni, procedura dhe praktika në lidhje me provat elektronike
* Ligji procedural/masat hetimore në legjislacionin e brendshëm
* Legjislacioni ndërkombëtar

## Pse është i domosdoshëm ky trajnim

Gjyqtarët dhe prokurorët luajnë një rol të rëndësishëm në hetimin dhe gjykimin e individëve ose grupeve që kryejnë krime. Me rritjen e numrit të krimeve që kanë brenda tyre elemente të krimit kibernetik ose të provave elektronike, rritet nevoja që gjyqtarët dhe prokurorët të jenë të trajnuar siç duhet dhe të kuptojnë natyrën e këtyre krimeve dhe gjithashtu të jenë të ndërgjegjshëm për legjislacionin dhe instrumentet e bashkëpunimit ndërkombëtar të disponueshme për trajtimin e këtyre çështjeve.

Kriminelët dhe grupet kriminale në përgjithësi nuk e kufizojnë veten dhe aktivitetin e tyre sipas kufijve të shteteve. Krimi kibernetik është një lloj krimi që e përjashton mundësinë që keqbërësi të udhëtojë nëpërmjet këtyre kufijve për të kryer krimin, pra duke e bërë hetimin dhe ndjekjen ligjore shumë më të vështirë. Kjo thekson nevojën për përmirësimin e bashkëpunimit rajonal/ndërkombëtar si dhe bashkëpunimin ndërmjet institucioneve në trajtimin e çështjeve të krimit kibernetik.

Çështjet e krimit kibernetik shpesh kërkojnë një bashkëpunim rajonal ose ndërkombëtar të shpejtë dhe shumë efikas, i cili do të realizonte një hetim dhe ndjekje ligjore të keqbërësve brenda afateve. Si rezultat, institucionet trajnuese duhet të bëjnë përpjekje për të përfshirë në programet e tyre mësimore module që përmbajnë udhëzime dhe instrumente të bashkëpunimit ndërkombëtar, të cilat mund të përdoren gjatë hetimit të çështjeve të krimit kibernetik, duke përfshirë përdorimin 24/7 të pikave të kontaktit, MLA, Aktivitetin e Bashkëpunimit Gjyqësor, Platformat e Bashkëpunimit Gjyqësor, etj.

## Programi Mësimor

Ky program është një instrument bazë për t’u marrë në konsideratë nga institucionet trajnuese gjatë realizimit të trajnimit për krimin kibernetik. Qëllimi i këtij dokumenti është fokusimi tek krijimi dhe prodhimi i kurseve dhe moduleve të standardizuara që do të përdoren në zonat/vendet e projektit në zhvillimin e trajnimit fillestar për gjyqtarët dhe prokurorët të angazhuar në ndjekjen ligjore ose gjykimin e çështjeve të krimit kibernetik.

Modeli i propozuar i modulit për trajnimin e gjyqtarëve duhet të shërbejë vetëm si bazë për trajnimin e gjyqtarëve dhe të prokurorëve dhe jo si objektivi final për trajnimin e tyre. Zonat/vendet e projektit duhet të diskutojnë nevojat në nivel kombëtar dhe të kërkojnë trajnime specifike shtesë në fushat e krimit kibernetik që do t’i përcaktojnë si më delikatet.

Mësimet që janë përgatitur japin titujt/temat e prezantimeve/leksioneve si dhe shpjegime të detajuara që duhet të jepen nga trajnerët. Kursi është hartuar të modifikohet për t’iu përshtatur kërkesave kombëtare, duke garantuar në të njëjtën kohë që të përmbushen objektivat dhe qëllimi i tij. Kjo do t’i japë njëtrajtësi moduleve të trajnimit në të gjitha vendet ndërkufitare. Trajnerët duhet të marrin në konsideratë numrin e ushtrimeve/diskutimeve që do të lehtësojnë përvojën e të mësuarit nga pjesëmarrësit në secilin vend.

Moduli bazë i trajnimit është ndërtuar në një mënyrë të tillë që t’iu mundësojë gjyqtarëve dhe prokurorëve që do të trajnohen me anë të tij asimilimin e njohurive bazë për natyrën e krimit kibernetik, terminologjinë dhe teknologjinë. Krahas kësaj, ky modul jep informacion bazë në lidhje me bashkëpunimin ndërkombëtar, provat elektronike, ligjin procedural dhe masat hetimore etj.

Do të ketë një modul për trajnim të avancuar që do të jetë shtesë dhe do të hartohet bazuar në Modulin Bazë. Ai do të ofrojë njohuri dhe informacion më të detajuar në lidhje me tematikat, dhe do të përdorë raste praktike për përforcimin e mësimeve në sesionet e paraqitura në modulin bazë. Moduli i avancuar do të krijohet me synimin e pajisjes së gjyqtarëve dhe të prokurorëve me njohuri të përparuara që mund të zbatohen në praktikë për funksionimin e kompjuterëve dhe rrjeteve, çfarë është krimi kibernetik, legjislacioni për krimin kibernetik, juridiksioni, mjetet hetimore dhe provat elektronike, dhe bashkëpunimi ndërkombëtar.

# Si përdoret guida për trajnerët

Kjo guidë ka për synim të pajisë trajnerët me informacion në lidhje me strukturën dhe përmbajtjen e kursit. Objektivat për secilin mësim japin informacionin që do të ofrohet. Është përgatitur metodologjia e trajnimit për këtë kurs dhe të gjithë komponentët ndihmues përkatës duhet të jenë me këtë paketë trajnimi. Synimi i guidës është ruajtja e standardit të kursit dhe garantimi i njëtrajtshmërisë gjatë zhvillimit të tij.

Kjo guidë është hartuar të ofrojë udhëzime në lidhje me llojin dhe nivelin e njohurive teknologjike që kërkohen që gjyqtarët dhe prokurorët të përmbushin me efektivitet rolin e tyre. Nuk pretendon të jetë një analizë e plotë e çështjeve dhe sipas rastit tregon se ku mund të merret informacion shtesë.

Rekomandohet që zhvilluesit e trajnimit të garantojnë që materiali që përgatisin të jetë i kohës dhe të përfshijë çështjet më të fundit për teknologjinë sepse ato ndikojnë në sjelljen kriminale; ndikimin e saj tek rregullat ligjore, procedurale dhe rregullat për provat brenda juridiksionit ku do të zhvillohet trajnimi. Ka ndryshime teknologjike që do të ndikojnë sistemin e drejtësisë penale, të tilla si ruajtja në gjendje të ngurtë e të dhënave dhe format e reja “Web 2.0” të faqeve të Internetit. Këto do të jenë çështje të rëndësishme për tu përfshirë në programet e trajnimit dhe kërkojnë përfshirje sepse bëhen më mbizotëruese.

Si me çdo program tjetër, çdo kurs trajnimi i zhvilluar për gjyqtarë dhe prokurorë duhet të ketë objektiva të qarta, të cilat duhet të jenë objektiva SMART (Specifike, të Matshme, të Arritshme, Reale dhe me Afat). Kjo është thelbësore për të garantuar se objektivat do të arrihen. Duhet të evitohet përdorimi i objektivave me fjalë të tilla si “kuptoj” ose “njoh” sepse këto nuk i përmbushin kriteret. Për shembull, si mund të matet nëse është arritur objektivi i “njohjes” së një subjekti? Është më mirë të përdoren fjalë të tilla si “rendit” ose “identifikoj”, të cilat janë të matshme.

Përdorimi i rasteve praktike për të informuar audiencën konsiderohet i përshtatshëm për këtë lloj trajnimi dhe është më në përputhje me stilet e mësimdhënies për të rriturit sesa thjesht mësimdhënia didaktike.

Roli kyç i zhvilluesit të trajnimit është garantimi i arritjes së synimit të përgjithshëm të çdo aktiviteti mësimdhënës dhe të objektivave specifike. Ky kapitull jep informacion për të ndihmuar këtë proces.

Megjithëse ky kurs është zhvilluar si një program bazë, jo i specifikuar për një shtet të caktuar, është e rëndësishme që trajnerët t’i modifikojnë materialet e tyre të trajnimit për të garantuar një asimilim efikas të materialeve të kursit. Përdorimi i rasteve praktike për informimin e audiencës konsiderohet i përshtatshëm dhe është më tepër në përputhje me stilet e mësimdhënies për të rritur sesa thjesht mësimdhënia didaktike. Përdorimi i shembujve konkret nga teknologjia e referuar dhe përdorimi i Internetit gjithashtu mund ta përmirësojnë të mësuarin. Konkretisht, sesionet për ligjin material dhe atë procedural në legjislacionin e brendshëm janë përgatitur si ekzemplarë të llojit të informacionit që duhet të përfshihet në nivel kombëtar. Trajnerët janë përgjegjës për të garantuar se legjislacioni i tyre kombëtar është i përfshirë në këto sesione përpara zhvillimit të kurseve në vendin e tyre.

# Vështrim i Përgjithshëm i Kursit

## Sa i gjatë është kursi dhe për kë është

Ky kurs është hartuar si një program tre ditor për gjyqtarët dhe prokurorët si pjesë e programit të tyre të formimit fillestar.

## Kush do ta japë kursin

Kursi është hartuar për tu zhvilluar nga trajnerët vendas të institucioneve të trajnimit gjyqësor. Sipas rastit, është e këshillueshme që specialistët e lëndës të njihen me trajtimin e çështjeve teknike specifike nëse ekspertiza nuk është e disponueshme në qendrat e trajnimit gjyqësor. Meqenëse ky është nivel bazë, është e pritshme që ky kurs të zhvillohet për të gjithë gjyqtarët dhe prokurorët.

## Si do të jepet kursi

Kursi, me strukturën aktuale, është hartuar të zhvillohet në klasë duke përdorur udhëzimet që mund të jepen nga trajneri në klasë. Nëse nevojitet materialet mund të konvertohen në module për mësimin në distancë apo mësimin nëpërmjet Internetit. Siç është e detajuar më lart në Seksionin 1, trajnerët duhet të marrin në konsideratë përfshirjen e ushtrimeve dhe metodave të tjera të mësimdhënies në programin e nivelit kombëtar.

## Objektivat e kursit

Objektivat e kursit janë hartuar në mënyrë tradicionale për t’i lejuar trajnerëve të përdorin metoda të ndryshme mësimdhënieje për ti arritur ato. Të gjitha objektivat janë në formën “SMART” për ta mbështetur arritjen e tyre. Për ata që nuk i njohin objektivat “SMART”, jepet shpjegimi i mëposhtëm i mnemonikës:

* **Specifike –** Objektivat duhet të specifikojnë atë që duhet të arrijnë.
* **(Të) Matshme** – Duhet të jesh në gjendje të matni nëse i arrini objektivat ose jo.
* **(Të) Arritshme** – A janë të arritshme objektivat e caktuara prej jush?
* **Reale –** A mund t’i arrini objektivat realisht me burimet që keni në dispozicion?
* **(Në) Kohë –** Kur dëshironi t’i arrini objektivat e caktuara?

Bazuar në sa më sipër, janë caktuar objektivat e mëposhtëm dhe ato duhet të lexohen në kuadër të synimit të përgjithshëm të kursit.

## Grupi i trajnerëve dhe pjesëmarrësit e synuar

### Pjesëmarrësit

Ky kurs është hartuar për tu zhvilluar me gjyqtarët dhe prokurorët gjatë periudhës së formimit të tyre fillestar.

### Kriteret e përvojës

Nuk kërkohen njohuri të mëparshme për temën.

### Trajnerët

Trajnerët për këtë kurs duhet të merren nga qendrat e trajnimit gjyqësor ku do të zhvillohet kursi.

### Kriteret e përvojës

Trajnerët duhet të kenë një nivel të mirë të njohurive për tendencat/çështjet dhe legjislacionin për krimin kibernetik në vendin e tyre të origjinës. Kërkohen të kenë përvoja të mëparshme si trajnerë me njohuri për teorinë dhe praktikën e mësimdhënies.

## Burimet

### Kriteret për burimet e kursit

Për dhënien e këtij kursi në një klasë, janë të nevojshme pajisjet e mëposhtme:

* Një sallë me madhësi të përshtatshme sipas numrit të pritshëm të pjesëmarrësve në kurs.
* Kompjuter tavoline apo kompjuter laptop me sistem operimi Windows 7 dhe me programin MS Office Professional të instaluar
* Projektor dhe ekran për shfaqjen e imazheve
* Lidhje Interneti (nëse është e disponueshme)
* Modele të komponentëve fizikë të kompjuterit (nëse janë të disponueshme)
* Klipin e Videos “Warriors of the Net”
* Konventën e Budapestit për Krimin Kibernetik duke përfshirë raportin shpjegues
* Kopje të guidës për provat elektronike të financuar nga EC OISIN
* Tabelë të Bardhë
* Markera shkrues për Tabelën e Bardhë (të paktën 2 për secilën ngjyrë: blu, të zinj, të kuq dhe jeshilë)
* 2 Tabela Flipchart me letër të mjaftueshme
* Stilolapsa dhe blloqe për pjesëmarrësit
* Kapëse aktesh, hapëse vrimash dhe gërshërë
* Ngjitës “Blu tack” ose një produkt të ngjashëm për të ngjitur përkohësisht letrën në mure .

## Vlerësimi

Nuk është kërkuar apo ofruar ndonjë vlerësim i njohurive të pjesëmarrësve si pjesë e këtij kursi pilot. Vendet që e zbatojnë këtë trajnim në nivel kombëtar mund të duan të përfshijnë ndonjë vlerësim paraprak të pjesëmarrësve. Në çdo rast, trajnerët duhet të kontrollojnë njohuritë e studentëve gjatë kursit, me anë të pyetjeve, kuizeve apo metodave të tjera për të garantuar arritjen e objektivave të mësimdhënies.

## Objektivat e mësimit dhe të kursit

| **Numri i Mësimit** | **Titulli i Mësimit** | **Objektivat** |
| --- | --- | --- |
| **1.1.1** | **Hyrja në Kurs** | * Identifikoni trajnerët dhe pjesëmarrësit * Përcaktoni strukturën dhe përmbajtjen e kursit * Plotësoni detyrat përkatëse administrative * Shpërndani dokumentacionin e kursit * Shpjegoni pajisjet dhe procedurat në vend duke përfshirë Çështjet e Sigurisë dhe të Shëndetit |
| **1.1.2** | **Hyrje në Krimin Kibernetik** | * Identifikoni llojet e ndryshme të krimit kibernetik dhe impaktin e tyre * Rendisni në një listë kërcënimet, tendencat dhe mjetet e krimeve kibernetike dhe përgjigjet ndaj këtij fenomeni. * Shpjegoni konceptet e krimit kibernetik që konsiderohen vepra penale sipas legjislacioneve kryesore dhe standardeve ndërkombëtare. * Analizoni nevojat dhe avantazhet e harmonizimit të legjislacionit të brendshëm dhe instrumenteve ndërkombëtare, në veçanti Konventa e Budapestit. |
| **1.1.3**  **1.2.2**  **1.2.5** | **Hyrje në Teknologji** | * Rendisni në një listë pjesët përbërëse të një sistemi kompjuterik * Identifikoni llojet e ndryshme të mjeteve për ruajtjen e të dhënave * Merrni në konsideratë implikimet e drejtësisë penale për kapacitetin e ruajtjes së të dhënave eksponenciale * Identifikoni sistemet e ndryshme të operimit në kompjuterë * Jepni informacionin bazë sesi funksionojnë rrjetet * Përshkruani funksionet e Internetit * Identifikoni të paktën 5 programe të mëdha përdorimi në Internet * Shpjegoni sesi është zhvilluar Interneti që nga fillimi deri më sot. * Diferenconi ndërmjet programeve të ndryshme të përdorimit në Internet * Identifikoni sesi keqbërësit përdorin programet e ndryshme të përdorimit në Internet |
| **1.2.3** | **Krimi kibernetik si vepër penale në legjislacionin e brendshëm** | * Rendisni në një listë dispozitat e ligjit penal material, dhe identifikoni disa prej faktorëve kyç të përdorur për përshkrimin e veprave penale, bazuar në Konventën e Budapestit. * Rendisni në një listë dispozitat e ligjit penal material, dhe identifikoni disa prej faktorëve kyç të përdorur për përshkrimin e veprave penale, bazuar në legjislacionin ekzistues të brendshëm. * Analizoni nevojat dhe avantazhet e harmonizimit ndërmjet legjislacionit kombëtar dhe instrumenteve ndërkombëtare, në veçanti Konventa e Budapestit. * Identifikoni dispozitat përkatëse të ligjit material nga diskutimet e rasteve praktike |
| **1.2.4** | **Ligji procedural/masat hetimore në legjislacionin e brendshëm** | * Shpjegoni dispozitat procedurale të Konventës së Budapestit * Shpjegoni dispozitat ekzistuese procedurale sipas legjislacionit të brendshëm |
| **1.3.3**  **1.3.4** | **Mbledhja e provave elektronike; masat hetimore dhe procedurale** | * Diskutoni llojet e ndryshme të provave elektronike * Shpjegoni parimet e praktikës më të mirë që lidhet me sekuestrimin dhe administrimin e provave elektronike * Identifikoni sfidat e paraqitura nga “mbledhja e provave me kompjuter të fikur”, “mbledhja e provave me kompjuter të ndezur” dhe burimet e provave elektronike në Internet * Identifikoni sfidat e marrjes së provave nga një juridiksion tjetër * Diskutoni çështjet e pranueshmërisë së provave elektronike në procedimet gjyqësore, përsa i takon vërtetësisë, saktësisë, dhe plotësisë së tyre * Shpjegoni dispozitat procedurale të Konventës së Budapestit |
| **1.3.4** | **Bashkëpunimi ndërkombëtar** | * Njihni dimensionin global të Internetit dhe dimensionin ndërkombëtar të krimit kibernetik * Shpjegoni rëndësinë e bashkëpunimit ndërkombëtar dhe njihni instrumentet e disponueshëm për bashkëpunimin ndërkombëtar në fushën e krimit kibernetik * Identifikoni nevojën për kanale të shpejta dhe efiçente për bashkëpunimin ndërkombëtar dhe instrumentet e disponueshëm, mënyrat e përdorimit të tyre, afatet kohore dhe efektshmërinë * Përshkruani përpjekjet nga organizatat ndërkombëtare në drejtim të implementimit të modaliteteve të reja të bashkëpunimit ndërkombëtar * Diskutoni Konventën e Budapestit për Krimin Kibernetik – identifikoni parimet e përgjithshme të saj, masat e përkohshme dhe rrjetin 24/7 për ndihmën e ndërsjellë juridike |
| **1.3.5** | **Mbyllja e kursit** | * Jepni informacionin e duhur për kursin dhe efektshmërinë e tij * Plotësoni formularët e vlerësimit të kursit të Këshillit të Evropës * Identifikoni nivelin pasues të mësimit që duhet që ata të përmirësojnë njohuritë dhe aftësitë e tyre në këtë fushë. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Këshilli i Evropës**  **Krimi Kibernetik për Gjyqtarët dhe Prokurorët**  **Kurs Trajnimi** | | | | | | | | | | | | |
| **Programi i Kursit – Moduli 1** | | | | | | | | | | | | |
|  | **09:00 - 10:00** | | **10:00 - 11:00** | | **11:00 - 12:00** | | **12:00 - 13:00** | **13:00 - 14:00** | **14:00 - 15:00** | **15:00 - 16:00** | | **16:00 - 17:00** |
| **Dita 1** | **1.1.1**  **Hapja e Kursit dhe Prezantimet** | | | **1.1.2**  **Hyrje në Kërcënimet, Tendencat dhe Sfidat e Krimit Kibernetik** | | | | **PUSHIM** | **1.1.3 Hyrje në Teknologji**  **Pjesa 1** | | | |
| **Dita 2** | **1.2.1**  **Rishikimi ditor** | **1.2.2 Hyrje në Teknologji**  **Pjesa 2** | | | | **1.2.3**  **Krimi Kibernetik si Vepër Penale në Legjislacionin e Brendshëm** | | **PUSHIM** | **1.2.4**  **Ligji Procedural dhe Masat Hetimore në Legjislacionin e Brendshëm** | | **1.2.5 Hyrje në Teknologji**  **Pjesa 3** | |
| **Dita 3** | **1.3.1**  **Rishikimi ditor** | **1.3.2 Provat Elektronike – Procedura dhe Praktika** | | | | **1.3.3**  **Provat Elektronike – Ligji Procedural dhe Ligji i Hetimit** | | **PUSHIM** | **1.3.4**  **Bashkëpunimi Ndërkombëtar** | | **1.3.5**  **Marrja e Vlerësimit nga pjesëmarrësit dhe Mbyllja e Kursit** | |

NB – Pushimet për kafe dhe pushimet e tjera do të bëhen në orare të përshtatshme gjatë secilës ditë të trajnimit

# Kontaktet Kryesore

Personat e mëposhtëm janë pikat e kontaktit për çdo pyetje në lidhje me kursin dhe përmbajtjen e tij:

|  |  |
| --- | --- |
| Alexander Seger  Drejtues i Departamentit të Mbrojtjes së të Dhënave dhe Krimit Kibernetik  Drejtoria e Përgjithshme për të Drejtat e Njeriut dhe Shtetin e së Drejtës (DG-I)  Këshilli i Evropës,  F-67075 Strasbourg Cedex  Tel. +33 3 90 21 4506  Fax +33 3 90 21 56 50  [alexander.seger@coe.int](mailto:alexander.seger@coe.int) | Mustafa Ferati  Oficer Programi  Departamenti i Mbrojtjes së të Dhënave dhe Krimit Kibernetik  Drejtoria e Përgjithshme për të Drejtat e Njeriut dhe Shtetin e së Drejtës (DG-I)  Këshilli i Evropës,  67075 Strasbourg Cedex, FRANCE Tel.: +33 (0)3 90 21 45 50 Fax: +33 (0)3 90 21 56 50  [Mustafa.Ferati@coe.int](mailto:Mustafa.Ferati@coe.int) |

# Planet Mësimore

|  |  |  |
| --- | --- | --- |
| Mësimi 1.1.1 Hyrje në Kurs | | **Kohëzgjatja: 90 Minuta** |
| **Burime materiale të nevojshme:**   * Kompjuter tavoline/laptop me Windows 7 dhe me Programin MS Office Professional të instaluar * Projektor dhe ekran për shfaqje imazhesh * Akses në Internet (nëse është i disponueshëm) * Modele të komponentëve fizikë të kompjuterit (nëse janë të disponueshëm) * Dërrasë të Bardhë * Markera për Dërrasë të Bardhë (të paktën 2 për secilën ngjyrë: blu, të zezë, të kuqe dhe jeshile) * 2 Tabela Flipchart me letër të mjaftueshme * Stilolapsa dhe blloqe për pjesëmarrësit * Kapëse aktesh, vrimahapëse dhe gërshërë * Ngjitës Blu ose një produkt të ngjashëm me të për ngjitjen e përkohshme të letrës në mure | | |
| **Synimi:** Pajisja e pjesëmarrësve me informacion në lidhje me nevojën për kursin e trajnimit dhe synimet dhe objektivat e tij. Garantimi se ata kanë informacion të mjaftueshëm për programin e aktiviteteve dhe axhendën e kursit. Ofrimi i informacionit për detajet administrative, të sigurisë dhe të shëndetit gjatë kursit. Prezantimi i pjesëmarrësve me trajnerët dhe pjesëmarrësit e tjerë. | | |
| **Objektivat:**  Nga fundi i mësimit, pjesëmarrësit do të jenë në gjendje të:   * Identifikojnë trajnerët dhe kolegët e tyre pjesëmarrës * Diskutojnë synimin e përgjithshëm të kursit * Shpjegojnë pse është i domosdoshëm ky kurs * Rendisin pjesët përbërëse të programit dhe aktiviteteve të kursit * Rendisin procedurat e sigurisë dhe shëndetit për vendin e kursit | | |
| **Slajdet** | **Përmbajtja:** | |
| Slajdet nga 1 në 23 | Hyrje  Ky është sesioni i hapjes së kursit. Gjatë këtij sesioni, pjesëmarrësit do të njihen me trajnerët dhe pjesëmarrësit e tjerë. Do të shpjegohen synimi dhe objektivat e kursit së bashku me metodologjinë e mësimdhënies.  Trajneri mund të zgjedhë që të përdorë “akullthyerësit” për t’i inkurajuar pjesëmarrësit të angazhohen në kurs dhe me njëri tjetrin që në fillim. | |
|  | **Prezantimet me PowerPoint (ose prezantimet e llojeve të tjera)**  Për këtë sesion është përgatitur një prezantim me PowerPoint. Ky është një prezantim i përgjithshëm dhe nuk merr në konsideratë çështjet kombëtare që mund të nevojitet të trajtohen kur ky kurs të zhvillohet në nivel kombëtar. Trajneri duhet të sigurohet që informacioni është i lidhur me vendin e zhvillimit të kursit. | |
| Slajdi 2 | Këtu trajtohen çështjet e shëndetit dhe të sigurisë. Këto do të varen nga vendi i zhvillimit të kursit. Është përgjegjësia e trajnerit të sigurohet që të ketë informacionin e saktë për t’iu dhënë pjesëmarrësve. | |
| Slajdi 3 | Këtu jepet informacion bazë i kursit për pjesëmarrësit: titulli i kursit është “Trajnim Bazë për Gjyqtarët dhe Prokurorët për Krimin Kibernetik dhe për Provat Elektronike”. Ai është zhvilluar si një produkt i Projektit të Përbashkët ndërmjet Bashkimit Evropian dhe Këshillit të Evropës për Bashkëpunimin Rajonal për Krimin Kibernetik në rajonin e IPA-s. | |
| Slajdi 4 | Synimet e sesionit janë renditur si më poshtë:   * Pajisja e pjesëmarrësve me informacion për nevojën për kurs trajnimi dhe synimi dhe objektivat e tij. * Garantimi që ata të kenë informacion të mjaftueshëm në lidhje me programin e aktiviteteve dhe kalendarin e tyre. * Ofrimi i informacionit për detajet administrative, të sigurisë dhe të shëndetit të kursit. * Prezantimi i pjesëmarrësve me trajnerët dhe pjesëmarrësit e tjerë. | |
| Slajdi 5 | Objektivat individuale janë gjërat që pjesëmarrësit do të jenë në gjendje të bëjnë në fund të sesionit. Këto objektiva mund të provohen për të testuar njohuritë që kanë fituar pjesëmarrësit dhe t’i lejojnë pjesëmarrësit të bëjnë vlerësimin e trajnimit. Për këtë sesion, pjesëmarrësit duhet të jenë në gjendje të:   * Identifikojnë trajnerët dhe kolegët e tyre pjesëmarrës * Diskutojnë synimin e përgjithshëm të kursit * Shpjegojnë pse është i domosdoshëm ky kurs * Rendisin pjesët përbërëse të programit dhe aktiviteteve të kursit * Rendisin procedurat e sigurisë dhe të shëndetit të vendit | |
| Slaidi 6 | Ky trajnim është i domosdoshëm sepse gjyqtarët dhe prokurorët luajnë një rol të rëndësishëm në hetimin dhe gjykimin e individëve dhe grupeve që kanë kryer vepra penale. Me rritjen e numrit të këtyre veprave, që kanë një element të krimit kibernetik ose provave elektronike, ekziston një nevojë në rritje që gjyqtarët dhe prokurorët të jenë të trajnuar siç duhet për të kuptuar natyrën e këtyre veprave penale dhe gjithashtu për të qenë të ndërgjegjshëm për legjislacionin dhe instrumentet e bashkëpunimit ndërkombëtar të disponueshme për trajtimin e çështjeve të krimit kibernetik. | |
| Slajdi 7 | Është e rëndësishme që synimi i përgjithshëm i kursit t’iu shpjegohet pjesëmarrësve që në fillim të tij. Kjo do t’iu mundësojë atyre të vlerësojnë arsyen gjithëpërfshirëse e prezencës së tyre në kurs. Synimi i përgjithshëm i këtij kursi është:  T’i pajisë gjyqtarët dhe prokurorët me një nivel bazë njohurish për krimin kibernetik dhe provat elektronike. Kursi do të japë informacion praktik dhe ligjor në lidhje me temën në fjalë dhe përqendrohet sesi këto çështje ushtrojnë ndikimin e tyre në punën e përditshme të pjesëmarrësve. | |
| Slajdi 8 | Në këtë fazë pjesëmarrësve duhet t’iu shpjegohet programi i kursit. Kjo duhet të përfshijë ndarjen e kohës gjatë kursit, pushimet e drekës dhe pushimet e tjera, si dhe një përshkrim të shkurtër për secilin sesion. Në këtë fazë do të trajtohet edhe përfshirja ose përjashtimi i ndonjë vlerësimi. Nëse ka një vlerësim, ky duhet të shpjegohet në detaje, duke përfshirë pritshmëritë e pjesëmarrësve sa i takon mësimit. | |
| Slajdet nga 9 në 17 | Këtu parashtrohen objektivat e detajuar për secilin sesion. Këto duhet të shpjegohen për pjesëmarrësit në këtë fazë. Në shpjegim janë të përfshira dhe pjesët themelore të secilit leksion. | |
| Slajdi 20 | Faza tjetër është prezantimi i trajnerëve dhe pjesëmarrësve. Është e rëndësishme që të shfrytëzohet kjo mundësi për t’i bërë pjesëmarrësit të ndërveprojnë me njëri tjetrin dhe me trajnerët. Pjesëmarrësve duhet t’iu kërkohet të bëhen dyshe në klasë me një pjesëmarrës që nuk e njohin. Më pas atyre do t’iu kërkohet që ta pyesin partnerin e tyre të japë përgjigje pyetjeve të mëposhtme:   * Emrin dhe Vendin * Ku punon * Çfarë bën * Përvojën e tij/saj si trajner * Diçka interesante rreth tij/saj * Përgjigje ndaj “pyetjeve për njohuritë” | |
| Slajdi 21 | “Pyetjet për njohuritë” janë hartuar të krijojnë ndërveprim dhe që trajnerët të mësojnë më shumë rreth njohurive dhe përvojave të pjesëmarrësve në secilën prej kategorive të teknologjisë dhe krimit kibernetik. Këto janë të renditura në slajdin pasues. Pjesëmarrësve duhet t’iu kërkohet të tregojnë se cili numër përfaqëson nivelin e njohurive të tyre në secilën prej kategorive.  Çiftet duhet të bëjnë të njëjtat pyetje për secilin. Më pas ata duhet t’ia prezantojnë “kolegun” pjesës së tjetër të klasës. Trajneri duhet të mbajë shënime për informacionin që jepet për të ndihmuar njohuritë e tyre për pjesëmarrësit. | |
|  | **Ushtrime Praktike (nëse nevojitet)**  Ushtrimi i vetëm praktik në këtë sesion është prezantimi i pjesëmarrësve dhe trajnerëve dhe kriteret për këtë janë parashtruar në seksionin e mëparshëm. | |
|  | Kontrolli i Njohurive  Nuk ka kontroll njohurish në këtë seksion. | |
| Slajdi 23 | Përmbledhje  Trajneri duhet të përsërisë/testojë njohuritë në çështjet e mëposhtme për tu siguruar se pjesëmarrësit i kanë vlerësuar objektivat e mësimit në këtë sesion. Gjatë sesionit duhet të lejohet një kohë e caktuar për pyetjet. | |

|  |  |  |
| --- | --- | --- |
| Mësimi 1.1.2 Hyrje në Krimin Kibernetik | | **Kohëzgjatja: 120 minuta** |
| **Burimet materiale të nevojshme:**   * Kompjuter tavoline apo laptop me Windows 7 dhe me programin Office 2010 të instaluar * Projektor * Prezantimi në formatin PowerPoint | | |
| **Synimi:**  Synimi i këtij mësimi është t’i japë pjesëmarrësve një vështrim të përgjithshëm për krimin kibernetik, edhe në këndvështrimin ligjor edhe në perspektivën e realiteteve të reja. Ai do të trajtojë skenarin e detajuar në vende të ndryshme dhe kuadrin ligjor në nivel ndërkombëtar. | | |
| **Objektivat:**   * Gjatë mësimit do të jepet për pjesëmarrësit një shpjegim se çfarë është krimi kibernetik dhe pse duhet të shqetësohemi për të. Mësimi do t’i referohet kërcënimeve, tendencave dhe instrumenteve të krimit kibernetik, si sfida për gjyqtarët dhe prokurorët. Krahas kësaj, sesioni do të përshkruajë reagimet kombëtare dhe ndërkombëtare ndaj këtij fenomeni. * Në fund të mësimit pjesëmarrësit do të jenë në gjendje të identifikojnë realitetet e përfshira në termin “krim kibernetik” dhe do të kuptojnë konceptet që konsiderohen lloje të krimit sipas shumicës së legjislacioneve dhe në përputhje me standardet ndërkombëtare. * Sesioni do të trajtojë dispozitat e ligjit penal material, mbas zhvillimeve më të fundit që lidhen me veprat penale të krimit kibernetik dhe do të verë theksin tek disa faktorë kyç të përdorur për të përshkruar krimet, bazuar në Konventën e Budapestit dhe në kuadrin përkatës ligjor në nivelin e Bashkimit Evropian. * Sa i takon kësaj pike të fundit, në këtë sesion do të nënvizohen nevojat dhe avantazhi i harmonizimit ndërmjet legjislacionit vendas dhe instrumenteve ndërkombëtare, dhe në veçanti Konventa e Budapestit. | | |
| **Slajde nr.** | **Përmbajtja:** | |
|  | Hyrje  Ky sesion ka qëllimin e posaçëm t’i japë pjesëmarrësve një vështrim të përgjithshëm për krimin kibernetik, edhe në këndvështrimin ligjor edhe në perspektivën e realitetit efektiv. Ai do të trajtojë skenarin e detajuar në vende të ndryshme dhe do t’i referohet kuadrit ligjor në nivel ndërkombëtar. | |
| Slajdi 2 | Axhenda  Pjesa e Parë e prezantimit do të përshkruajë realitetet e reja të shoqërisë së informacionit dhe do t’i referohet aktiviteteve të paligjshme që po shfaqen në rrjete.  Pjesa e Dytë do të trajtojë disa prej qasjeve historike ndaj krimit kibernetik nga disa organizata ndërkombëtare.  Pjesa e Tretë do të përpiqet të arrijë realitetin e përshkruar nga koncepti eventual i krimit kibernetik.  Pjesa e Katërt do të shpjegojë se çfarë është Konventa e Budapestit dhe do të nënvizojë rëndësinë e këtij instrumenti të vetëm të detyrueshëm ndërkombëtar në luftën kundër krimit kibernetik.  Pjesa e Pestë do t’i referohet disa prej aktiviteteve të paligjshme më të rëndësishme online, në ditët e sotme.  Pjesa e Gjashtë do të trajtojë temat më të rëndësishme në të gjithë prezantimin. | |
| Slajdi 3 | Objektivat e Sesionit  Synimi i këtij sesioni është paraqitja, nga një këndvështrim i përgjithshëm ose si një hyrje, e çështjeve që lidhen me krimin kibernetik.  Do të shpjegohet koncepti i krimit kibernetik, duke shpjeguar arsyet se pse duhet të preokupohemi. Do të diskutohen këtu disa prej kërcënimeve kryesore, tendencat dhe mjetet e krimit kibernetik dhe disa prej reagimeve ndaj këtij fenomeni.  Do të jepet një vështrim i asaj çfarë jepet nga shprehja “krim kibernetik”. Krahas kësaj, do të diskutohet për përshkrimin e disa prej koncepteve që konsiderohen lloje të krimit kibernetik sipas shumicës së legjislacioneve dhe në përputhje me standardet ndërkombëtare.  Një prej temave më të rëndësishme për tu diskutuar lidhet me dispozitat e ligjit penal material, dhe disa prej faktorëve kyç të përdorur në përshkrimin e krimeve kibernetike, bazuar në Konventën e Budapestit dhe në kornizat ligjore përkatëse të Bashkimit Evropian.  Do të jetë gjithashtu e rëndësishme të nënvizohen nevojat dhe avantazhi i harmonizimit të legjislacionit të brendshëm me instrumentet ndërkombëtare, në veçanti Konventa e Budapestit. | |
| Slajdi 4 | Pjesa e Parë – Shoqëria e Informacionit dhe Krimi Kibernetik | |
| Slajdet 5 deri 7 | Shoqëria e informacionit, një model zhvillimi social ekonomik, bazuar në përftimin dhe përhapjen e informacionit me anë të rrjeteve të komunikimit, përshkonte jetën e përditshme të qytetarëve, vendin e tyre të punës, shtëpitë e tyre dhe shumë prej aktiviteteve të tyre zbavitëse.  Në këtë mjedis social ekonomik, nuk ekzistojnë distanca fizike ndërmjet njerëzve në vende të ndryshme të botës. Me disa përjashtime të njohura mirë, në këtë “botë të hapur”, potencialisht, nuk ekzistojnë kufijtë politikë (ndërmjet Shteteve), ndërmjet naviguesve në Internet. Këtu, kushdo mund të marrë në mënyrë demokratike informacion dhe njohuri, pavarësisht se ku mbahet ky informacion. Kjo do të thotë gjithashtu se ka konkurrencë ndërmjet të gjithë operatorëve ekonomikë.  Informacioni është i disponueshëm për këdo, në mënyrë të hapur dhe të lirë. Përdoruesit e Internetit ndjejnë se nuk ekziston asnjë sovranitet mbi rrjetet. | |
| Slajdi 8 | Ndërsa përdorimi i Internetit mbërrin kudo dhe tek kushdo në botë, krimet rriten dhe kriminelët zbulojnë aktivitete të reja të mundshme, të paligjshme. Krimet e kryera me anë të rrjeteve janë ndër krimet më transnacionale.  Kjo natyrë e krimeve krijon vështirësi të posaçme për ata që hetojnë këto aktivitete kriminale: nga ana tjetër e botës, provat mund të zhduken nëse nuk ruhen menjëherë dhe autoritetet e zbatimit të ligjit duhet të respektojnë kufijtë politikë. Krahas kësaj, ata duhet të ndjekin procedimet ligjore dhe kanalet publike për të kërkuar ndihmë ndërkombëtare në hetimet penale. | |
| Slajdi 9 | Në këtë kontekst qasja ndërkombëtare është thelbësore. Qasja ndërkombëtare dhe shumështetësore është më e pasur sesa një qasje thjesht kombëtare ose madje dhe rajonale; gjithpërfshirja globale e fenomenit i jep një dimension më të gjerë. Bashkëpunimi ndërkombëtar ndërmjet institucioneve të zbatimit të ligjit – brenda policisë ose ndërmjet prokurorive – është thelbësor për arritjen e rezultateve në hetimet penale. | |
| Slajdi 10 | Të gjithë vëzhguesit janë në një mendje se krimi kibernetik është një fenomen global dhe qasja e vetme adekuate për të adresuar natyrën pa kufij të rrjeteve globale është një qasje e përbashkët, ku përpjekjet e brendshme plotësohen nga norma specifike dhe kanale të bashkëpunimit ndërkombëtar që mund të përballen me krimin kibernetik që lehtësohet globalisht, me pasoja të mundshme në çdo pjesë të botës.  Është shumë e qartë se krimi kibernetik është një fenomen global me dimensione globale. Në mënyrë tipike, secili aktivitet i paligjshëm ka lidhje territoriale të shumëfishta: zakonisht keqbërësit bazohen në juridiksionin e secilit vend, por veprimet e tyre mbërrijnë deri tek kompjuterët dhe viktimat në shumë vende të tjera.  Kjo është një karakteristikë e përbashkët me forma të tjera moderne të kriminalitetit, por në lidhje me krimin kibernetik dhe provat elektronike në përgjithësi, është e integruar me natyrën e tyre. Për shkak të zgjerimit të rrjeteve të komunikimit, veçanërisht të Internetit, është e pamundur për çdo vend në botë të veprojë i vetëm kundër problemeve të këtij krimi. | |
| Slajdi 11 | Shoqëritë moderne varen nga teknologjitë e informacionit. Shtetet, qytetarët dhe ekonomitë janë aktualisht të lidhura me Internetin. Kjo është një fushë shumë pjellore për lindjen e aktiviteteve të reja të paligjshme, brenda rrjeteve të komunikimit, duke përdorur rrjetet, ose kundër rrjeteve. | |
| Slajdi 12 | Kudo, krimi kibernetik identifikohet me fenomene si *hacking[[3]](#footnote-4)*, ose përhapjen e *malware[[4]](#footnote-5)* (kryesisht viruse ose krimba[[5]](#footnote-6)), ose popullore, brenda njësisë kompjuterike, sulme kompjuterike (*DoS* ose *DDos*). Megjithatë, në ditët e sotme edhe qytetari i thjeshtë është i ndërgjegjshëm për shumë prej aktiviteteve të tjera të paligjshme në rrjete, shumica e tyre për qëllime përfitimi (vg. mashtrimet e zakonshme dhe mashtrimet kompjuterike). Gjithashtu gjithsecili është në dijeni të mundësive të mëdha të përdorimit të mjedisit kibernetik, ose ekosistemit kibernetik, për kryerjen ose lehtësimit e krimeve tradicionale. | |
| Slajdi 13 | Shprehja, “*mjedis kibernetik”*, edhe pse mbetet akoma e papërcaktuar, edhe në literaturën juridike edhe në atë akademike, pasurohet çdo ditë dhe bëhet gjithnjë e më komplekse. Teknologjia është duke rritur numrin dhe llojet e pajisjeve që mund të komunikojnë në rrjet dhe që janë në gjendje të transferojnë të dhëna ose vetëm ti regjistrojnë ato. | |
| **Slajdet 15 dhe 16** | Pjesa e Dytë – Organizatat ndërkombëtare dhe krimi kibernetik  Shumë organizata ndërkombëtare, për shumë vite, kanë trajtuar çështjen e krimit kibernetik dhe provave elektronike. | |
| Slajdet 17 deri 20 | Kombet e Bashkuara është një nga forumet ku diskutohet rreth krimit kibernetik. Asambleja e Përgjithshme e Kombeve të Bashkuara, që nga viti 2000, ka miratuar rezoluta zyrtare për *Luftën kundër Abuzimit Kriminal të Teknologjive të Informacionit* (e para ishte Rezoluta e miratuar nga Asambleja e Përgjithshme 55/63, për luftën kundër abuzimit me teknologjitë e informacionit, miratuar nga seanca plenare e 81-të, në 4 Dhjetor 2000).  Këto rezoluta zyrtare nxjerrin në pah nevojën për të garantuar që një Shtet Anëtar të miratojë rregulla të brendshme, me qëllimin për kriminalizimin e disa aktiviteteve dhe eliminimin e të ashtuquajturave *vende të sigurta* për keqbërësit e hapësirës kibernetike.  Rezoluta e Asamblesë së Përgjithshme të Kombeve të Bashkuara 64/211 (Mars 2010) për “krijimin e një kulture globale të sigurisë kibernetike” përmban një instrument vetë-vlerësues vullnetar për përpjekjet e shteteve në mbrojtje të infrastrukturës së informacionit delikat. Ndër të tjera, rezoluta rekomandon që Shtetet të miratojnë legjislacion penal duke marrë në konsideratë instrumente të tilla si Konventa e Budapestit për krimin kibernetik.  Çdo pesë vjet, Kombet e Bashkuara organizojnë Kongresin për Parandalimin e Krimit dhe Drejtësinë Penale. Kongresi i vitit 2005 në Bangkok dhe Kongresi i vitit 2010 në Salvador (Brazil) ranë dakord për nevojën për ndihmë teknike dhe ngritjen e kapaciteteve.  Propozimet për zhvillimin e traktateve të reja nuk kanë gjetur konsensus. | |
| Slajdi 21 | OECD – Organizata për Zhvillimin dhe Bashkëpunimin Ekonomik ndan me Kombet e Bashkuara shqetësimin për fenomenet e krimit kibernetik. Megjithatë, ajo ka zhvilluar një qasje të ndryshme. Që nga viti 1983, OECD-ja ka studiuar nevojën ekzistuese për legjislacion të brendshëm për krimin kibernetik dhe ka nxjerrë rekomandime për këtë. OECD-ja deklaron se nga niveli ndërkombëtar në atë kombëtar, fakte të njëjta penale mund të kualifikohen brenda kornizave të ngjashme penale. | |
| Slajdi 22 | Qasja e Shteteve të Grupit të Tetëshes (G8) shkon edhe një hap më tej, duke përzgjedhur alternativa edhe më proaktive. G8-a krijoi një rrjet pikash kontakti që u bë referencë në skenarin e bashkëpunimit ndërkombëtar. Në thelb, rrjeti është një direktori me emra që mund të merren dhe mund të lehtësojnë veprimet e menjëhershme sipas nevojës.  G8-a ishte një pionier, në përballje me subjektet e krimit kibernetik, dhe përveç Këshillit të Evropës, kjo është puna më e rëndësishme e zhvilluar në nivel ndërkombëtar, në luftën kundër krimit kibernetik, në ditët e sotme. | |
| Slajdet 23 dhe 24 | Bashkimi Evropian (BE) gjithashtu duket në gatishmëri për krimin kibernetik. Në vitin 2005 BE-ja miratoi një instrument detyrues – Vendimin Kuadër të Këshillit 2005/222/JHA[[6]](#footnote-7) të 24 Shkurtit 2005 për sulmet kundër sistemeve të informacionit. Ky Vendim Kuadër u imponon të gjitha Shteteve Anëtare kriminalizimin e disa veprave të renditura: aksesi i paligjshëm në sistemet e informacionit, ndërhyrja e paligjshme në sistem, dhe ndërhyrja e paligjshme tek të dhënat. Vendimi gjithashtu përfshin rregullat që i referohen nxitjes, bashkëpunimit dhe tentativës.  Krahas kësaj, përsa i takon bashkëpunimit ndërkombëtar, Vendimi Kuadër thotë se të gjithë Shtetet Anëtare të Bashkimit Evropian duhet të sigurohen që të shfrytëzojnë rrjetin ekzistues të pikave operacionale të kontaktit të disponueshme 24 orë në ditë dhe shtatë ditë në javë.  Vendimi Kuadër 2005/222/JHA aktualisht është duke u rishikuar – që nga Janari 2011 (një draft i parë publik i projektit u publikua në Tetor 2011). | |
| Slajdi 25 | Gjithashtu është e rëndësishme të merret në konsideratë puna e bërë nga OSBE-ja, Organizata për Sigurinë dhe Bashkëpunimin në Evropë, për krimin kibernetik.  OSBE-ja nxjerr rekomandime për anëtarët e organizatës. Me vendimin nr. 7/06, OSBE-ja tha se Shtetet pjesëmarrëse duhet të marrin në konsideratë anëtarësimin në Konventën e Budapestit për Krimin Kibernetik. Ky vendim gjithashtu i inkurajoi Shtetet pjesëmarrëse të bëhen pjesë e rrjetit 24/7 kundër krimeve kompjuterike, i administruar nga Shtetet e G8-s dhe të caktonin një pikë të përshtatshme kontakti me qëllim lehtësimin e bashkëpunimit ndërkombëtar për zbatimin e ligjit në luftën kundër abuzimit kriminal të hapësirës kibernetike. | |
| Slajdi 26 | Këshilli i Evropës e ka trajtuar çështjen e krimit kibernetik që nga viti 1980. Puna përgatitore dhe rekomandimet e guidave më pas çuan drejt vendimit për të negociuar një traktat ndërkombëtar detyrues ligjërisht; Konventën e Budapestit për Krimin Kibernetik (ky traktat do të diskutohet më vonë).  Qasja e Këshillit të Evropës konsiston në një trekëndësh me:   1. Standarde si p.sh. Konventa e Budapestit 2. Aktivitete pasuese dhe “monitorim” i zbatimit nga Komiteti i Konventës për Krimin Kibernetik (T-CY) 3. Programet e bashkëpunimit teknik për të ndihmuar vendet në rritjen e kapaciteteve të drejtësisë penale. | |
| Slajdet 28 dhe 29 | Pjesa e Tretë – Çfarë është krimi kibernetik? | |
| Slajdi 30 | Teknologjia si viktimë  Teknologjia si objektiv i krimeve – tradicionalisht është konsideruar të jetë “krim kompjuterik” i vërtetë dhe përfshin vepra të tilla si hyrja e paautorizuar në sisteme kompjuterike, sulmet e mohimit të shërbimit dhe shpërndarjen e viruseve. | |
| Slajdi 31 | Teknologjia si ndihmë për krimin  Teknologjia si një ndihmë për krimin – ndodh kur kompjuterët dhe pajisjet e tjera përdoren për të ndihmuar në kryerjen e krimeve tradicionale, për shembull, prodhimin e dokumenteve të falsifikuar, dërgimin e kërcënimeve për vdekje ose kërkesat e shantazheve, ose krijimin dhe shpërndarjen e materialeve të paligjshme të tilla si imazhet e abuzimit me të miturit. | |
| Slajdi 32 | Teknologjia si një mjet komunikimi  Teknologjia si një mjet komunikimi – është kur kriminelët e përdorin teknologjinë për të komunikuar me njëri tjetrin në mënyra që i pakësojnë mundësitë e zbulimit, për shembull me anë të teknologjisë së kodimit. | |
| Slajdi 33 | Teknologjia si pajisje për mbajtjen e të dhënave  Teknologjia si një mjet për mbajtjen e të dhënave – është mbajtja e qëllimtë ose e paqëllimtë e informacionit në pajisje të përdorura në secilën prej kategorive të tjera dhe që zakonisht ka të bëjë me të dhëna të mbajtura në sistemet kompjuterike të viktimave, dëshmitarëve ose të dyshuarve. | |
| **Slajdi 34** | Teknologjia si dëshmitare për një vepër penale  Teknologjia si dëshmitare e një vepre penale – mund të gjendet kur provat e ndodhura në pajisjet e teknologjisë së informacionit mund të përdoren për mbështetjen e provave me të cilat nuk ka lidhje të dukshme, për shembull në vërtetimin ose hedhjen poshtë të alibisë së dhënë nga një i dyshuar apo një pretendim të bërë nga një dëshmitar. | |
| Slajdi 35 | Teknologjia – një krim?  Ky slajd mund të përdoret si përsëritje për të kontrolluar nëse pjesëmarrësit e kanë kuptuar se çfarë është shpjeguar deri tani. Sugjerohet që trajneri të fillojë vetëm me kreun dhe më pas t’i kërkojë pjesëmarrësve të identifikojnë llojet e veprave që mund të përshkruajmë kur përdorim fjalën Krim Kibernetik. Do të ishte e dobishme nëse trajneri i kupton tashmë llojet e ndryshme të veprave penale të dhëna në detaje në konventën e Budapestit me qëllim që t’i përdorë ato si shembuj ose t’iu përgjigjet pyetjeve që mund të ngrihen nga pjesëmarrësit. | |
| Slajdi 36 | Që nga viti 1984, kur novelisti William Gibson e përdori fjalën *hapësirë kibernetike*, në romanin fantastiko-shkencor *Neuromancer*, me të cilën i referohej Internetit dhe rrjeteve të tjera, numri i shprehjeve të ngjashme me të njëjtën parashtesë u zgjerua. Sigurisht krimi kibernetik është njëra prej tyre. Pothuaj tre dekada më vonë, autorët nuk kanë arritur një konsensus për një përkufizim të saktë të shprehjes *krim kibernetik*, pavarësisht nga literatura në rritje që pretendon të jetë për krimin kibernetik.  Nuk ekziston as edhe një marrëveshje nëse krimi kibernetik është në të vërtetë një fushë e re dhe e dallueshme e të drejtës penale, ose nëse është thjesht një set me dispozita individuale të të drejtës penale, që rastis t’i referohen mjedisit dixhital. | |
| **Slajdet 37 deri 44** | Megjithatë, nga pikëpamja sociologjike, krimi në mjediset kibernetike është tashmë një realitet autonom dhe i rëndësishëm. Në të gjithë Evropën ekzistojnë njësi të posaçme investigative në nivelin e forcave të policisë dhe disa shërbime të posaçme të prokurorisë. Organizatat publike ndërkombëtare dhe kompanitë private kanë përherë e më shumë preokupime për pasojat e akteve të dëmshme dhe të paligjshme të kryera nëpërmjet rrjeteve të komunikimit ose brenda këtyre rrjeteve.  Kur juristët duan të trajtojnë këtë realitet të ri nuk ekziston asnjë konsensus në lidhje me shprehjen *krim kibernetik*. Disa autorë e cilësojnë si *krim kompjuterik, ose krim informatik.* Të tjerët preferojnë *krim i teknologjisë së lartë*. Të gjitha këto përmbajnë riskun ose të zgjerimit të çështjes shumë larg, ose të kufizimit të saj në mënyrë të tepruar.  Krimet që përfshijnë kompjuterët nuk janë domosdoshmërisht “të teknologjisë së lartë”. Shumica e aktivitetit kriminal në hapësirën kibernetike përdor metoda relativisht të thjeshta dhe nxjerr relativisht pak probleme teknologjike në hetimin e tij. Megjithatë, ndoshta kjo është një çështje false sepse të gjithë bien dakord se në ditët e sotme ekziston një realitet social/kriminal, i kryer me anë të një sistemi kompjuterik.  Krimi kibernetik zakonisht përcaktohet edhe në sensin e ngushtë edhe në atë të gjerë: zakonisht shprehja përdoret, në një mënyrë të kufizuar, për të përshkruar një aktivitet kriminal, në të cilin një kompjuter ose një rrjet kompjuterik janë pjesë thelbësore e krimit; megjithatë krimi kibernetik përdoret gjithashtu për të përfshirë krimet tradicionale në të cilat po këto kompjuterë ose rrjete kompjuterike përdoren për të mundësuar realizimin e aktivitetit të paligjshëm.  Sipas kësaj perspektive, jemi duke folur për krimin kibernetik ku kompjuteri është një mjet për realizimin e aktivitetit kriminal (p.sh. *spamming[[7]](#footnote-8)*, *krimet e cënimit të të drejtave të autorit të kryera nëpërmjet rrjeteve* *peer-to-peer[[8]](#footnote-9)*, etj.); krime kibernetike në sensin që kompjuteri ose rrjeti kompjuterik është objektivi i krimit si p.sh. aksesi i paautorizuar, kodi i dëmshëm, etj.; krim kibernetik ku kompjuteri ose rrjeti kompjuterik është vendi i aktivitetit kriminal si p.sh. mashtrimet me telekomunikacionet; dhe së fundi krimi kibernetik që lehtësohet nëpërmjet përdorimit të kompjuterëve ose rrjeteve kompjuterike (d.m.th *Mashtrimi Nigerian[[9]](#footnote-10)*, *hyrja e paautorizuar në sistemin kompjuterik*, *phishing[[10]](#footnote-11)*, pornografia e të miturve, vjedhja e identitetit, etj.) – në kategorinë e parë, kompjuteri është thelbësor në kryerjen e veprës penale; në kategorinë e fundit, vepra mund të kryhet me mjete të tjera, por kompjuteri e bën kryerjen më të lehtë.  Jo larg prej këtyre realiteteve, disa vepra penale të *epokës së re* janë thjesht modalitete të veprave penale tradicionale, të cilat kanë tipar dallues faktin se ato mund të kryhen brenda mjedisit dixhital.  Në fakt, për vetë natyrën e tyre, ato nuk mund të ndodhin jashtë botës virtuale dhe gjenerohen brenda saj. Për shembull kështu është mashtrimi kompjuterik ose rasti i falsifikimit kompjuterik.  Disa prej veprave penale kryhen me anë të sistemeve kompjuterike që, pavarësisht nga përdorimi i kompjuterëve si *mjete*, teorikisht nuk mund të dallohen nga i njëjti lloj i veprave të kryera me mënyra të tjera. Edhe sikur të jenë vepra penale të kryera *online*, ky tipar në vetvete nuk i transformon në lloje të reja të veprave penale. Nga ana doktrinale, asgjë nuk i dallon ato nga veprat penale tradicionale. Shembuj janë: shpifjet e kryera me anë të gazetave elektronike, ose kërcënimet me anë të postës elektronike, ose madje pastrimi i parave duke përdorur një bankë online.  Në këtë kontekst, ka dhe një kategori edhe më bazë: Krimet tradicionale *offline* që prapëseprapë gjenerojnë prova dixhitale – për shembull një sulmues që filmon sulmin e tij “të papritur” me celularin e tij dhe e poston filmimin në uebsajtin *youtube*. Edhe pse ky incident mund të mos quhet *krim kibernetik*, ai ngre disa çështje të njëjta për hetimin dhe provat siç quhen kështu në krimin kibernetik.  Por zakonisht, lloji i kriminalitetit i identifikuar si krim kibernetik është kategoria e veprave penale që mund të karakterizohet si kategoria që ka në objektiv mjedisin kompjuterik ose ekosistemin. Si shembuj klasikë të këtyre llojeve të veprave penale mund të jenë rastet e ndërhyrjes tek të dhënat, si për shembull sulmet e mohimit të shërbimit, ose madje dhe hyrja e paligjshme. Të gjithë këto cënime janë vepra penale kundër vetë sistemeve kompjuterike, përballë konfidencialitetit, integritetit ose disponueshmërisë së të dhënave kompjuterike ose të sistemit kompjuterik.  Shpesh, në skenarin e një krimi “real”, disa prej këtyre kategorive do të paraqiten së bashku. Për shembull, një keqbërës mund të kërcënojë një kompani me një sulm të mohimit të shërbimit kundër uebsajtit të kompanisë (veprat penale kundër sistemeve kompjuterike) po të mos u jepen para (një version i ri i shantazhit duke përdorur kompjuterët si mjete), dhe kërcënimi komunikohet nëpërmjet postës elektronike por që gjithashtu mund të dërgohet fare mirë edhe me anë të një letre të zakonshme).  Megjithatë, në terma realë ekziston një gamë e gjerë e modaliteteve kriminale në rritje: krimet kibernetik tipike si p.sh *phishing* ose përdorimi i *botnets*[[11]](#footnote-12) janë në rritje, si dhe grumbullimi i madh dhe kreativ i krimeve kibernetike për qëllime përfitimi. Ekziston gjithashtu një pirateri e konsiderueshme e programeve kompjuterike dhe probleme të tjera me të drejtat e pronësisë intelektuale. Përhapja e pornografisë së të miturve është në rritje, dhe po kështu është dhe vlera e parave që pastrohen me anë të Internetit. Në përgjithësi, çdo ditë ka një rritje të përdorimit të pajisjeve kibernetike nga organizatat e paligjshme dhe krimi i organizuar, si organizatat terroriste. | |
| Slajdet 46 deri 49 | Pjesa e Katërt – Konventa e Budapestit për Krimin Kibernetik | |
|  | Konventa e Budapestit për Krimin Kibernetik e Këshillit të Evropës (ETS 185), e njohur gjithashtu si Konventa e Budapestit, u hap për nënshkrim në 23 Nëntor 2001 në Budapest dhe hyri në fuqi në Korrik 2004.  Në Prill 2013, 39 Shtete janë tashmë Palë në Konventën e Budapestit (Shtetet Evropiane, Australia, Republika Dominikane, Japonia dhe SHBA-të), 10 shtete e kishin nënshkruar atë (Evropa, Kanadaja dhe Afrika e Jugut) dhe 8 të tjera janë ftuar të aderojnë (Argjentina, Kili, Kosta Rika, Meksiko, Maroku, Panamaja, Filipinet dhe Senegali). Janë në proces kërkesat për aderim nga vende të tjera.  Shumë të tjerë e kanë përdorur gjithashtu Konventën e Budapestit si guidë për legjislacionin e tyre të brendshëm.  Traktati është i hapur për aderim nga çdo Shtet që është i përgatitur ta zbatojë atë në legjislacionin e brendshëm dhe të angazhohet për bashkëpunim.  Konventa u kërkon Shteteve të bëjnë sa më poshtë:   * Të kriminalizojnë veprat penale kundër sistemeve kompjuterike (aksesi i paligjshëm, kapja e paligjshme e të dhënave, ndërhyrjet në sisteme dhe të dhëna etj.) dhe vepra penale të kryera me anë të sistemeve kompjuterike (të tilla si mashtrimi, veprat penale të pornografisë së të miturve dhe shkeljen e të drejtave të pronësisë intelektuale). E rëndësishme: Traktati është neutral nga ana e teknologjisë dhe mbulon sjelljen kriminale dhe jo teknologjinë apo teknikat (mashtrimin dhe jo phishing, aksesin e paligjshëm dhe jo piraterinë, ndërhyrjen në sistem dhe jo sulmet e përhapura të mohimit të shërbimit etj.) * Të pajisin autoritetet e zbatimit të ligjit me mjete për sigurimin e provave elektronike (kontrolli dhe sekuestrimi, ruajtja e përshpejtuar etj.) E rëndësishme: këto masa zbatohen jo vetëm për krimet kibernetike por edhe ndaj çdo vepre penale që ka të bëjë me provat elektronike në një sistem kompjuterik. * Të angazhohen në bashkëpunim ndërkombëtar efiçent nëpërmjet kombinimit të masave të përkohshme të menjëhershme dhe ndihmës së ndërsjellë zyrtare si dhe pikave të kontaktit 24/7.     Të gjitha këto masa – në veçanti mjetet ligjore procedurale – duhet të përmbushin kriteret e të drejtave të njeriut dhe shtetit të së drejtës. Për këtë arsye, neni 15 (kushtet dhe masat mbrojtëse) janë veçanërisht të rëndësishme.  Në përgjithësi, Konventa e Budapestit i lejon Qeverive të përmbushin detyrimin e tyre pozitiv të mbrojtjes së individëve kundër krimit (kibernetik) dhe në të njëjtën kohë të respektojnë të drejtat e individëve kur ndërmarrin veprime kundër krimit kibernetik.  Deri më sot arritjet janë:   * Procesi i reformave legjislative në mbarë botën * Rritja e masave të drejtësisë penale * Rritja e besimit dhe bashkëpunimit ndërmjet palëve * Përhapja dhe impakti në botë: 56 shtete ratifikuese, nënshkruese, dhe të ftuara për aderim. Bashkëpunim me të paktën 50 shtete të tjera * Katalizator për rritjen e kapaciteteve * Rritja e sigurisë ligjore dhe e besimit nga sektori privat * Një element thelbësor i normave të sjelljes për hapësirën kibernetike * Kontributi për të drejtat e njeriut dhe shtetin e së drejtës në hapësirën kibernetike * Mbrojtja juaj dhe e të drejtave tuaja | |
| Slajdi 51 | Pjesa e Pestë – Disa aktivitete të paligjshme online  Qëllimi i kësaj pjese është përshkrimi i shkurtër i disa prej aktiviteteve të paligjshme që kryhen në rrjete. | |
| Slajdi 52 | “Phishing” (“peshkimi për fjalëkalime”) është një teknikë e përdorur si tentativë për të bindur dikë të dërgojë të dhëna personale tek njerëz të tjerë. Ky informacion mund të përdoret më vonë për kryerjen e vjedhjeve ose mashtrimeve. Zakonisht, keqbërësi përdor mesazhet e postës elektronike për të kandisur viktimat, nga të cilët merr informacionin personal, duke përfshirë fjalëkalime ose të dhëna të tjera të aksesit. Nganjëherë, kjo teknikë përdoret për të çuar përdoruesit tek një uebsajt i rremë ose i dëmshëm. | |
| Slajdi 53 | SPAM-i është një problem shumë i përhapur. Ai konsiston në shpërndarjen e mesazheve të pakërkuara të postës elektronike, të dërguara në miliona kopje. Ata që i marrin këto mesazhe nuk mund ta evitojnë dot këtë gjë. Nganjëherë, mesazhet kanë vetëm qëllime marketingu. Por shpesh ato janë transmetues për programe të dëmshme për infektimin e kompjuterëve.  Zakonisht, dërguesi është dikush që viktima nuk e njeh dhe që të cilit nuk iu kërkua apo nuk iu dha autorizimi të dërgojë mesazhet. | |
| Slajdi 54 | Bashkimi i termave “*malicious*"[[12]](#footnote-13) dhe "*software*”[[13]](#footnote-14) çoi tek “malware”[[14]](#footnote-15), një term që përgjithësisht tregon një program kompjuterik të krijuar me synimin për të aksesuar një sistem kompjuterik pa pëlqimin e pronarit ose përdoruesit, ose me synimin e dëmtimit të tij. Viktima mund ta marrë këtë program të dëmshëm në sistemin kompjuterik pa dijeninë e tij/saj, me anë të skedarëve të bashkëngjitura mesazheve të postës elektronike ose imazheve në këto mesazhe.    Ky program kompjuterik zakonisht është program i dëmshëm dhe futet në kompjuterin e viktimës pa pëlqimin e tij/saj dhe vendoset për të kryer funksione dhe veprime të dëmshme. | |
| Slajdi 55 | Viruset janë një shembull specifik i një programi kompjuterik të dëmshëm. Përgjithësisht, një virus është një program kompjuterik me aftësinë për të riprodhuar veten nga një skedar tek një tjetër dhe për tu vendosur në një sistem të caktuar – një disk të fortë ose një mjet tjetër për mbajtjen e të dhënave. Zakonisht, virusi përhapet kur skedari i infektuar kopjohet apo ekzekutohet. Sigurisht, e gjithë kjo kryhet pa pëlqimin ose madje dijeninë e viktimës dhe me synimin e shkaktimit të dëmit në sistemin kompjuterik. | |
| Slajdi 56 | Një krimb është shumë i ngjashëm me një virus. Si virusi, krimbi është një program kompjuterik me aftësinë për të riprodhuar veten dhe për tu instaluar në një sistem të caktuar dhe për të konsumuar burimet e sistemit. Gjithsesi në ndryshim nga virusi, ai përhapet vetë nëpërmjet një rrjeti kompjuterik dhe nuk i nevojitet t’i bashkëngjitet ndonjë skedari. | |
| Slajdi 57 | Programi “Adware” është gjithashtu një program i dëmshëm. Është një program kompjuterik që automatikisht shfaq ose shkarkon reklama komerciale, pa pëlqimin dhe ndërhyrjen e përdoruesit të kompjuterit. Nganjëherë përhapet i bashkëngjitur me një program tjetër kompjuterik – që është gjithashtu i disponueshëm nëpërmjet shkarkimeve pa pagesë.  Disa lloje të këtyre programeve janë më të rrezikshme, sepse monitorojnë sistemin, si për shembull uebsajtet e vizituara dhe preferencat e përdoruesit të kompjuterit. | |
| Slajdi 58 | Një nga format më ndërhyrëse të programeve kompjuterike të dëmshme është programi “spyware”, ose programi kompjuterik i instaluar në një sistem pa pëlqimin e përdoruesit, me synimin e monitorimit të përdorimit të sistemit nga përdoruesi. Programi kompjuterik “Spyware” mbledh informacion në lidhje me përdoruesin e sistemit kompjuterik. Mbas monitorimit të aktivitetit, programi automatikisht e dërgon informacionin tek palë të treta – objektivi i tij specifik është fshehja në kompjuterin e viktimës dhe raportimi i informacionit të mbledhur tek një palë tretë. | |
| Slajdi 59 | Trojanët (Kuajt Trojanë) është një emër i frymëzuar nga kali i famshëm i ndërtuar nga Odiseu, dhe i ofruar qytetit të Trojës me qëllim hapjen e portave të Trojës nga brenda. Është emri i një programi kompjuterik të dëmshëm që kryen funksione të padëshirueshme për përdoruesin, pa dijeninë e tij. Ky lloj programi mund të shkaktojë shkatërrimin e të dhënave, ç’aktivizon programin e sigurisë së kompjuterit, duke lehtësuar aksesin nga distanca në kompjuterin e sulmuar (për t’i lejuar një personi tjetër akses të paautorizuar në kompjuter) ose për shkarkimin dhe instalimin e programeve të tjera të dëmshme.  Si kali i famshëm i Luftës së Trojës, ky program kompjuterik është dizenjuar që të hapë në mënyrë të fshehte sistemin kompjuterik që të aksesohet nga jashtë. | |
| Slajdi 60 | Termi Botnet është një akronim (*robot networks[[15]](#footnote-16)*) i përdorur për t’i dhënë emër një rrjeti kompjuterësh të infektuar, të quajtura *zombi*, të kontrolluara nga një person ose një organizatë, me synimin e përdorimit për aktivitete të paligjshme.  Një botnet krijohet me anë të infektimit nëpërmjet programeve të dëmshme të dërguara nga pronari i botnet-it. Të gjithë kompjuterët e infektuar kontrollohen nga një program kompjuterik që realizon automatizimin e veprimeve nëpër të gjithë rrjetin kompjuterik. Pronari i rrjetit kontrollon aktivitetin e tij dhe mund ta udhëzojë atë të mbetet joaktiv derisa të jetë e nevojshme.  Një botnet mund të përbëhet nga miliona kompjuterë zombi që janë urdhëruar të dërgojnë mesazhe elektronike të pakërkuara ose programe të dëmshme tek individë të ndryshëm ose të sulmojnë infrastrukturën informatike. Botnet-et shërbejnë për disa qëllime kriminale dhe për këtë arsye quhen gjithashtu “Thikë Zvicerane e Krimit Kibernetik”. | |
| Slajdi 62 | Pjesa e Gjashtë – Përmbledhje | |
| Slajdi 63 | Çfarë është krimi kibernetik dhe pse të preokupohemi për të.  Kërcënimet, tendencat dhe mjetet e krimit kibernetik dhe reagimet ndaj këtij fenomeni.  Realitetet e përfshira në shprehjen *krim kibernetik* dhe konceptet që konsiderohen lloje veprash penale në shumicën e legjislacioneve dhe standardeve ndërkombëtare.  Nevoja dhe avantazhi i harmonizimit ndërmjet legjislacionit të brendshëm dhe instrumenteve ndërkombëtare, në veçanti Konventa e Budapestit. | |
|  | Ushtrime Praktike (sipas rastit)Nuk është parashikuar asnjë ushtrim praktik për këtë sesion specifik sepse nuk ka asnjë garanci se niveli i teknologjisë dhe i aksesit në Internet për dhënien e ushtrimeve të tilla do të jetë i disponueshëm në të gjithë vendet.  Trajnerët në të ardhmen mund të kërkojnë të plotësojnë mësimdhënien duke shtuar ushtrime praktike, kur mësimi të zhvillohet në një mjedis ku pajisjet të jenë të përshtatshme. | |
|  | **Kontrolli i Njohurive**  Nuk është parashikuar asnjë kontroll specifik i njohurive krahas atij të renditur më lart për këtë kurs. Nuk është kërkuar asnjë vlerësim zyrtar. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mësimi 1.1.3, 1.2.2 & 1.2.5 - Teknologjia | | | | **Kohëzgjatja: 330 Minuta** |
| **Burimet materiale të nevojshme:**   * Kompjuter Laptop ose kompjuter tavoline me Windows 7 dhe me Programin Office 2010 * Projektor * Akses në Internet (nëse është i disponueshëm) * Prezantim me programin PowerPoint * Modele të komponentëve fizikë të Kompjuterit (nëse janë të disponueshme) * Klipi i videos me titull “Warriors of the Net” | | | | |
| **Synimi:** Ky sesion jep informacion në lidhje me teknologjinë që do të haset nga gjyqtarët dhe prokurorët gjatë punës së tyre dhe që përdoret nga keqbërësit për kryerjen e krimeve dhe nga autoritetet e zbatimit të ligjit për zbulimin e tyre. Synimi i sesionit është bërja e mundur që audienca të marrë njohuritë e mjaftueshme rreth teknologjisë në mënyrë që ata të kryejnë më me efektivitet rolet e tyre. | | | | |
| **Objektivat:**  Në përfundim të leksionit, pjesëmarrësit do të jenë në gjendje të:   * Shpjegojnë ndikimet e ndryshme që ka teknologjia mbi krimin * Rendisin pjesët përbërëse të një sistemi kompjuterik * Identifikojnë llojet e ndryshme të pajisjeve për mbajtjen e të dhënave * Marrin në konsideratë implikimet e drejtësisë penale për kapacitetin eksponencial të ruajtjes së të dhënave * Identifikojnë sistemet e ndryshme të operimit të kompjuterëve * Shpjegojnë bazat sesi funksionojnë rrjetet * Përshkruajnë funksionet e Internetit * Identifikojnë të paktën 5 programe të mëdha për Internetin * Shpjegojnë sesi është zhvilluar Interneti që nga fillimi deri më sot * Bëjnë dallimin ndërmjet programeve të ndryshme të Internetit * Identifikojnë sesi i përdorin keqbërësit programet e ndryshme të Internetit | | | | |
| **Koha** | **Përmbajtja:** | | | |
| 30 minuta  60 minuta  60 minuta  60 minuta  60 minuta  30 minuta  30 minuta | * Hyrja dhe hapja (Axhenda dhe Objektivat e Sesionit) * Pjesa 1 – Si funksionojnë kompjuterët * Pjesa 2 – Si funksionon Interneti * Pjesa 3 – Shërbimet e Internetit * Pjesa 4 – Programe të tjera të lidhura me Internetit * Pjesa 5 – Krimet në Internet * Pjesa 6 – Përmbledhje | | | |
| **Slajdi nr.** | **Përmbajtja:** | | | |
|  | Hyrje  Teknologjia për Gjyqtarët dhe Prokurorët  Ky sesion ka për synim të pajisë trajnerët me një kornizë për zhvillimin e materialeve të trajnimit që do të zhvillohet si pjesë e një programi më të gjerë. Nuk mund të jetë gjithëpërfshirës sepse teknologjia ndryshon me kaq shpejtësi saqë çdo specifikim i detajuar teknik do të vjetrohej sapo të botohej ky dokument. Garantimi që gjyqtarët dhe prokurorët të kenë kuptuar mjaftueshëm çështjet teknike meqë ato lidhen me çështjet përpara tyre është thelbësore për funksionimin e drejtë të çdo sistemi gjyqësor. Ky sesion ofron një vështrim të përgjithshëm të aspekteve përkatëse të teknologjisë dhe lidhjen e tyre me sistemin e drejtësisë penale. Është përgatitur dhe një Prezantim me Power Point si burim që të përdoret nga trajnerët nëse konsiderohet i përshtatshëm.  Një burim shtesë në formën e një klipi video me titull “Warriors of the Net” është dhënë për t’i pajisur pjesëmarrësit me kuptimin e qartë sesi funksionojnë rrjetet. Video është e disponueshme në adresën www.warriorsofthe.net në gjuhët e mëposhtme: në gjuhën angleze, gjermane, frënge, hebraike, holandeze, suedeze, italiane, portugeze, daneze, norvegjeze, hungareze, çeke, spanjolle dhe gjuhën ukrainase.  Ky sesion jep informacion në lidhje me teknologjinë që do të hasin gjyqtarët dhe prokurorët gjatë punës së tyre, e cila përdoret nga keqbërësit për kryerjen e veprave penale dhe nga autoritetet e zbatimit të ligjit për zbulimin e këtyre veprave. | | | |
|  | Prezantimi me PowerPoint  Është përgatitur një prezantim me PowerPoint me shënime për trajnerët për të plotësuar këtë plan leksioni dhe për ta pajisur trajnerin me shembuj sesi të zhvillojë materialet e tij/saj për përmbushjen e objektivave të mësimit. Është e rëndësishme të mbahet mend se është përgjegjësia e trajnerit për të zhvilluar materiale mësimore që janë të kohës dhe që lidhen me audiencën dhe jo thjesht të mbështetet tek materiali që është përgatitur nga një trajner tjetër. | | | |
| Slajdet 2 dhe 3 | Axhenda  Slajdet e axhendës rendisin pjesët e sesionit dhe trajneri duhet t’i kalojë një për një duke dhënë shpjegimet sa herë është e nevojshme për aspekte specifike që kanë rëndësi për pjesëmarrës të caktuar. Trajneri duhet të shpjegojë sesi do të zhvillohen materialet dhe që do të ketë seanca të caktuara për pyetjet dhe ndërveprimin. Trajneri duhet të theksojë se ky trajnim është dizenjuar që të jetë interaktiv dhe se pjesëmarrësit pritet që të jenë aktivë gjatë gjithë trajnimit. Trajneri duhet të shpjegojë nëse ka një vlerësim dhe çfarë forme ka ai, duke përfshirë detaje për ndonjë notë kalimi që mund të zbatohet. (Për këtë program pilot nuk është përfshirë asnjë vlerësim). | | | |
| Slajdi 4 | Objektivat e Sesionit  Është e rëndësishme që pjesëmarrësit të kuptojnë se cilat janë objektivat e leksionit. Këto duhet të jenë objektiva “SMART” dhe të shpjeguara në detaje për pjesëmarrësit përpara se të fillojë sesioni, duke përdorur informacionin në slajd. | | | |
| Slajdet 5 deri 54 | Pjesa e Parë – Si funksionojnë kompjuterët  Në përfundim të sesionit, pjesëmarrësit do të jenë në gjendje të:   * Rendisin pjesët përbërëse të një sistemi kompjuterik * Identifikojnë llojet e ndryshme të pajisjeve për mbajtjen e të dhënave * Marrin në konsideratë implikimet e drejtësisë penale për kapacitetin eksponencial të ruajtjes së të dhënave * Identifikojnë sistemet e ndryshme operative të kompjuterit | | | |
| Slajdi 5 | Me qëllim që Gjyqtarët dhe Prokurorët të kuptojnë plotësisht impaktin e teknologjisë mbi krimin, është e domosdoshme që ata të përfitojnë një kuptim të informacionit bazë sesi funksionon teknologjia që iu paraqitet. Në veçanti, në çështjet që kanë të bëjnë me kriminalistikën dixhitale në kuptimin e gjerë të saj, kjo njohuri do të japë kontekstin dhe do t’iu mundësojë të marrin vendime të informuara. Ky sesion do të ofrojë njohuri bazë për kompjuterët, komponentët e tyre, mbajtjen e të dhënave dhe impaktin e sasive të mëdha të të dhënave që mbahen në pajisje individuale. Edhe njëherë trajneri duhet të përpiqet që ta bëjë këtë sesion sa më interaktiv që të jetë e mundur dhe të përdorë informacionin e dhënë për të inkurajuar pjesëmarrësit të marrin në konsideratë ndikimin e rolit të teknologjisë dhe çështjet sesi mund të menaxhohen sasi të mëdha të dhënash dhe të futen me efektivitet në sistemin e drejtësisë penale.  Nëse do të jetë e mundur, trajneri duhet të marrë modele të komponentëve fizikë të kompjuterit që i përmend në këtë sesion, me qëllim që ato t’ua tregojë pjesëmarrësve dhe ata t’i shohin nga afër.  Ka dhe komponentë të tjerë fizikë të kompjuterit që nuk janë trajtuar në këtë sesion; megjithatë janë përfshirë komponentët më të rëndësishëm për qëllimet e kursit. Për zhvillimin e programeve të trajnimit, rekomandohet që të shpjegohen komponentët fizikë të kompjuterit që nuk janë përfshirë këtu, në varësi të njohurive të individëve. Pritet që shumica e pjesëmarrësve të trajnimit ta kuptojnë se çfarë është një tastierë apo një maus, megjithatë trajnerët nuk duhet të mbivlerësojnë njohuritë e individëve. Pajisjet që mund të përfshihen në listën më lart mund të jenë: printera, skanera, kamera internet, modeme, altoparlantë për kompjuter, telefona video dhe ata kompjuterik, dhe pajisje të ndryshme për mbajtjen e të dhënave dhe pajisjet lidhëse të rrjetit si dhe portat e jashtme të tilla si portat Firewire dhe portat USB.    Konkretisht, për më shumë informacion në lidhje me komponentët fizikë të kompjuterëve vizitoni adresën http://computer.howstuffworks.com/computer- hardware-channel.htm; duke përfshirë foto, të cilat e lehtësojnë shumë të kuptuarin e këtyre koncepteve. Mos harroni të merrni leje nga pronarët e të dhënave nëse ato propozohen të përfshihen në programet e trajnimit. | | | |
| Slajdi 6 | Qëllimi i këtij slajdi është të tregojë se edhe individët që kanë njohuri të mëdha për teknologjinë nuk mund të parashikonin ndryshimet që do të sillte ajo. Pjesëmarrësit nuk janë të vetmit nëse nuk e kuptojnë impaktin që ka teknologjia në rolet e tyre dhe thëniet në këtë slajd mund t’i inkurajojnë ata të besojnë se teknologjia në sistemin e drejtësisë penale nuk duhet të merret me frikë por të asimilohet me të gjitha masat mbrojtëse ekzistuese. | | | |
| Slajdi 7 | Trajneri duhet të bëjë një shpjegim të shkurtër të zhvillimit të kompjuterëve nga kompjuterët e vetëm, tek terminalet kompjuterike, deri tek bota e rrjeteve kompjuterike, si hyrje në fillimin e shpjegimit të komponentëve të kompjuterëve. | | | |
| Slajdi 8 | Komponentët e Kompjuterit  Trajneri duhet të shpjegojë se një kompjuter përbëhet nga shumë komponentë dhe është e nevojshme që gjyqtarët dhe prokurorët të kuptojnë emrat dhe funksionet e këtyre komponentëve sepse do t’iu referohen në deklaratat e tyre dhe tek provat.  Një shpjegim i shkurtër për secilin komponent jepet si më poshtë: | | | |
| Slajdet 9 dhe 10 | * “Motherboard” – Pllaka mëmë njihet gjithashtu dhe si kuadri kryesor ose kuadri i sistemit të kompjuterit. Pllaka mëmë është kuadri me qark të stampuar i një kompjuteri. Të gjithë komponentët e tjerë dhe pjesët periferike vendosen në foletë e tij. Puna e pllakës mëmë është transmetimi i informacionit ndërmjet të gjithë komponentëve të tij. Kuadri mëmë strehon BIOS-in (Sistemin Bazë Input/Output), i cili është një program i thjeshtë kompjuterik, i vënë në funksionim nga kompjuteri që sapo ndizet. Komponentët e tjerë janë direkt të bashkëngjitur me të, të tilla si memorja, CPU (Procesori), karta grafike, karta e zërit, njësia e diskut të fortë, njësitë e disqeve, së bashku me porta të jashtme dhe pjesë periferike të tjera. * “Expansion slots” – mbrapa kompjuterit ka disa të çara/kanale tek të cilat mund të lidhen kartat e zërit, kartat e videos, përshtatësit pa kabëll, etj. | | | |
| Slajdet 11 deri 13 | * CMOS dhe BIOS - CMOS dhe BIOS shpesh përdoren në mënyrë të shkëmbyeshme; BIOS-in mund ta mendoni si një program kompjuterik, dhe CMOS-in si komponentin fizik që e vë atë në funksionim. I formuar nga germat e para të fjalëve “Complementary Metal Oxide Semiconductor”[[16]](#footnote-17), CMOS zakonisht shqiptohet "si-mos". CMOS-i është komponenti fizik në një kompjuter që kryen funksione të një niveli shumë të ulët dhe realizon procedurën bazë të fillimit të funksionimit të kompjuterit. CMOS-i realizon funksione të tilla si: mban në funksionim orën e kompjuterit dhe siguron ndërfaqen për pjesën tjetër të komponentëve fizikë të kompjuterit në mënyrë që BIOS-i të kryejë punën e tij. Ai kërkon shumë pak energji që të funksionojë. I formuar nga germat e para të shprehjes “Basic Input / Output System”[[17]](#footnote-18), zakonisht shqiptohet "baj-os". BIOS-i është një ndërfaqe që i lejon një përdoruesi të bëjë ndryshime të nivelit të ulët në kuadrin mëmë, tek procesori, memorja dhe pajisje të tjera të një kompjuteri. Parametrat automatik të paracaktuar të BIOS-it zakonisht janë vendosur drejtë. Një nga ndryshimet më të zakonshme të bëra në BIOS gjatë kryerjes së kriminalistikës dixhitale është ndryshimi i rendit sipas të cilit kompjuteri kërkon pajisjet për t’i vënë në funksionim. Zakonisht një hetues mund të përdorë një program kompjuterik në një Kompakt Disk (CD) dhe do ta ndryshonte BIOS-in në mënyrë të tillë që kompjuteri të fillonte funksionimin nga CD-ja dhe jo nga disku i ngurtë sepse kjo do të ndryshonte të dhënat vetëm duke hyrë dhe duke filluar funksionimin e sistemit nga njësia e diskut të ngurtë. | | | |
| Slajdi 14 | * Furnizimi me Energji – Njësia e Furnizimit me Energji Elektrike (PSU) në një kompjuter rregullon dhe ushqen me energji elektrike komponentët e vendosur në kasën e kompjuterit. Furnizimi standard me energji elektrike konverton rrymën hyrëse 110V ose 220V AC (rrymë alternative) në rrymë DC (rrymë të drejtpërdrejtë) të përshtatshme për furnizimin me energji të komponentëve të kompjuterit. Furnizimi me energji ka një output të caktuar të specifikuar në Vat, dhe një furnizim standard me energji elektrike zakonisht është në gjendje të japë rreth 350 Vat. Sa më shumë komponentë të ketë një kompjuter, aq më e madhe energjia elektrike e kërkuar nga njësia e furnizimit me energji. | | | |
| Slajdi 15 | * Njësia Qendrore e Përpunimit të të Dhënave/Procesori (CPU) - CPU do të thotë “Central Processing Unit”[[18]](#footnote-19) i një sistemi kompjuterik. Njerëzit shpesh e marrin kasën e një kompjuteri gabimisht për procesorin. Megjithatë, procesori është komponent i brendshëm i kompjuterit. Ai nuk mund të shihet nga jashtë sistemit. Procesorët e parë u përdorën në fillim të viteve 1960. Me hyrjen e qarqeve të integruar në fund të viteve 1970, u bë e mundur që të prodhoheshin procesorë më të vegjël. Kjo ndihmoi në transformimin e kompjuterëve nga pajisje të mëdha kaba që zinin salla të tëra në modele kompjuterësh më të menaxhueshëm, si kompjuterë tavoline apo kompjuterë laptop. Pavarësisht nga lloji i kompjuterit, procesori funksionon me anë të ekzekutimit të një serie komandash të ruajtura, dhe të njohura me emrin program. Shumica e procesorëve i janë përshtatur arkitekturës së von Neumann-it, që thotë se Procesori duhet të marrë, deshifrojë, ekzekutojë dhe shkruajë mbrapsht të dhënat në seri mjaft të shpejtë. Për amatorët Procesori nuk është asgjë tjetër përveçse truri i kompjuterit, d.m.th ajo që realizon kompjuteri faktikisht kryhet me ndihmën e procesorit. | | | |
| Slajdi 16 | * Random Access Memory – Memorja e kompjuterit është teknikisht çdo formë e mbajtjes së të dhënave elektronike, megjithëse më së shumti përdoret për përshkrimin e formave të përkohshme të mbajtjes së të dhënave që mund të aksesohen shpejt. Do të ishte një proces shumë i ngadaltë nëse Procesori duhet të merrte të dhëna nga disku i ngurtë çdo herë që do të ekzekutonte një komandë. Memorja e kompjuterit teknikisht është çdo formë e mbajtjes së të dhënave elektronike, megjithatë përgjithësisht përdoret për të përshkruar formën e përkohshme të mbajtjes së të dhënave që mund të aksesohen në mënyrë të shpejtë. Do të ishte një proces shumë i ngadaltë sikur Procesorit t’i duhej të merrte të dhëna nga disku i ngurtë sa herë që do t’i duhej të ekzekutonte një komandë; kaq pak të dhëna ruhen në memorien e përkohshme në mënyrë që të mund të aksesohen në mënyrë me të shpejtë. Kjo lloj memorje njihet si Random Access Memory (RAM). Procesori i kërkon të dhëna memories RAM, i përpunon ato dhe ia shkruan mbrapsht memories RAM. Kjo ndodh me miliona herë në sekondë. Të kuptuarit e memories së përkohshme është e rëndësishme në marrjen e të dhënave nga kompjuterët gjatë hetimeve sepse këto të dhëna nuk janë të ruajtura dhe humbasin nëse ndërpritet furnizimi me energji elektrike i kompjuterit, meqë kjo është një karakteristikë e njohur e kontrollit dhe sekuestrimit të sistemeve kompjuterike. Aktualisht është më e zakonshme për punonjësit e zbatimit të ligjit të përpiqen të kapin të dhënat në memorien RAM përpara ndërprerjes së rrymës gjatë kontrollit të kompjuterëve. Kjo zakonisht njihet si “Live Data Forensics”[[19]](#footnote-20). Ky aktivitet po ndodh gjithnjë e më shpesh sepse sasia të dhënave që mund të humbasin është më e madhe sesa madhësia e njësisë së diskut të ngurtë më të madh vetëm pak vite më parë. | | | |
| Slajdi 17 | * Universal Serial Bus (USB) – Ndërlidhësit USB të gjendur në shumë kompjuterë mundësojnë lidhjen e thjeshtë të një numri të madh pajisjesh me kompjuterin si p.sh. mauset, printerat, pajisjet e jashtme të mbajtjes së të dhënave dhe telefonat celularë. Aktualisht është metoda më e zakonshme e lidhjes së pajisjeve të jashtme me kompjuterët. Historikisht, metodat e tjera të lidhjes, të tilla si lidhjet me porta paralele ose në seri ishin më problematike sepse numri i pajisjeve që mund të lidheshin njëherazi ishte i kufizuar, dhe shpejtësia e transferimit të të dhënave ishte shumë më e ngadaltë sesa me USB. Është e mundur të lidhen deri në 127 pajisje me një kompjuter me anë të përdorimit të USB-ve. Lehtësia me të cilën mund të përdoren USB-të do të thotë se ato dominojnë në shumë hetime të kriminalistikës dixhitale. | | | |
| Slajdet 18 deri 20 | * Hard Disk Drives[[20]](#footnote-21) – Shumica e kompjuterëve kanë të paktën një disk të ngurtë dhe shumë të tjerë kanë më shumë. Kompjuterët më të mëdhenj si p.sh. terminalet kanë zakonisht shumë disqe të ngurtë. Tani është e zakonshme për pajisje të tjera si p.sh. CCTV-të dhe pajisjet për luajtjen e muzikës të kenë gjithashtu disqe të ngurta, të cilat mund të mbajnë sasi shumë të mëdha të dhënash. Këto disqe kanë pllakëza të forta në të cilat mbahet informacion dhe mund të fshihen dhe rishkruhen lehtësisht të dhënat, ndërkohë që struktura e diskut ruhet, duke e bërë atë të vlefshme për periudha të gjata kohe. Të dhënat ruhen në sipërfaqen e diskut në sektorë dhe vija rrethore. Vijat janë rrathë koncentrikë, dhe sektorët janë në formë V-je në një vijë rrethore. Të dhënat ruhen në disqet e ngurtë si skedarë, të cilët janë thjesht një grup me “bytes”[[21]](#footnote-22). Programet janë gjithashtu skedarë dhe këto komandohen nga Procesori që të futen në përdorim. | | | |
| Slajdi 21 | * Solid State Storage[[22]](#footnote-23) – Një Njësi në Gjendje të Ngurtë (SSD), nganjëherë e quajtur edhe disk elektronik ose disk në gjendje të ngurtë, është një pajisje për mbajtjen e të dhënave që përdor memorien në gjendje të ngurtë për ruajtjen e të dhënave të qëndrueshme me synimin e dhënies së aksesit në të njëjtën mënyrë si një njësi e zakonshme e diskut të ngurtë input/output. Disqet SSD dallohen nga disqet e zakonshme magnetike si p.sh. njësitë e disqeve të ngurta (HDDs) ose disketat, se këto të fundit janë pajisje elektromekanike që përmbajnë disqe rrotullues dhe koka të lëvizshme për leximin/shkrimin e të dhënave. Në dallim nga ato, disqet SSD përdorin mikroçipe që ruajnë të dhëna në çipe të memories jo të paqëndrueshme[1] dhe nuk përmbajnë pjesë të lëvizshme.[1] Krahasuar me disqet e ngurta elektromekanike, disqet SSD zakonisht janë më pak të ndjeshme ndaj goditjeve fizike, janë pa zhurmë, kanë gjendje latente dhe kohë aksesi më të pakët, por janë më të shtrenjta për gigabajt (GB). Disqet SSD përdorin të njëjtën ndërfaqe si njësitë e disqeve të ngurta, duke i zëvendësuar ato në shumicën e programeve. | | | |
| Slajdi 22 | * Kompakt Disqet/DVD-të/Disqet Blu-Ray – Këto disqe mund të mbajnë sasi të ndryshme të dhënash dhe zakonisht përdoren për të mbajtur muzikë, video ose skedarë për shpërndarje. Një DVD, për shembull, është me madhësi të njëjtë sa një Kompakt Disk dhe mban rreth 7 herë më shumë të dhëna sesa një Kompakt Disk. Një disk Blu-Ray, i cili mund të përdoret për të mbajtur përmbajtje me definicion të lartë mban më shumë sesa 10 herë sasinë që mban një DVD. Me fjalë të tjera, ato mund të mbajnë më shumë të dhëna sesa ishte e mundur të mbante një disk i ngurtë vetëm pak vite më parë. Ata të gjithë i mbajnë të dhënat në një mënyrë të ndryshme nga disqet e ngurtë dhe të dhënat e mbajtura në to nuk janë po aq të paqëndrueshme sa të dhënat e ruajtura në disqet e ngurtë. | | | |
| Slajdi 23 | Ruajtja e të Dhënave  Është praktikë e përditshme që provat që rrjedhin nga kompjuterët ose nga pajisjet dixhitale, si p.sh. telefonat celularë, të paraqiten në procedimet civile ose penale. Ndërsa teknologjia vazhdon të pushtojë shoqërinë, do të bëhet normë që gjithnjë e më shumë pajisje të përmbajnë prova elektronike që mund të përdoren në procedimet gjyqësore. Tashmë jemi dëshmitarë që pajisje shtëpiake janë pjesë e hetimit për të nxjerrë prova të tilla.    Për rrjedhim është thelbësore që Gjyqtarët dhe Prokurorët të kuptojnë çështjet që kanë impakt në integritetin dhe pranueshmërinë e provave dixhitale. Si pikë fillestare, do të ishte e dobishme që gjyqtarët dhe prokurorët të vlerësonin sesi ruhen të dhënat dhe sesi merren nga hetuesit.    Të dhënat dixhitale ose elektronike ruhen në shumë forma, nga të cilat më mbizotëruesja dhe në shumë mënyra më e lehta për tu vlerësuar është ruajtja e të dhënave në njësitë e diskut të ngurtë në kompjuterë. Metodat e zakonshme për ruajtjen dhe prodhimin e provave dixhitale mbështeten tek ekzaminimi i pajisjeve në gjendje statike. Me fjalë të tjera kur një kompjuter është i fikur dhe të dhënat nuk janë në një gjendje realisht të paqëndrueshme. Hetuesit e kriminalistikës dixhitale janë të përgatitur mirë në kriteret e udhëzimeve kombëtare dhe ndërkombëtare në lidhje me administrimin e provave të tilla. Një guidë e tillë e titulluar “Sekuestrimi i Provave Elektronike” u zhvillua me mbështetjen financiare nga Programi Oisin i Komisionit Evropian dhe mund të gjendet në adresën: <http://www.e-evidence.info>. Kjo guidë promovon parimet e përgjithshme, në bazë të të cilave funksionon shumica e punës së autoriteteve të zbatimit të ligjit. Është e rëndësishme që Gjyqtarët të kenë një kuptim të qartë të mënyrës sesi ruhen të dhënat si dhe sesi sillen provat e paraqitura përpara tyre. Kjo kërkon një kuptim themelor të koncepteve të të dhënave dixhitale, ruajtjes, nxjerrjes së të dhënave dhe mjeteve dhe procedurave të përdorura për sjelljen e provave në sistemin e drejtësisë penale. Ekzistojnë burime të shumta të hapura që zhvilluesit e trajnimeve të mbledhin informacion në lidhje me ruajtjen e të dhënave në disqet e ngurtë që t’i përdorin më pas në programet e trajnimit. Një shembull i tillë mund të gjendet në adresën: <http://www.storagereview.com/hard_disk_drive_reference_guide>. Kjo zakonisht ka të bëjë me ruajtje të dhënash jo të paqëndrueshme të tilla si njësi magnetike, mjete optike të mbajtjes së të dhënave, memorie flash etj.    Tani është më e zakonshme për provat që të përftohen nga burime të paqëndrueshme të tilla si Memoria RAM ose pajisje të tilla si telefonat celularë ku të dhënat janë më të paqëndrueshme. Gjyqtarët duhet të kuptojnë ndryshimet në mënyrën sesi merren të dhëna të tilla dhe çdo efekt mbi integritetin e provave. Rëndësia e mbledhjes së të dhënave të paqëndrueshme është thjesht që ato zakonisht humbasin kur një pajisje fiket dhe mundësia për të rikuperuar sasitë e mëdha të informacionit që mund të jenë të vlefshme është humbur. Teknikat e përdorura për të rikuperuar këtë informacion duhet të jenë në përputhje me parimet e përgjithshme për ruajtjen dhe rikuperimin e të dhënave të tilla. Është gjithashtu e zakonshme që të dhënat e paqëndrueshme të rikuperohen nga sistemet e rrjeteve kompjuterike që nuk mund të fiken për bërjen e një analizë statike. | | | |
| Slajdi 24 | Memorja dhe ruajtja e të dhënave – ky slajd jep një paraqitje të termave të përdorura për përshkrimin e të dhënave dhe madhësisë së tyre dhe është një prezantim që do të jetë i nevojshëm që pjesëmarrësit të kuptojnë pjesën e mëvonshme të sesionit që trajton pajisjet e ndryshme të ruajtjes së të dhënave dhe kapacitetet e tyre. | | | |
| Slajdi 25 | Sistemet e Operimit  Me qëllim që të funksionojnë, kompjuterët dhe pajisjet e tjera dixhitale kërkojnë një sistem operimi. Sistemi i operimit është një program kompjuterik që i lejon komponentëve fizikë të kompjuterit të komunikojnë me programet kompjuterike. Pa një sistem operimi kompjuteri nuk do të ishte në gjendje të funksiononte. Ekzistojnë lloje të ndryshme të sistemeve të operimit në varësi të llojit të kompjuterit ose të pajisjeve të tjera dixhitale.    Sistemet më të zakonshme të operimit në përdorim në ditët e sotme njihen zakonisht me emrat e mëposhtëm: Windows, Unix/Linux dhe Apple Mac. Ekzistojnë sisteme të tjera në përdorim veçanërisht për lloje të tjera pajisjesh të tilla si ndihmësit dixhital dhe telefonat celularë. Këto shpesh janë versione të reduktuara të sistemeve të mëdha, megjithëse aktualisht është më e zakonshme që të zhvillohen sisteme me porosi për pajisje më të vogla.  Shumica e programeve të zhvilluara për kompjuterët shkruhen për sisteme specifike operimi, megjithëse është e zakonshme që ato të jenë të disponueshme për më shumë sesa një platformë.  Është e rëndësishme që Gjyqtarët dhe Prokurorët të vlerësojnë rëndësinë e sistemeve të operimit dhe të jenë të njohur me faktin se sistemet e operimit sillen në mënyra të ndryshme. Ekzistojnë shumë referenca që i mundësojnë një zhvilluesi të një trajnimi që ai/ajo të përfshijë informacion të mjaftueshëm në lidhje me sistemet e operimit për të përmbushur objektivat e përcaktuara në këtë sesion. Ndërmjet këtyre burimeve është dhe: <http://en.wikipedia.org/wiki/Operating_systems> | | | |
| Slajdet 26 deri28 | Sistemet e Operimit – këto slajde japin një shpjegim të qëllimit të sistemeve të operimit, identifikojnë sistemet më të zakonshme në përdorim sot, dhe ofrojnë informacion statistikor për mbizotërimin në përdorimin e këtyre sistemeve. Trajnerët duhet të jenë të ndërgjegjshëm se duhet ta mbajnë informacionin të azhurnuar, në veçanti informacioni për slajdin 38 duhet të azhurnohet një herë në vit. | | | |
| Slajdi 29 | Pajisjet Dixhitale  Sesioni për pajisjet dixhitale është dizenjuar të garantojë që gjyqtarët dhe prokurorët të jenë në gjendje të identifikojnë llojet e ndryshme të pajisjeve që potencialisht mund të përmbajnë prova. Kjo çon në diskutimin e mëvonshëm sesa shumë të dhëna mund të mbajnë pajisjet dhe trajtimi i disa prej sfidave që sasitë e të dhënave sjellin përpara sistemit të drejtësisë penale. | | | |
| Slajdet 30 deri 38 | Slajdet që janë përfshirë në këtë sesion janë shumë të zgjeruara dhe trajneri duhet të marrë në konsideratë se sa prej tyre janë të nevojshme për objektivin.  Megjithatë sesioni nuk trajton ndryshimet ndërmjet pajisjeve të tilla si celularë, USB në formë gishti, ose kompjuterët, përsa i takon sfidave që ato krijojnë për kontrollin, sekuestrimin dhe ekzaminimin e provave nga këto pajisje. Trajnerët duhet të marrin parasysh që të përdorin shembujt për mbështetjen e objektivave të tyre të trajnimit.  Në këtë fazë të kursit, pjesëmarrësit do të jenë njohur me aspektet teknike të shumta dhe konsiderohet se disa prej slajdeve do t’iu japin atyre një perspektivë që nuk është shumë e vështirë për tu kuptuar dhe sjell disa shembuj interesantë në vëmendjen e tyre.  Pikat e rëndësishme për tu trajtuar këtu janë natyra e ndryshme e pajisjeve, në të cilat ruhen të dhënat dhe shkalla e sfidave që këto sjellin përpara sistemit të drejtësisë penale. Trajnerët duhet të marrin në konsideratë përdorimin e shembujve kur pajisje të pazakonta kanë përbërë burime thelbësore të provave në çështjet penale. | | | |
| Slajdi 39 | Disa Kompjuterë të Ndryshëm  Ky sesion i shkurtër pason menjëherë atë më lart dhe është një zgjerim i diskutimit për pajisjet dixhitale. Edhe njëherë, trajneri mund të përdorë sa më shumë ose sa më pak slajde që nevojiten për të transmetuar mesazhin tek pjesëmarrësit se provat mund të gjenden në një sërë pajisjesh dhe se jo të gjitha pajisjet që hasen janë ato që duken.    Një karakteristikë e rëndësishme e sesionit është lehtësia e aksesit të pajisjeve që mund të përmbajnë me mijëra faqe dokumentesh që mund të përbëjnë prova. | | | |
| Slajdet 40 deri 45 | Pikat e rëndësishme për tu trajtuar këtu janë natyra e ndryshme e pajisjeve tek të cilat mund të ruhen të dhënat dhe niveli i sfidave që këto pajisje sjellin përpara sistemit të drejtësisë penale. Trajnerët duhet të marrin në konsideratë përdorimin e shembujve kur pajisje të pazakonta kanë përbërë burime thelbësore të provave në çështjet penale. | | | |
| Slajdet 46 deri 54 | Sa të dhëna mund të mbajnë pajisjet dixhitale  Ky është një sesion i rëndësishëm që përkthen informacionin teknik që është dhënë në lidhje me pajisjet dixhitale, në realitetin e sasisë së informacionit që pajisjet mund të mbajnë dhe se çfarë do të thotë kjo në drejtim të sasisë së dokumentacionit që mund të prodhohet. Është prezantimi në diskutimet e mëvonshme që do të zhvillohet në lidhje me integritetin dhe pranueshmërinë e provave dixhitale dhe produkteve të tyre.  Fotografia e përshkruar është që të pajisë pjesëmarrësit me një standard përcaktues nga i cili të kuptohet sasia e të dhënave që mund të mbajnë pajisjet e ndryshme dixhitale. Trajnerët inkurajohen të përdorin shembuj të tjerë që mund të kenë më shumë lidhje me vendin e tyre.  Një pikë tjetër e rëndësishme për t’u përçuar është fakti se këto pajisje nuk janë më të shtrenjta dhe sasi shumë të mëdha të dhënash mund të mbahen në pajisje të ndryshme.  Trajnerët duhet gjithashtu të theksojnë sfidat nëse gjyqtarët dhe prokurorët marrin vendime që në efekt e bëjnë pothuaj të pamundur administrimin efektiv të sasive shumë të mëdha të të dhënave ose materialeve të shtypura. | | | |
| Slajdet 55 deri 81 | Pjesa e Dytë – Si funksionon Interneti  Në përfundim të sesionit pjesëmarrësit do të jenë në gjendje të:   * Shpjegojnë sesi është zhvilluar Interneti që nga fillimi deri më sot. * Përshkruajnë funksionet e Internetit * Bëjnë dallimin ndërmjet programeve të ndryshme të Internetit * Identifikojnë të paktën 5 programe të mëdha të Internetit * Identifikojnë sesi mund t’i përdorin keqbërësit programet e ndryshme të Internetit. | | | |
| Slajdi 55 | Ky sesion ofron informacion bazë në lidhje me historinë, funksionimin dhe shërbimet e disponueshme në Internet si dhe ofron informacion që i lejon pjesëmarrësve të bëjnë dallimin dhe të përcaktojnë qartësisht komponentët e Internetit dhe të kuptojnë sesi ndikon ai tek sistemi i drejtësisë penale. Trajnerët duhet të garantojnë që të jepen shembuj praktikë për të shtuar vlerë tek të dhënat teknike të ofruara në prezantim. | | | |
| Slajdet 56 deri 57 | Termi INTERNET vjen nga shkurtimi i fjalëve “INTERconnected NETwork”[[23]](#footnote-24). Shumë aktivitete kriminale përfshijnë përdorimin e Internetit dhe kjo përfshin lloje specifike të veprave penale të tilla si hyrja e paautorizuar në sistemin kompjuterik, përhapja e viruseve dhe sulmet për marrjen e të dhënave personale, si dhe vepra penale më tradicionale si p.sh. mashtrimet. Me qëllim që Gjyqtarët të menaxhojnë me efektivitet çështje të tilla që iu dalin përpara, është e domosdoshme për ta që të asimilojnë njohuritë bazë të Internetit dhe programeve të tij të tilla si Rrjeti Mbarë Botëror dhe posta elektronike. Më poshtë jepet një prezantim i kësaj teme dhe ofrohet një model për një modul të suksesshëm trajnimi. | | | |
| Slajdet 58 dhe 59 | Historia e Internetit  Interneti e filloi jetën e tij si ARPANET në vitet 1960. Lidhja e këtij informacioni mund të mos jetë menjëherë e qartë; megjithatë fakti se Interneti nuk u dizenjua asnjëherë të ishte i sigurtë mund të shpjegojë se pse është e lehtë për kriminelët të abuzojnë me sistemet. Lidhjet e para fizike u krijuan në vitin 1969 me 4 nyje lidhjeje që ishin universitetet. Mesazhi i parë elektronik u dërgua në vitin 1972 dhe në vitin pasues u krijua një protokoll i ri i komunikimit, i cili tani përbën bazën në të cilën zhvillohen komunikimet. Zhvillimi i Internetit, si e njohim ne, ishte i pakët në fillim sepse ekzistonin rrjete të veçuara dhe të shkëputura, të shërbyera vetëm nga rrugë kalimi të kufizuara ndërmjet tyre. Kjo çoi drejt aplikimit të shkëmbimit të grupeve të të dhënave në rrjet për zhvillimin e një protokolli për ndërlidhjen në rrjet, ku rrjete të shumta të ndryshme mund të bashkohen së bashku në një super-kornizë me rrjete.  Kjo mundësoi ndërlidhjen e mëtejshme, e cila filloi të ndodhte më shpesh në rrjetet e përparuara të botës perëndimore dhe më pas filloi të hynte në pjesën tjetër të botës. Pabarazia e zhvillimit ndërmjet kombeve të zhvilluar dhe botës në zhvillim çoi drejt një ndarjeje dixhitale që akoma dhe sot ekziston.  Më pas vijoi komercializimi i Internetit dhe futja e Kompanive Shërbimofruese private të Internetit në vitet 1980. Këto të fundit mundësuan një akses edhe më të madh, i cili u zhvillua në të vërtetë në vitet 1990. Interneti ka një impakt shumë të madh në tregti si dhe në kulturë. Tani ekzistojnë komunikimet pothuaj të menjëhershme me postë elektronike (e-mail), rrjetet sociale, forumet e diskutimit me shkrim, dhe Rrjeti Mbarë Botëror. Interneti vazhdon të zhvillohet, i nxitur nga tregtia, sasitë e mëdha të njohurive dhe informacionit online. Jemi në prag të mbërritjes së Web 2.0. | | | |
| Slajdi 60 | Trajneri duhet të sigurohet që pjesëmarrësve t’u jepet informacioni që do t’iu mundësojë atyre të kuptojnë bazat e rrjeteve dhe kufizimet e tyre. Ato duhet të jenë në gjendje të bëjnë dallimin ndërmjet rrjeteve lokale dhe rrjeteve më të gjera. Këto slajde e japin këtë informacion bazë. Trajnerët duhet të marrin në konsideratë dhënien e shembujve dhe inkurajimin e pjesëmarrësve për të diskutuar për llojet e ndryshme të rrjeteve dhe sesi është zhvilluar Interneti. Në këtë fazë duhet të jepet një shpjegim i disa termave përkatëse për rrjetet, të tilla si Portat dhe Bandwidth[[24]](#footnote-25). Pjesëmarrësit duhet të inkurajohen të marrin në konsideratë përvojat e tyre personale; për shembull nëpërmjet aksesit të tyre në Internet në shtëpi ose në punë. | | | |
| Slajdi 61 | Local Area Network (LAN) – është një rrjet kompjuterik që mbulon një zonë të vogël gjeografike, të tillë si një shtëpi, zyrë, ose grup ndërtesash, p.sh. një shkollë. Karakteristikat përcaktuese të LAN-eve përfshijnë shpejtësinë e tyre shumë më të madhe të transferimit të të dhënave, shtrirje të vogël gjeografike, dhe pa pasur nevojën për qiramarrjen e linjave të telekomit.    Wide Area Network (WAN) – është një rrjet kompjuterik që mbulon një zonë të gjerë (d.m.th., çdo rrjet, lidhjet e komunikimit të të cilit kalojnë nëpër kufij metropolitan, rajonal apo kombëtarë). Ose më pak zyrtarisht, një rrjet që përdor routers[[25]](#footnote-26) dhe lidhje publike komunikimi.  Ndryshojnë nga personal area networks[[26]](#footnote-27) (PANs), campus area networks[[27]](#footnote-28) (CANs), or metropolitan area networks[[28]](#footnote-29) (MANs), të cilat zakonisht janë të kufizuara respektivisht tek një dhomë, ndërtesë, kampus universiteti ose zonë specifike metropolitane (p.sh., në një qytet). Shembulli më i madh dhe më i njohur i një WAN-i është INTERNET-i. | | | |
| Slajdi 62 | Ports – janë një pikë fundore ose “kanal" për komunikimet në rrjet. Numrat e Portave lejojnë që programe të ndryshme në të njëjtin kompjuter që përdorin burimet e rrjetit pa ndërhyrë tek njëri tjetri. Portat janë ‘virtuale’ – JO priza ku futet spina!  Bandwidth[[29]](#footnote-30) – është sasia e informacionit që mund të transportohet nëpërmjet një linje telefoni, linje me kabull, transmetim satelitor, dhe të tjera. Sa më e madhe të jetë gjerësia e valës, aq më e madhe shpejtësia e lidhjes dhe po aq shumë eksperienca jote me Internetin i afrohet shkarkimit të menjëhershëm të të dhënave, apo një përvoje si me një Televizor. | | | |
| Slajdi 63 | Network Interface Controller[[30]](#footnote-31) (NIC) – është një qark ose një kartë e instaluar në një kompjuter që i mundëson kompjuterit të lidhet me një rrjet.  Adresa e Media Access Control[[31]](#footnote-32) (MAC) – është një identifikues gati-unik i caktuar për shumicën e përshtatësve ose kartave të rrjetit (NICs) nga prodhuesi për identifikim, dhe që i cili jep një vlerë unike.  Network Hub – ose përqendrues është një pajisje për lidhjen e pajisjeve të Eternetit me fibra optike ose çifte të ndërlidhura së bashku, duke i kthyer ato në një segment të vetëm të rrjetit. Hub-et funksionojnë në shtresën fizike (shtresën 1) të modelit OSI, dhe termi “layer 1 switch” shpesh përdoret në mënyrë të shkëmbyeshme me termin “hub”. Pajisja është një lloj repetitori me shumë porta. Network hubs janë gjithashtu përgjegjëse për kalimin e një sinjali bllokimi tek të gjitha portat nëse diktohet një përplasje trafiku të dhënash. | | | |
| Slajdi 64 | Network Switch[[32]](#footnote-33) – është një pajisje për rrjetin kompjuterik që lidh segmentet e rrjetit. Në të kaluarën, ishte më e shpejtë të përdoreshin teknikat e quajtura “Layer 2” për këtë pajisje, kur vetëm adresat MAC mund të shiheshin tek content addressable memory[[33]](#footnote-34) (CAM). Me ardhjen e memories (TCAM), ishte po aq e shpejtë të kërkoje një adresë IP ose një adresë MAC.  Router[[34]](#footnote-35) – është një pajisje që përcakton pikën e radhës së rrjetit tek e cila duhet të përcillet një paketë të dhënash në drejtim të destinacionit të saj. Ajo duhet të lidhet me të paktën 2 rrjete. Ajo është inteligjente dhe funksionon me tabela. Është e vendosur tek porta e hyrjes së rrjetit. Termi “layer 3 switch” shpesh përdoret në mënyrë të shkëmbyeshme me termin “router”, por një “switch” në fakt është një term i përgjithshëm pa një përkufizim rigoroz.  Server – është një kompjuter ose një pajisje që jep informacion ose shërbime për kompjuterët e tjerë në një rrjet. Me programin kompjuterik të duhur, çdo kompjuter i lidhur në rrjet mund të konfigurohet si server. Në shumicën e rasteve, serveri është një kompjuter i fuqishëm, i krijuar të jetë “gjithnjë i disponueshëm”. Një kompjuter mund të verë në funksionim disa shërbime – p.sh. server uebi, server për postën elektronike, server për skedarët, server për printerët etj. Në mjedisin e biznesit është normale të ofrohen disa shërbime në makina të ndryshme për arsye të sigurisë dhe për të minimizuar impaktin e ndonjë avarie. | | | |
| Slajdet 65 dhe 66 | **Bazat e Internetit**  Interneti mund të mendohet si infrastruktura në të cilën mund të funksionojnë programe të ndryshme në të njëjtën kohë. Nëse ndonjë pjesë e Internetit funksionon keq ose prishet, komunikimi prapëseprapë mund të vazhdojë. Askush nuk e ka në pronësi Internetin – asnjë organizatë, asnjë korporatë, asnjë qeveri. Ai është i vetërregullueshëm përgjithësisht. Përdor të njëjtën teknologji për lidhje.  Shumica e rrjeteve moderne të të dhënave, si Interneti, përshkruhen si “connectionless”[[35]](#footnote-36) or “packet switched”[[36]](#footnote-37). Trafiku është i ndarë në paketa të vogla të dhënash, të cilat kalojnë nga dërguesi tek marrësi. Ato nuk ndjekin të gjitha të njëjtën rrugë dhe bashkohen bashkë përsëri kur mbërrijnë në destinacion. | | | |
| Slajdet 67 dhe 68 | Trajnerët duhet të japin shpjegime të qarta në lidhje me programet e ndryshme që funksionojnë në Internet, me shembuj të qartë sesi duhet të paraqiten ato. Duhet të merret në konsideratë demonstrimi i shembujve për secilin prej programeve krahas përshkrimit të dhënë në këtë slajd.  Ka mjaft Protokolle Interneti, nga të cilat më i rëndësishmi është the Internet Protocol[[37]](#footnote-38) (IP). Secili kompjuter i lidhur me Internetin DUHET ta përdorë atë. Një adresë IP është “numri i telefonit” tënd në Internet dhe pa një Adresë IP, ti nuk do të jesh në gjendje të përdorësh Internetin. Programe dhe shërbime të ndryshme përdorin protokolle të ndryshme për komunikimin ndërmjet rrjeteve, disa prej tyre janë: HTTP – HyperText Transfer Protocol[[38]](#footnote-39); SMTP – Simple Mail Transfer Protocol[[39]](#footnote-40); FTP – File Transfer Protocol[[40]](#footnote-41); NNTP – Network News Transfer Protocol[[41]](#footnote-42). *Shprehja e përdorur këtu është: run “over” IP[[42]](#footnote-43) (jo në vend të).* | | | |
| Slajdet 69 dhe 70 | Shumica e njerëzve lidhen me Internetin nëpërmjet një Internet Service Provider[[43]](#footnote-44) (ISP). Këto janë organizata komerciale që marrin me qira hapësirën kibernetike. Ato mbajnë të dhëna...por përsa kohë? Ka çështje kombëtare dhe ndërkombëtare të jetës private dhe mbrojtjes së të dhënave ligjore që mund të ndikojnë faktin sesa duhet të ruhen të dhënat nga ISP-të. Sigurisht kjo ka një impakt mbi aftësinë e autoriteteve të drejtësisë penale për të siguruar provat nga këto burime. Lidhja zakonisht bëhet me një nga metodat e mëposhtme: Dial-up[[44]](#footnote-45), Broadband (ADSL)[[45]](#footnote-46), ISDN[[46]](#footnote-47), me kabëll, Wireless[[47]](#footnote-48) ose me lidhje satelitore.  Duhet të jepet informacion sesi realizohen lidhjet në Internet dhe të inkurajohen pjesëmarrësit që të diskutojnë eksperiencat e tyre. Duhet të shpjegohet se ISP-të mbajnë të dhëna por legjislacioni i mbrojtjes së të dhënave i kufizon kohën sesa gjatë duhet t’i mbajnë të dhënat.  Duhet të shpjegohet roli i ISP-së, me statusin ligjor dhe numrat. Kjo është një mundësi e mirë për të diskutuar rëndësinë e marrëdhënies me ISP-të në lidhje me aksesimin e të dhënave dhe kryerjen e interceptimit të ligjshëm të të dhënave.  Terminologjia e thjeshtë është se ISP-të e japin me qira aksesin në Internet tek njerëzit – pavarësisht nëse ata janë individë ose organizata.  Secila ISP mban njëfarë informacioni për klientët e saj. Detajet dhe sasia e të dhënave varet nga ISP-ja, dhe do të zgjasë për aq kohë – ditë ose orë në varësi të nevojës.  Duhet të jetë e mundur të merret informacioni: Emri, adresa dhe informacion tjetër i përdorur për regjistrim Data e regjistrimit dhe sesi u regjistrua personi Adresat specifike të postës elektronike ose emrat e përdoruesit që janë unike për përdoruesin Detajet financiare si p.sh. kartat e kreditit të përdorura për tu regjistruar me Kompaninë Shërbimofruese të Internetit Mundësisht ndonjë detaj nga ndonjë program kompjuterik për përdoruesin Më e rëndësishmja, detaje të historisë së aktivitetit të përdoruesit online – data, koha dhe kohëzgjatja  KOHA ËSHTË THELBËSORE (Çështjet e zonave kohore trajtohen më vonë në këtë sesion). Duhet të dalë në pah se është e mundur të përdoren detaje të rreme për regjistrimin e një llogarie.  A mundet një ISP të interceptojë trafikun e Internetit – PO – por varet nga pajisjet e posaçme për regjistrimin e përdorimit dhe monitorojë se çfarë ndodh – kështu që i nevojiten burime njerëzore për këtë – kosto? Gjithashtu, duhet të marrin në konsideratë autoritetin e nevojitur për të vepruar kështu. Sidoqoftë, është e nevojshme të kontaktohet kompania shërbimofruese e Internetit shumë herë në një hetim.  Network Address Translation[[48]](#footnote-49) – është një teknikë ku burimi dhe/ose adresa IP e destinacionit rishkruhet sepse kalon nëpërmjet një firewall[[49]](#footnote-50) ose router[[50]](#footnote-51). Më zakonisht gjendet i përdorur për hostimin e shumëfishtë në një rrjet privat për aksesimin e Internetit me një adresë të vetme IP.  Rekomandohet që çdo kurs trajnimi të përfshijë një shpjegim të adresimit në rrjet në detaje dhe në veçanti të përfshijë: faktin se në versionin 4 të IP-së, adresat janë në 4 grupe me nga 3 shifra (adresë 32 bit), ku secili grup varion nga 0 deri 255, që nënkupton një maksimum prej 256 zgjedhjesh. Secili grup quhet Oktet (28) dhe disa vlera janë të rezervuara. Duhet të jepet një shpjegim me detaje sesi dalin adresat e IP. Kjo mund të arrihet më mirë me anë të një prezantimi vizual të numrave Binarë nga të cilët rrjedhin ato. Duhet të jepet një shpjegim i mëtejshëm i ndryshimit ndërmjet adresave dinamike dhe statike IP dhe efektin që mund të ketë mbi hetimet. Duhet të jepet shpjegim i ndryshimeve në Versionin 6 të IP dhe nevojën për të ndryshuar versionin duke qenë se Internetit po i mbarojnë adresat IP. | | | |
| Slajdet 71 dhe 72 | Shkalla e përdorimit të Internetit në të gjithë botën është një karakteristikë e rëndësishme. Dy Slajdet e dhëna këtu demonstrojnë, së pari, dy metoda të ndryshme të prezantimit të informacionit dhe së dyti, infiltrimin e gjuhëve të ndryshme në përdorimin e Internetit dhe ndryshimet e bëra gjatë një periudhe mjaft të shkurtër. Si me informacionin tjetër që lidhet me kohën, trajneri do të duhet të garantojë që informacioni të jetë sa më shumë i azhurnuar dhe të deklarohen burimet . | | | |
| Slajdi 73 | Interneti – Si funksionon  Ky sesion është hartuar të lejojë pjesëmarrësit të kuptojnë se si qarkullojnë të dhënat në Internet. Informacioni është shumë bazë sic kërkohet për këtë audiencë të caktuar. | | | |
| Slajdi 74 | Në rastin e një IP-je, paketat e të dhënave janë me madhësi të ndryshme. Çdo dy paketa nuk kanë nevojë të marrin të njëjtën rrugë nga burimi në destinacion. Kompjuteri marrës e rigrumbullon trafikun e të dhënave dhe nëse mungon ndonjë paketë të dhënash ai kërkon ridërgimin e saj.  Avantazhi është se rrjeti është një burim i ndarë ndërmjet njerëzish dhe mund të alokohet në mënyrë dinamike në varësi të nevojave të asaj kohe. Disavantazhi është se bëhet e vështirë të garantohet cilësia e shërbimit sepse nuk ka një lidhje të dedikuar. Kjo është objekt trajtimi në ditët e sotme dhe disa shërbime voice over IP[[51]](#footnote-52) ofrojnë një cilësi të shkëlqyer të zërit. | | | |
| Slajdet 75 dhe 76 | Dy ilustrimet në këto slajde jepen që t’i mundësojnë trajnerit të shpjegojë se si qarkullon trafiku në Internet. | | | |
| Slajdi 77 | Një burim i shkëlqyer për shpjegimin e Internetit është një film i titulluar “Warriors of the Net”[[52]](#footnote-53). Është mjeti perfekt për prezantimin e Internetit për përdoruesit e rinj. Filmi është 12 minuta i gjatë. Flet për udhëtimin e paketave IP nëpërmjet ruterave të rrjetit, firewall-eve dhe kabllove transatlantike. Filmi është i disponueshëm për shkarkim pa pagesë për qëllime jo-komerciale në adresën www.warriorsofthe.net dhe është aktualisht i disponueshëm (Janar 2012) në gjuhët e mëposhtme: Anglisht, Gjermanisht, Spanjisht, në gjuhën izraelite, Hollandisht, Suedisht, Frëngjisht, Italisht, Portugalisht, Danisht, Norvegjisht, Hungarisht, dhe Çekisht. Një burim tjetër i dobishëm për përcaktimin e nivelit të hyrjes dhe zhvillimit të Internetit në vende dhe rajone mund të gjendet në adresën http://www.internetworldstats.com/. Rekomandohet që të jepet brenda trajnimit një element i informacionit statistikor për të garantuar që pjesëmarrësit të jenë në gjendje të vlerësojnë impaktin e Internetit në vendin e tyre. | | | |
| Slajdi 78 | Është e rëndësishme që pjesëmarrësit të kuptojnë Adresat IP dhe kufizimet e IPv4[[53]](#footnote-54). Kjo do t’i ndihmojë ata kur diskutimi i mëvonshëm të zhvillohet në lidhje me Adresat IP dinamike dhe statike. Ky informacion i thjeshtë çon në seksionin tjetër për të ardhmen e Internetit. | | | |
| Slajdi 79 | Shumica e ISP-ve kanë më pak adresa IP sesa klientët – duke u mbështetur në faktin se jo të gjitha do të lidhen në të njëjtën kohë. Caktimi i adresave dinamike IP përdoret për riciklimin e adresave.  Meqenëse adresa e njëjtë IP ka shumë të ngjarë të përdoret nga njerëz të ndryshëm në të njëjtën ditë, koha dhe data (dhe zona kohore) janë të rëndësishme kur bëhet kontrolli i ISP-ve për të dyshuar.  ISP-të do të ofrojnë adresa IP statike (të cilat sigurisht janë kërkesa që vijnë nga një uebsajt) – por me një kosto më të lartë | | | |
| Slajdet 80 dhe 81 | E ardhmja e Internetit është një banket, megjithatë mbërritja e IPv6[[54]](#footnote-55) do të sjellë shumë ndryshime në mënyrën tonë të jetesës dhe gjithashtu në sistemin e drejtësisë penale. Trajneri duhet të shpjegojë sesi IPv6 do t’i mundësojë pothuaj çdo pajisjeje të ketë adresën e saj të IP-së dhe kjo do të ketë impakte në mënyrën që do të kryhen hetimet në të ardhmen.  Duhet të jepen shembuj sesi po ndryshon Interneti dhe impakti që do të kenë këto ndryshime në mënyrën sesi kryhen dhe menaxhohen hetimet që i interesojnë një audience të caktuar. Në shembuj jepen efektet në gjerësinë e valës, tregtinë dhe shërbimet pa kabull. | | | |
| Slajdet 83 deri 111 | Pjesa e Tretë – Shërbimet e Internetit | | | |
| Slajdi 83 | Ky sesion shpjegon më në detaje shërbimet që janë të disponueshme në Internet, në veçanti Rrjetin Mbarë Botëror dhe Postën Elektronike. | | | |
| Slajdi 84 | Përpara se të japim në detaje shërbimet e disponueshme në Internet, është me vlerë të reflektohet se sa vende tani mbështeten në këto shërbime në nivel kombëtar. Trajnerët duhet të japin një vështrim të përgjithshëm për infrastrukturën kritike kombëtare në vendet e tyre për të garantuar që pjesëmarrësit të kuptojnë se sa i rëndësishëm është bërë Interneti në çështjet e sigurisë së infrastrukturës kombëtare brenda një kohe të shkurtër. | | | |
| Slajdi 85 | **Rrjeti Mbarë Botëror (WWW)**  Rrjeti Mbarë Botëror (WWW) lindi efektivisht në vitin 1991 kur u shpik nga Sir Tim Berners-Lee HTML – Hyper Text Markup Language[[55]](#footnote-56). HTML shërbeu si platforma për kombinimin e fjalëve, fotove dhe tingujve në faqet e rrjetit. Standardet e rrjetit u krijuan nga Konsorciumi i Rrjetit Mbarë Botëror (W3C). Pjesa pasuese jep një farë shpjegimi të këtij emri. “Këndvështrimi i W3 për botën përbëhet prej dokumentesh që i referohen njëri tjetrit me anë të linkeve. Për shkak të ngjashmërisë me punën e një merimange, kjo botë quhet Rrjetë.” *(Tim Berners-Lee, Robert Cailliau; Rrjeti Mbarë Botëror; Shtator 1992.* | | | |
| Slajdet 86 dhe 87 | Aksesi në Rrjetin Mbarë Botëror zakonisht arrihet nëpërmjet përdorimit të një Browser[[56]](#footnote-57), i cili është një program kompjuterik i krijuar për gjetjen dhe shfaqjen e faqeve të rrjetit. Programet më të zakonshme që nga Janari 2012 janë: Mozilla Firefox, Google Chrome, Internet Explorer, Safari dhe Opera. Trajnerët duhet të garantojnë që të gjitha statistikat si këto të dhëna këtu të azhurnohen me intervale të rregullta. | | | |
| Slajdet 88 dhe 89 | Hyper-Text Transfer Protocol (HTTP) është gjuha e përbashkët që Programet e Navigimit në Internet dhe Serverët e Rrjetit përdorin për të komunikuar me njëri tjetrin në Internet.  Megjithëse programet e navigimit në rrjet mbështesin një shumëllojshmëri protokollesh, p.sh., FTP, NNTP, SMTP, etj., HTTP-ja është protokolli i përdorur më shpesh në kombinim me programet e navigimit të Rrjetit. HTTP-ja është një protokoll i thjesht kërkesë/përgjigje (RR) nëpërmjet TCP[[57]](#footnote-58).  Shumë njerëz në mënyrë të gabuar mendojnë se Rrjeti Mbarë Botëror është në fakt Interneti dhe kjo ndodh për shkak sepse Rrjeti Mbarë Botëror është aplikacioni i përdorur nga shumë njerëz. Është e zakonshme që kriminelët ta shfrytëzojnë këtë përdorim.  Në zhvillimin e një programi trajnimi, duhet të merret në konsideratë përfshirja e shembujve të aktivitetit kriminal në Rrjetin Mbarë Botëror, aty ku lidhen me juridiksionin e vendit ku zhvillohet trajnimi. | | | |
| Slajdi 90 | Emrat e Domeneve dhe Adresimi IP  Ky seksion është krijuar t’i japë pjesëmarrësve kuptimin bazë të adresave IP dhe se çfarë duan të thonë ato, pa hyrë në shumë detaje se si adresat IP dhe emrat e domeneve lidhen me njëri tjetrin. Detajet teknike merren në konsideratë përtej fushës së objektivave të këtij kursi. Është e rëndësishme që trajneri ta bëjë këtë aspekt sa më të lehtë që të jetë e mundur. Materiali prezantues i ofruar kërkon të identifikojë se si mund të arrihet kjo. | | | |
| Slajdet 91 deri 93 | Ka tre pika kryesore që duhet të jepen në këtë seksion:   1. Së pari, një shpjegim për një Uniform resource locator[[58]](#footnote-59) (URL) dhe se si është strukturuar ai; 2. Një shpjegim i adresave IP dhe adresave statike – Adresat IP Statike janë të caktuara në mënyrë permanente dhe janë efektivisht gjithmonë online.   Adresat IP dinamike caktohen sa herë që hyhet online, megjithatë sapo del jashtë, adresa IP mund të ricaktohet.  Është për këtë arsye që koha e saktë e hyrjes në Internet është e rëndësishme.   1. Një shpjegim i marrëdhënies ndërmjet një adrese IP dhe një URL-je. – Emrat e domeneve dhe adresat IP janë të shkëmbyeshme, nëse e di adresën IP duhet të jesh në gjendje të hysh në linjën e adresës dhe të lidhesh me të njëjtën faqe interneti.   Në praktikë ajo që ndodh zakonisht është se ti hyn në një emër domeni [www.open.gov.uk](http://www.open.gov.uk) dhe serveri brenda sistemit të Internetit e përkthen për ty dhe të dërgon në faqen e saktë të Internetit.  Në Adresat e Protokollit të Internetit, emri i domenit konvertohet në një numër unik 32 bit, zakonisht të shkruar në një *Dotted Quad notation*[[59]](#footnote-60), një seri prej katër numrash 8 bit të shkruar me shifra dhjetore dhe të ndara me pika. Si më lart 212.140.189.10, të gjitha numrat në këtë sekuencë duhet të variojnë ndërmjet shifrave 0 dhe 255 (në fakt janë 256 alternativa). Sigurisht në shembullin e dhënë numri i fundit duhet të lexohet 010, megjithatë, zakonisht lejohet që ai të shkurtohet në numrin 10. | | | |
| Slajdi 94 | Gjurmët  Një aspekt i rëndësishëm i trajtimit të krimit kibernetik është të kuptuarit se çfarë gjurmësh mund të lihen nga hetuesit gjatë përdorimit të Internetit për kryerjen e hetimeve. Kjo ka lidhje jo vetëm me hetuesin por gjithashtu edhe me prokurorin që mund të urdhërojë kryerjen e hetimeve dhe për gjyqtarin nga këndvështrimi i pranueshmërisë së provave. Ky seksion duhet të kërkojë të japë njohuritë bazë që do t’i lejojnë pjesëmarrësve të kuptojnë rreziqet që hyrja online mund t’i sjellë hetimit. | | | |
| Slajdet 95 deri 98 | Informacioni i dhënë në slajdet e prezantimit jep të dhëna bazë që duhet t’i jepen pjesëmarrësve, për të treguar se çfarë informacioni lihet pas nga kushdo, duke përfshirë edhe hetuesit kur vizitojnë uebsajtet. Kjo duhet të lidhet me rëndësinë e garantimit që hetuesit të mbrojnë identitetin e tyre në këto rrethana dhe identifikimin se në disa juridiksione, mund të ketë kushte ligjore për tu përmbushur me qëllim që të kryhen hetime të tilla. | | | |
| Slajdet 101 deri 104 | Posta Elektronike  Posta Elektronike ose Email-i është një metodë e shkëmbimit të mesazheve dixhitale.  Për përdoruesin duket sikur Mesazhi Elektronik kalon direkt nga makina e dërguesit tek ajo e marrësit; megjithatë secili mesazh zakonisht kalon të paktën nëpërmjet katër kompjuterëve.   1. Një mesazh krijohet në kompjuterin e përdoruesit/dërguesit, më pas dërgohet në serverin SMTP[[60]](#footnote-61) të dërgimit të postës elektronike të Kompanisë Shërbimofruese të Internetit. 2. Kompania dërguese e përcjell mesazhin elektronik tek serveri SMTP i Kompanisë ISP të marrësit (SMTP – SMTP). 3. Serveri i postës elektronike të Marrësit e gjen serverin e marrjes së postës (Post Office Protocol ose POP3) dhe dërgon mesazhin në “kutinë e postës së marrësit”. 4. Marrësi futet në llogarinë e tij dhe mesazhi tërhiqet në kutinë e postës së marrësit, zakonisht duke e fshirë atë nga serveri i postës gjatë këtij procesi.   *\* Mail server[[61]](#footnote-62) – kompjuter i dedikuar për përdorimin e postës elektronike* | | | |
| Slajdi 105 | Ekzistojnë lloje të ndryshme të postës elektronike; E-mail – Posta e zakonshme me programin “Outlook” – dërguar nëpërmjet SMTP-së – tërhequr nëpërmjet POP3 dhe sapo shkarkohet vendoset në kompjuterin tënd.    Posta në Rrjet **–** Posta POP3; për shembull duke përdorur programin “Outlook Express” – kur futesh në program zakonisht shkarkon të gjitha mesazhet e reja në kutinë tënde postare të vendosur në kompjuterin tënd; posta IMAP[[62]](#footnote-63) – Posta në Internet – që mund të kontrollohet nga kompjuteri juaj por është e vendosur në një server të largët – mund të organizohet në foldera, etj. por mund të kontrollohet vetëm kur jeni online. | | | |
| Slajdet 106 deri 109 | Kokat e Email-it  Shpesh është më e lehtë të krahasosh mesazhin elektronik me një letër kur e shpjegon. Mesazhet Elektronike kanë pjesën që quhet koka (zarfi), dhe pjesën e trupit (vetë letra) me skedarë bashkëngjitur. Koka e mesazhit është fokusi kryesor i hetuesve sepse përmban informacion për dërguesin, marrësin, adresat IP, serverët e postës elektronike, regjistrimi i kohës etj. Ky informacion përdoret për të ndihmuar gjurmimin e dërguesit të një mesazhi kur nuk është menjëherë i dukshëm, për shembull në rastin e një kërkese për shpërblesë të dërguar nëpërmjet postës elektronike. Koka e plotë ose e zgjeruar është e rëndësishme për gjurmimin e burimit të një mesazhi dhe është e rëndësishme që Gjyqtarët të njohin ndryshimin ndërmjet kokës që shihet kur dërgohet një mesazh dhe kokës së zgjeruar që përmban të gjithë informacionin përkatës. Posta elektronike është një nga aplikacionet më të zakonshme që do të haset nga Gjyqtarët, dhe hartuesit e trajnimit duhet të sigurohen që të përfshijnë informacionin më të fundit për llojet e ndryshme të postës elektronike dhe se si merren në mënyrë korrekte provat nga mesazhet elektronike si dhe Kompanitë Shërbimofruese të Internetit nëpërmjet të cilave kalon mesazhi elektronik. Informacion shtesë në lidhje me funksionimin e postës elektronike që mund të shfrytëzohet nga hartuesit e trajnimit mund të gjendet në adresën: http://www.learnthenet.com/english/html/20how.htm | | | |
| Slajdet 112 deri 159 | Pjesa e Katërt – Programe të tjera përkatëse të Internetit  Ky seksion i kursit është hartuar t’iu japë pjesëmarrësve një vështrim të përgjithshëm për programet në Internet që nuk janë përfshirë në seksionet e mëparshme. Këto janë të nevojshme sepse do të hasen gjatë zhvillimit normal të aktiviteteve me audiencën e synuar. Ky informacion do të mbështesë objektivat e kursit. Niveli i detajeve të dhëna konsiderohet i përshtatshëm për nivelin e mësimdhënies që kërkohet. Duhet të tregohet kujdes nga trajnerët që të mos japin shumë njohuri të detajuara sepse ato do të përfshihen në kursin e avancuar që po hartohet. | | | |
| Slajdet 113 dhe 114 | Ruajtja e të dhënave Online  Cloud Computing[[63]](#footnote-64)  Cloud computing është një term marketingu për teknologjitë që bëjnë llogaritje, programe kompjuterike, akses tek të dhënat, dhe shërbimet e ruajtjes së të dhënave që nuk kërkojnë njohuri nga përdoruesi për vendndodhjen fizike dhe konfigurimin e sistemit që i ofron shërbimet. Një paralelizëm mund të bëhet me rrjetin elektrik, ku konsumatorët konsumojnë energji pa iu dashur të kuptojnë pajisjet përbërëse ose infrastrukturën e kërkuar për ofrimin e shërbimit/energjisë. Shërbimi Cloud computing ofron një suplement të ri, konsumin, dhe modelin e ofrimit të shërbimeve të Teknologjisë së Informacionit bazuar në protokollet e Internetit, dhe zakonisht ka të bëjë me sigurimin e burimeve të virtualizuara dhe të shkallëzuara nga ana dinamike. Është një produkt i gatshëm dhe pasojë e lehtësimit të aksesit në uebsajtet në Internet që ofrojnë “remote computing[[64]](#footnote-65)”. Kjo mund të marrë formën e mjeteve të vendosura në Rrjet ose programeve që përdoruesit mund të aksesojnë dhe përdorin nëpërmjet një programi për navigimin në Internet njësoj sikur programet të ishin instaluar në kompjuterin e tyre. Ofruesit e shërbimeve të hostuara në Internet vënë në dispozicion të përdoruesve programe nëpërmjet Internetit, të cilat aksesohen nga programi navigues i Internetit dhe programet e kompjuterit apo të telefonit celular, ndërkohë që të dhënat dhe programi janë të vendosura në një server në një vendndodhje të largët. Në disa raste, programet e vjetra ofrohen nëpërmjet një teknologjie që i bën të përbashkëta për të gjithë, ndërsa burimet e shërbimeve janë të konsoliduara në një vendndodhje të largët të të dhënave; në raste të tjera, të gjitha programet janë koduar duke përdorur teknologjitë e Rrjetit, të tilla si AJX. Në themel të “cloud computing” është koncepti më i gjerë i konvergjencës midis infrastrukturës dhe shërbimeve të përbashkëta. Ky lloj mjedisi qendror për të dhënat i lejon ndërmarrjeve të vënë në funksionim shpejt programet e tyre, me menaxhim të lehtë dhe me pak mirëmbajtje. Ajo i mundëson teknologjisë së informacionit t’i përshtatë më shpejt burimet e saj (si p.sh. serverët, ruajtjen e të dhënave dhe lidhjen në rrjet) për të përballuar kërkesën e paparashikueshme dhe të paqëndrueshme të biznesit. Shumica e infrastrukturës për “cloud computing” përbëhet nga shërbime të ofruara nëpërmjet qendrash të të dhënave, të cilat duken si pika të vetme aksesi për nevojat e konsumatorëve për shërbime. Mund të nevojiten oferta tregtare për përballimin e marrëveshjeve të shërbimit por kushtet specifike po negociohen gjithnjë e më pak nga kompanitë e vogla. Impakti i madh i “cloud computing” tek biznesi ka nxitur qeverinë federale Amerikane ta shikojë “renë” si mjet për riorganizimin e infrastrukturës së saj të teknologjisë së informacionit dhe të reduktojë buxhetet e saj për IT-në. (Burimi [www.wikipedia.com](http://www.wikipedia.com))  Çështjet që lidhen me identifikimin dhe grumbullimin e të dhënave nga “reja” dhe implikimet ligjore të veprimeve të tilla trajtohen kudo në këtë kurs. | | | |
| Slajdet 115 deri 116 | Informacioni mund të jepet nga trajneri në lidhje me mbizotërimin e ruajtjes online të të dhënave dhe si shembull numri i kërkimeve në faqen Google dhe rritja për një periudhë të caktuar kohe, jep një ide në lidhje me interesin që ekziston për një ruajtje të tillë të dhënash. Informacioni duhet të jepet në lidhje me llojet e ndryshme të ruajtjes së të dhënave online në ndryshim nga shërbimet me pagesë dhe pa pagesë. Duhet të bëhet i qartë fakti se keqbërësit mund ta përdorin këtë lloj ruajtjeje. | | | |
| Slajdet 117 dhe 118 | Duhet të jetë me interes për pjesëmarrësit të dinë mënyrat sesi mund t’i përdorin keqbërësit shërbimet në Internet. Një përdorim i tillë është me anë të një “dead letter box”[[65]](#footnote-66). Kjo mund të shpjegohet nga trajneri sepse është shumë e lehtë për tu kuptuar se si kjo metodë komunikimi mund të përdoret me shumë pak rrezik për tu kapur. | | | |
| Slajdet 119 dhe 120 | Peer to Peer (P2P)[[66]](#footnote-67)  Shërbimet “Peer to Peer” kanë lejuar për shumë vite transferimin e skedarëve të paligjshëm si dhe skedarëve që janë subjekt i të drejtave të pronësisë intelektuale. Programet “Peer to peer” kanë qenë popullore ndër grupet kriminale të përfshira në këto aktivitete. Gjenerata e parë e strukturës “peer-to-peer” ka funksionuar me parimin e përdorimit të një serveri qendror, me të cilin lidheshin njerëzit me qëllimin për të shkarkuar skedarë. Kjo e bënte identifikimin e atyre që ofronin shërbime të paligjshme shumë të lehtë për tu gjetur dhe për tu mbyllur. Gjenerata e dytë e programeve “peer to peer” përdorin metoda të ndryshme për tu lidhur: që nga ato që mbajnë lista të skedarëve të disponueshëm për tu gjetur më lehtësisht deri tek ato që veprojnë si supernyje që identifikojnë se ku janë të disponueshme këto skedarë.  Gjyqtarët do të duhet të jenë të ndërgjegjshëm për këtë aktivitet “peer to peer” sepse mund të ketë lidhje me shumë lloje gjykimeve penale dhe civile. Nuk është e nevojshme pasja e njohurive të thella dhe hartuesit e trajnimit duhet të marrin në konsideratë uebsajte të tilla si http://ezinearticles.com/?How-Peer-to-Peer-(P2P)-Works&id=60126 për të dhënë një informacion më të azhornuar. | | | |
| Slajdet 121 dhe 122 | Newsgroups[[67]](#footnote-68)  Termi “Newsgroup” është në njëfarë mënyre ç’orientues sepse priret të shkaktojë diskutime. Ato janë teknikisht të ndryshëm por funksionojnë në një mënyrë të ngjashme me forumet e diskutimit të hostuara në Internet. Serverët për Newsgroups mbahen nga organizata të ndryshme, të cilat bien dakord me të tjerët që të sinkronizojnë informacionin e tyre rregullisht. Kjo i lejon përdoruesve të postojnë mesazhe në një server dhe të shihen nga një audiencë shumë e gjerë. | | | |
| Slajdet 123 dhe 124 | File Transfer Protocol[[68]](#footnote-69) (FTP)  FTP-ja është një protokoll i fuqishëm që lejon transferimin e skedarëve nga një kompjuter tek një tjetër. Ajo funksionon në një server me një program FTP të instaluar në atë server, i cili i lejon përdoruesit të ndërveprojë me serverin me qëllimin për të pasur akses tek shërbimet dhe informacioni në atë server. Kur një përdorues dëshiron të transferojë një skedar, krijohet një lidhje TCP[[69]](#footnote-70) me sistemin e synuar të destinacionit. Emri identifikues dhe fjalëkalimi lejohen të transmetohen dhe përdoruesit i lejohet të specifikojë skedarët dhe veprimin e dëshiruar. Kur miratimi merret për transferimin e skedarit, një tjetër lidhje TCP krijohet në mënyrë që të transferohen të dhënat. Pse duhet Gjyqtarët ta dinë ekzistencën e shërbimeve FTP? Përgjigjja është se ata mund të hasin përdorimin e skedarëve të tillë në çështjet kur kriminelët mund të shkëmbejnë materiale me njëri tjetrin ose kur lidhja me FTP përdoret si metoda e transferimit nga protokolle të tjera si Internet relay Chat (IRC). | | | |
| Slajdet 125 dhe 126 | Internet Relay Chat[[70]](#footnote-71) (IRC)  Internet Relay Chat (IRC) është në të vërtetë një sistem telekonference që është pak i vjetër por prapëseprapë i përdorur nga keqbërësit për të komunikuar dhe shkëmbyer skedarët. Funksionon nëpërmjet një serie serverësh të lidhur me njëri tjetrin dhe që ndajnë mesazhe që postohen në “kanale”, të cilat janë dhoma virtuale të shkëmbimit të mesazheve me shkrim. Temat e diskutimit janë të renditura dhe përdoruesit që kanë një program IRC mund të lidhen me një apo më shumë kanale dhe të futen në diskutime me njerëz të interesuar për të njëjtën tematikë diskutimi. IRC-ja nuk është shërbimi më i lehtë për tu përdorur në Internet dhe më së shumti përdoret nga ata që janë më me eksperiencë dhe përdorues më të vjetër. Është një protokoll i përdorur nga keqbërësit dhe shumë pak njohuri kërkohet nga Gjyqtarët dhe Prokurorët për funksionimin e tij. | | | |
| Slajdet 127 deri 132 | Instant Messaging (IM) dhe Social Networking  Mesazhet Direkte dhe Rrjetet Sociale kanë marrë kryesimin si mjetet e zgjedhura të komunikimit vitet e fundit me shumë shembuj të mirënjohur të ofrimit të aksesit të menjëhershëm dhe shumë të lehtë për të gjithë përdoruesit në të gjithë botën. Karakteristika kryesore e këtyre uebsajteve është aftësia për të krijuar një profil personal dhe ndarja e të dhënave personale dhe njohja me njerëz të rinj. Është e mundur të ndash me të tjerët foto, muzikë dhe video. Sasia e informacionit e postuar nga individët mund t’i bëjë ata objektiv për keqbërës për shembull përfshirja në vjedhjen e identitetit apo joshja e fëmijëve për veprime të turpshme. Informacion i mëtejshëm që mund të ndihmojë në zhvillimin e materialeve të trajnimit mund të gjendet në adresën http://communication.howstuffworks.com/how-social-networks-work.htm.    Mesazhet e menjëhershme janë një formë e bisedimit në kohë reale ndërmjet dy apo më shumë individëve duke përdorur programe të përbashkëta. Ky lloj bisedimi ka të bëjë me kontaktin ndërmjet njerëzve që njihen me njëri tjetrin përkundrejt llojeve të tjera të chat-it që lejojnë komunikimin ndërmjet personave të panjohur. Keqbërësit dihet se i përdorin mesazhet e menjëhershme si mënyrë komunikimi.    Informacion i mëtejshëm mund të jepet nga trajneri në formën e të dhënave statistikore në lidhje me rritjen e përdorimit të rrjeteve sociale. Shembuj të rritjes së faqeve të caktuara në Internet dhe impakti global mund të jepen si shembuj.    Trajneri duhet të marrë në konsideratë dhënien e shembujve për llojet e informacionit që është i disponueshëm për hetuesit. Disa shembuj që mund të përdoren jepen tek prezantimet, megjithëse trajnerët duhet të përpiqen të gjejnë shembuj që kanë lidhje me vendndodhjen gjeografike të pjesëmarrësve në trajnim. | | | |
| Slajdet 133 deri 136 | Lojrat Online  Një lojë Online është një lojë e luajtur në ndonjë formë të një rrjeti kompjuterik. Kjo pothuaj gjithmonë nënkupton Internetin ose një teknologji të ngjashme me të, por lojrat kanë përdorur gjithmonë teknologjinë që është më e fundit; pajisjet modem përpara Internetit dhe terminalet me kabull përpara pajisjeve modem.    Përhapja e lojërave online ka reflektuar përhapjen e përgjithshme të rrjeteve kompjuterike nga rrjetet e vogla lokale tek Interneti dhe rritja e vetë aksesit në Internet. Lojërat online mund të variojnë nga lojërat me tekste të thjeshta tek lojërat që përfshijnë grafika komplekse dhe botë virtuale të populluara nga shumë lojtarë njëkohësisht.  Shumë lojëra online kanë lidhur komunitete online me njëri tjetrin, duke i bërë lojërat një formë aktiviteti social përtej lojërave me një lojtar.    Trajneri duhet të përpiqet të japë shembuj të krimeve që përfshijnë lojërat. Këto po bëhen më mbizotëruese dhe do të ishte e dobishme të merreshin në konsideratë implikimet ligjore në vende të ndryshme. | | | |
| Slajdet 137 deri 146 | Gjurmueshmëria dhe Anonimiteti në Internet  Anonimiteti në Internet është një subjekt i rëndësishëm që do të trajtohet në nivelin fillestar të këtij kursi. Këto terma do të hasen nga gjyqtarët dhe prokurorët rregullisht. Shembuj të shërbimeve anonime duhet të jepen me një shpjegim sesi funksionojnë ato. Duhet të shpjegohet ndryshimi ndërmjet transmetimeve anonime dhe transmetimeve transparente. Slajdet e dhëna në prezantim mund t’i ndihmojnë trajnerët të zhvillojnë materialet e tyre. Trajneri duhet të japë shembuj edhe për shërbimet anonime të postës elektronike dhe të Internetit. | | | |
| Slajdet 147 deri 159 | Pjesa e Pestë – Krimet në Internet  Si pjesa përfundimtare substantive e mësimit, trajneri duhet të përpiqet të identifikojë mënyrat në të cilat përdoret teknologjia që është shpjeguar në kryerjen e veprave penale. Në të vërtetë, i vetmi vend në botë që i merr ankesa për krimet në Internet janë Shtetet e Bashkuara të Amerikës. Statistikat e dhëna nga Qendra e Ankesave për Krimet në Internet japin një farë ideje për shkallëzimin e problemit. Këto mund të përdoren dhe duhet të mbahen të azhurnuara nga trajneri. | | | |
|  | ***Skemat e Investimit***  Përdorimi i Internetit për marrjen e mbështetjes financiare për skema të teknologjisë së lartë si për shembull uebsajte për shopping ose shërbimofrues të rinj.    ***Skemat me Kartat e Kreditit***  Përdorimi i të dhënave të Kartave të Kreditit të marra në mënyrë të paligjshme për blerjen e mallrave me vlerë nëpërmjet Internetit.  ***Skemat për Mundësitë për Biznes / Skemat e Punës nga Shtëpia***  Përdorimi i Internetit për reklamimin e mundësive për punë ku viktima paguan paraprakisht për marrjen e informacionit.    ***Mashtrimet 419***  Mashtrimet nga Afrika Perëndimore – mjetet e dërgimit kanë ndryshuar – aktualisht realizohen nëpërmjet postës elektronike në vend të postës tradicionale ose kërkesave me faks, por asgjë tjetër nuk ka ndryshuar – potencialisht akses i madhe me anë të dërgimit të mesazheve elektronike të pakërkuara.    ***Veprimet Bankare nëpërmjet Internetit***  Thjesht kopjimi i uebsajtit të një Banke, ndryshimi paksa i adresës së Internetit, vendosja e disa linkeve për legjitimimin e shërbimeve bankare dhe vetëm një apo dy linke për investime shumë fitimprurëse që kërkojnë transferimin e shumave të mëdha për garantimin e përfshirjes në një mundësi të pabesueshme për investime.    ***Apelet për Bamirësi për Fatkeqësi Natyrore***  Nuk kishte kaluar as edhe një orë nga ndodhja e Tsunamit në Lindjen e Largët, kur uebsajtet që kërkonin ndihma për viktimat mbushën Internetin, shumë prej tyre (për të mos thënë të gjitha) ishin të rreme.    ***Herbal Viagra***  Në fushën e trajtimit alternativ mjekësor online, dërgime me email të pakërkuara nga “klientët”, shumica e produkteve nuk kanë asnjë efekt përfitues (nëse dërgohen), disa janë edhe të rrezikshme.    ***Nuset Ruse***  Faqe Interneti që ofrojnë kontakte me femra të bukura nga vendet e Evropës Lindore dhe vizita të lira në shtetet e Rusisë.    ***Fitimet e Lotarive***  Kërkesë për pagesë për marrjen e fitimeve të lotarive ose ndihmë për të fituar në lotari (shpesh me llogaritë e huaja).  ***Phishing***  Mesazhe të postës elektronike që pretendojnë të jenë nga një burim i mirënjohur (të tilla si banka, ose kompani shërbimofruese të Internetit) që kërkojnë konfirmimin e të dhënave personale.    Trajneri duhet të përpiqet të identifikojë çështje gjyqësore nga rajoni ku zhvillohet kursi dhe t’i përdorë ato si shembuj. Në fund të sesionit, trajneri duhet të inkurajojë pjesëmarrësit të ndajnë përvojat dhe njohuritë e tyre në lidhje me Krimet në Internet. | | | |
|  | Ushtrime Praktike (sipas rastit)  Nuk është parashikuar asnjë ushtrim praktik për këtë sesion të veçantë sepse nuk ka asnjë garanci se niveli i teknologjisë dhe aksesi në Internet për ofrimin e shembujve të tillë do të jetë i disponueshëm në të gjitha vendet e zhvillimit të trajnimeve.  Në të ardhmen trajnerët mund të duhet të plotësojnë këtë seksion duke shtuar shembuj, në rastet kur trajnimi zhvillohet në një mjedis ku pajisjet janë të përshtatshme për ofrimin e shembujve. | | | |
|  | **Kontrolli i Njohurive**  Nuk është parashikuar ndonjë kontroll njohurish përveç atij të parashikuar më lart për këtë kurs. Nuk është kërkuar asnjë vlerësim zyrtar. | | | |
| Slajdet 160 deri 162 | Pjesa e Gjashtë – Përmbledhje / Përsëritje | | | |
|  | Trajneri duhet të kontrollojë njohuritë për pikat e mëposhtme për të garantuar se janë arritur objektivat për pjesëmarrësit:   * Të shpjegojë impaktet e ndryshme që teknologjia ka mbi krimin * Të rendisë pjesët përbërëse të një sistemi kompjuterik * Të shpjegojë sesi ruhen të dhënat në sistemet kompjuterike * Të identifikojë sistemet e ndryshme kompjuterike * Të shpjegojë sesi funksionojnë rrjetet * Të përshkruajë funksionet e Internetit * Të identifikojë të paktën 5 programe të mëdha të Internetit * Të shpjegojë sesi është zhvilluar Interneti nga fillimi deri në më sot. * Të bëjë dallimin ndërmjet programeve të ndryshme të Internetit * Të identifikojë sesi i përdorin keqbërësit programet e ndryshme të Internetit   Kjo mund të arrihet me anë të diskutimit në grup, pyetjes së pjesëmarrësve, një kuici apo metodave të tjera të njohura.  Ky mësim u përpoq të jepte disa udhëzime në lidhje me tipin dhe nivelin e njohurive teknologjike që kërkohen nga Gjyqtarët dhe Prokurorët për përmbushjen e rolit të tyre me efektivitet. Mësimi nuk pretendon të jetë një analizë e plotë e çështjeve dhe aty ku është e përshtatshme tregon se ku mund të merret informacion i mëtejshëm.  Rekomandohet që zhvilluesit e trajnimit të garantojnë që materiali që përgatisin është i azhurnuar dhe përfshin çështjet më të fundit teknologjike sepse ato kanë ndikim në sjelljen kriminale; ndikimi i tij mbi rregullat ligjore, procedurale dhe rregullat e marrjes së provave brenda juridiksionit ku zhvillohet trajnimi. Ka ndryshime teknologjike që do të ndikojnë sistemin e drejtësisë penale, të tilla si ruajtja në gjendje të ngurtë e të dhënave dhe Web 2.0. Këto do të jenë çështje të rëndësishme për tu përfshirë në programet e trajnimit dhe kërkojnë përfshirje sepse bëhen më shumë mbizotëruese.  Si me çdo program tjetër, çdo kurs trajnimi i hartuar për Gjyqtarët dhe Prokurorët duhet të ketë objektiva të qarta, të cilat janë SMART (Specifike, (të) Matshme, (të) Arritshme, Reale dhe (në) Afat). Kjo është e rëndësishme që të garantohet arritja e objektivave. Evitoni përdorimin e objektivave me fjalë të tilla si “kuptoj” ose “njoh” sepse ato nuk i përmbushin kriteret. Për shembull si do ta matnit sesi do të arrihej objektivi i “njohjes”? Është më mirë të përdoren fjalë të tilla si rendit ose identifiko, të cila janë të matshme. Një guidë për caktimin e objektivave SMART mund të gjendet në adresën [www.sheffield.ac.uk/.../Guide%20to%20setting%20objectives.doc](http://www.sheffield.ac.uk/.../Guide%20to%20setting%20objectives.doc)  Përdorimi i rasteve studimore për informimin e mësimit konsiderohet i përshtatshëm për këtë lloj mësimdhënieje dhe është më shumë afër me stilet e mësimdhënies për të rritur sesa thjesht mësimdhënia didaktike.  Roli kryesor i zhvilluesit të trajnimit është të garantojë që të arrihet synimi i përgjithshëm i çdo aktiviteti të mësimit dhe objektivat specifike. Ky kapitull jep pak informacion për të ndihmuar këtë proces. | | | |
| **Burime të Mundshme Shtesë**  E mëposhtmja është një listë me botime nga organizatat/vendet që mund të jetë e dobishme për trajnerët në zhvillimin e materialeve të kursit në lidhje me provat elektronike. | | | | |
| **Organizata** | | **Vendi i Origjinës** | **Dokumentacioni Shembull** | |
| Organizata Ndërkombëtare për Standardizimin (ISO) dhe Komisioni Ndërkombëtar Elektroteknik (IEC) | | Ndërkombëtar | ISO/IEC 17025:2005 Kriteret e përgjithshme për kompetencën e testimit dhe laboratorëve të kalibrimit (18.10 klasa e provave elektronike, 01 Ruajtja e të dhënave, .02 Analiza e të dhënave)  ISO/IEC CD 27037 Teknologjia e Informacionit – Teknikat e sigurisë – Udhëzime për identifikimin, mbledhjen, përftimin dhe ruajtjen e provave dixhitale  ISO/IEC 9797-2:2011 Teknologjia e Informacionit – Teknikat e sigurisë – Kodet e Vërtetimit të Origjinalitetit të Mesazhit (MACs) – Pjesa 2: Mekanizmat e përdorimit të një funksioni të vlerës hash të dedikuar | |
| Rrjeti Evropian i Instituteve të Shkencës së Kriminalistikës (ENFSI) | | KE | EA-5/03 Udhëzime për zbatimin e ISO/IEC 17020 në fushën e hetimit të skenës së krimit | |
| Shoqata e Shefave të Policisë (ACPO)  PCeU  Forcat e Policisë së Uellsit  Krimi elektronik Uells | | Angli, Uells dhe Irlanda e Veriut  Uells | Guidë e Praktikave të Mira për Provat Elektronike Kompjuterike.  Guida e përgjigjes së parë: guida e përgjigjes së parë për hetuesit në lidhje me incidentet e lidhura me kompjuterët. | |
| ACPO | | Angli, Uells dhe Irlanda e Veriut | Guida e Praktikave të Mira dhe Konsulencës: Për Menaxherët e Njësive të Krimeve Kompjuterike/të Teknologjisë së Lartë. | |
| ACPO | | Angli, Uells dhe Irlanda e Veriut | Guida për Menaxherin: Guida e Konsulencës dhe e Praktikave të Mira për Menaxherët e Hetimit të Krimeve Elektronike. | |
| Institucioni i Standardeve Britanike (BSI) | | MB | ASTM E1732 – 11 Terminologjia Standarde e lidhur me Shkencën e Kriminalistikës  ASTM E1492 – 11 Praktikat Standarde për Marrjen, Dokumentimin, Ruajtjen dhe Tërheqjen e Provave në një Laborator të Kriminalistik | |
| Shërbimi i Akreditimit të Mbretërisë së Bashkuar (UKAS) | | MB | Botime që lidhen me akreditimin e Organit të Certifikimit | |
| Rregullatori i Kriminalistikës (FSR) | | MB (Ministria e Brendshme) | Kodet e Praktikës dhe Etikës për Ekspertët Kriminalistë dhe Praktikuesit në Sistemin e Drejtësisë Penale  Procesverbali i Grupit të Kriminalistikës Dixhitale | |
| Instituti i Inxhinierisë dhe Teknologjisë (IET) | | Ndërkombëtar (IIT përfshin IIE (Institutin e Inxhinierëve Elektrikë) dhe III (Institutin e Inxhinierëve të Inkorporuar)). | Zhvillimi i standardeve në fushat ekzistuese dhe të reja të teknologjisë. | |
| Grupi Evropian i Trajnimi dhe Edukimit për Krimin Kibernetik (ECTEG) | | KE (Europol) | Procesverbali i takimeve të ECTEG | |
| Shoqata Britanike për Kompjuterët, Grupi i specialistëve për kriminalistikën dixhitale | | MB | Dokumentet e Politikave | |
| Departamenti i Drejtësisë së SHBA | | SHBA | Hetimi kriminalistik i Provave Dixhitale: Një guidë për zbatimin e ligjit | |
| FBI/SWGDE | | SHBA | Provat Dixhitale: Standarde dhe Parime | |
| Departamenti Amerikan i Tregtisë | | SHBA | Udhëzime për kriminalistikën e telefonave celularë | |
| Organizimi ndërkombëtar i Provave Kompjuterike | | Ndërkombëtar | Udhëzime për Provat Dixhitale | |
| Këshilli i Evropës | | KE | Konventa për Krimin Kibernetik, kriteret procedurale dhe legjislative për vendet që dëshirojnë të ratifikojnë konventën | |
| Interpol | | Ndërkombëtar | Manual për Krimin Kibernetik | |
| Aftësitë për Drejtësinë | | MB | Standardet profesionale kombëtare për përballjen me krimin elektronik, dhënia e standardeve për njohuritë dhe aftësitë në trajtimin e provave elektronike, kriminalistikës dixhitale dhe hetimeve për krimin kibernetik. | |
| Shërbimi Sekret i SHBA-ve (Departamenti i Sigurisë Kombëtare) | | SHBA | Praktikat më të Mira për Sekuestrimin e Provave Elektronike  v.3A Guidë xhepi për përgjigjen e parë | |
| Komisioni Evropian | | KE | Sekuestrimi i “provave elektronike” Projekti Oisin 2002/OIS/014 | |
| Instituti Kombëtar i Drejtësisë (NIJ)  (Instituti Kombëtar i Standardeve në Teknologji NIST) | | SHBA | Hetimi i Skenës së Krimit Elektronik – Një guidë për përgjigjen e parë (Botimi i 2) | |

|  |  |  |
| --- | --- | --- |
| Mësimi 1.3.1 – Rishikimi ditor | | **Kohëzgjatja: 30 Minuta** |
| **Burimet materiale të nevojshme:**   * Kompjuter Laptop ose Kompjuter Tavoline me Windows 7 dhe me Office 2010 * Projektor * Prezantimet me PowerPoint | | |
| **Synimi:**  Synimi i këtij sesioni është rishikimi i aktiviteteve të ditëve të mëparshme, marrja e vlerësimeve nga pjesëmarrësit dhe kontrolli i përmbushjes së objektivave të sesioneve. | | |
| **Objektivat:**  Nga fundi i mësimit, pjesëmarrësit do të jenë në gjendje të:   * Identifikojnë fushat e aktiviteteve të ditëve të mëparshme që kanë kuptuar * Identifikojnë fusha të tilla ku kanë nevojë të rishikojnë materialet për të sjellë njohuritë e tyre në nivelin e kërkuar. | | |
| **Hyrje**  Ky sesion është përgatitur për ti lejuar pjesëmarrësit të kontrollojnë se i kanë kuptuar mësimet e ditëve të mëparshme dhe se janë në gjendje të përmbushin objektivat për sesionet individuale. Është gjithashtu për t’i dhënë trajnerit mundësinë e kontrollit të nivelit të njohurive të pjesëmarrësve dhe identifikimin e fushave ku mund të përmirësohen materialet e mësimdhënies. | | |
| **Slajdet nr.** | **Përmbajtja:** | |
| **Slajdet**  **1 deri 12** | **Prezantimi me PowerPoint** (ose prezantim të lloji tjetër)  Slajdet në këtë prezantim janë hartuar për të ndihmuar trajnerin dhe pjesëmarrësit me aktivitetet e ditëve të mëparshme. Trajneri duhet të bëjë përmbledhjen e aktiviteteve duke përdorur axhendat dhe objektivat si etapa. | |
|  | **Ushtrimet Praktike** (sipas rastit)  Nuk është përgatitur asnjë ushtrim praktik për këtë sesion. | |
|  | **Kontrolli i Njohurive**  Trajneri duhet të kontrollojë njohuritë me anë të bërjes së pyetjeve përkatëse nga secili aspekt i sesioneve. | |
|  | **Përmbledhje**  I gjithë ky sesion është hartuar si një përmbledhje e aktiviteteve të ditëve të mëparshme dhe nuk kërkohet asnjë përmbledhje. | |

|  |  |  |
| --- | --- | --- |
| Mësimi 1.2.3 Krimi Kibernetik si vepër penale – Legjislacioni i Brendshëm | | **Kohëzgjatja: 90 Minuta** |
| **Burimet materiale të nevojshme:**   * Kompjuter Laptop ose kompjuter tavoline me Sistemin Windows 7 dhe me Programin Office 2010 * Projektor * Prezantimi me PowerPoint | | |
| **Synimi:**  Synimi i këtij sesioni është njohja e pjesëmarrësve me rregullat kombëtare për krimin kibernetik, llojet e veprave penale të përshkruara dhe relevante dhe kuadri ligjor ndërkombëtar i zbatueshëm. | | |
| **Objektivat:**  Në përfundim të mësimit, pjesëmarrësit do të jenë në gjendje të:   * Identifikojnë rregullat kombëtare për krimin kibernetik * Identifikojnë llojet e veprave penale të përshkruara në të drejtën e brendshme * Identifikojnë disa specifika të rregullave kombëtare për krimin kibernetik, në kontekst të kuadrit ligjor ndërkombëtar. | | |
| **Hyrje**  Objektivi i këtij sesioni është dhënia e të gjithë informacionit të nevojshëm gjyqtarëve dhe prokurorëve për t’iu mundësuar atyre të përdorin me efektivitet dispozitat ligjore në legjislacionin e brendshëm për ndjekjen ligjore dhe gjykimin e çështjeve të krimit kibernetik. Në përfundim të sesionit pjesëmarrësit do të jenë në gjendje të identifikojnë dispozitat ligjore në legjislacionin e brendshëm që lidhen me:   * Veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së sistemeve kompjuterike dhe të dhënave * Veprat penale të kryera nëpërmjet sistemeve kompjuterike dhe të dhënave * Veprat e tjera të lidhura me përmbajtjen, etj.   Ky sesion është përgatitur për ti dhënë pjesëmarrësve një shembull sesi konventa e Budapestit është inkorporuar në legjislacionin kombëtar të një vendi, në këtë rast të Portugalisë. Trajnerët do të nevojitet të zëvendësojnë informacionin Portugez me detajet legjislative korresponduese të vendit të tyre. | | |
| **Slajdet nr.** | **Përmbajtja:** | |
| Slajdet 1 deri 66 | Prezantimi me PowerPoint (ose lloj tjetër prezantimi)  Përmbajtja e slajdeve në këtë seksion është vetëm një shembull i asaj që mund të përshkruhet në secilën prej trajnimeve lokale.  Në mënyrë ideale, sesioni në të drejtën e brendshme materiale duhet të përmendë instrumentet ligjore ndërkombëtare të nënshkruara ose të ratifikuara dhe rezultatin e transpozimit të tyre në të drejtën e brendshme.  Krahas kësaj, duhet të jepet një përshkrim i llojeve të veprave sipas ligjit të brendshëm, dhe në fund, sipas rastit, të jepet një përshkrim i çdo specifike eventuale të ligjit material të brendshëm. | |
| Slajdi 2 | Axhenda  Ky sesion ka katër pjesë:   1. Pjesa e Parë do të fokusohet tek e Ligji Penal Material i Konventës së Budapestit për Krimin Kibernetik. 2. Ligji Material Penal Kombëtar do të jetë objekti i Pjesës së Dytë. 3. Pjesa e Tretë do të fokusohet tek Rastet Praktike. 4. Së fundi, një përmbledhje e të gjithë pjesëve do të paraqitet në Pjesën e Katërt. | |
| Slajdi 3 | Trajneri do të mbulojë pikat e mëposhtme:     * Dispozitat e ligjit penal material dhe disa prej faktorëve kyç të përdorur për përshkrimin e veprave penale, bazuar në Konventën e Budapestit * Dispozitat e Ligjit Penal Material dhe disa prej faktorëve kyç të përdorur për përshkrimin e veprave penale, bazuar në legjislacionin e brendshëm ekzistues. * Nevojat dhe avantazhet e harmonizimit ndërmjet legjislacionit kombëtar dhe instrumenteve ndërkombëtare, në veçanti Konventa e Budapestit. | |
| Slajdi 4 | * Dispozitat përkatëse të ligjit material bazuar në diskutimet në lidhje me rastet praktike të paraqitura. | |
| Slajdet 5 dhe 6 | Pjesa e Parë – Konventa e Budapestit për Krimin Kibernetik – Ligji Penal Material  Si traktati i parë ndërkombëtar për krimin kibernetik, Konventa e Budapestit synon të lehtësojë dhe zhvillojë bashkëpunimin ndërkombëtar në hetimet penale.    Një synim primar është harmonizimi i ligjit material ndërmjet Palëve për të lejuar bashkëpunimin. Për këtë qëllim, Konventa e Budapestit përcakton:   * Veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së sistemeve kompjuterike dhe të dhënave. * Veprat penale të kryera me ndihmën e kompjuterëve. | |
| Slajdet 7 | Ky sesion trajton një nga kategoritë më të rëndësishme të krimit kibernetik: veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave dhe sistemeve kompjuterike. Kjo gjë mund të quhet krim kibernetik në kuptimin e ngushtë të fjalës. | |
| Slajdet 8 dhe 9 | Vepra penale e aksesit të paligjshëm kryhet nga ata që hyjnë në të gjithë apo një pjesë të sistemit kompjuterik pa të drejtë. Ky veprim duhet të jetë i qëllimshëm dhe përshkruhet në Nenin 2 të Konventës së Budapestit.  Ky veprim shpesh referohet si *hacking[[71]](#footnote-72)* në sistemet kompjuterike dhe është një nga veprat penale më të zakonshme kompjuterike. Megjithatë, ka dhe fenomene të tjera, përveç hyrjes së paautorizuar në sistemet kompjuterike, që mund të klasifikohet si akses i paligjshëm – në fakt, hyrja e paautorizuar përdoret zakonisht për të përshkruar veprimin e hyrjes së paligjshme në një sistem kompjuterik, me anë të teknologjisë. Por aksesi i paligjshëm mbulon gjithashtu çdo hyrje të paautorizuar në një sistem, pavarësisht nga teknologjia e përdorur apo madje edhe përdorimin ose jo të teknologjisë. Për shembull, një rast i tillë do të ishte marrja e paligjshme e fjalëkalimit nga keqbërësi. Interesi që mbrohet këtu është konfidencialiteti i të dhënave dhe i sistemit kompjuterik. | |
| Slajdet 10 dhe 11 | Kapja e paligjshme e të dhënave, e përshkruar në Nenin 3 të Konventës së Budapestit, është gjithashtu një cënim i qëllimshëm. Kryhet nga ata, që pa të drejtë, kapin transmetimet jopublike të të dhënave kompjuterike, për, nga ose brenda një sistemi kompjuterik, me anë të mjeteve teknike.  Kjo dispozitë mbron integritetin e transmetimeve jo-publike të të dhënave kompjuterike, duke kriminalizuar kapjen e tyre të paautorizuar.  Transmetimet e të dhënave për një sistem kompjuterik, ose nga ky sistem kompjuterik, ose brenda të njëjtit sistem kompjuterik, janë realitetet më aktuale në jetën e përditshme të sotme të rrjeteve.  Teknikisht, mund të jetë shumë e lehtë të kapësh komunikimet nëse rrjeti dhe komunikimi nuk janë të mbrojtur siç duhet. Për shembull kapja e komunikimeve mund të zbulojë se cilat faqe interneti janë vizituar, ose mesazhet e postës elektronike që janë dërguar.  Vepra penale e kapjes së paligjshme të të dhënave synon, për rrjedhim, të tregojë dobësinë e teknologjisë së komunikimeve, duke mbrojtur sekretin e komunikimeve jo-publike. | |
| Slajdet 12 dhe 13 | Ata që, me dashje dhe pa të drejtë, shkaktojnë dëmtim, fshirje, shkatërrim, ndryshim, ose prishje të të dhënave kompjuterike, kryejnë veprën penale të ndërhyrjes tek të dhënat, të përshkruar nga Neni 4 i Konventës së Budapestit.  Ndërhyrja tek të dhënat mbron integritetin e të dhënave kundër ndërhyrjes së paautorizuar. Pronari i të dhënave ka të drejtën t’i mbajë ato siç janë, njësoj si pronari i mallrave në jetën reale ka të drejtë të mbajë të sigurtë pronën e tij nga ndërhyrjet e të tjerëve. Në disa juridiksione, dëmtimi i zakonshëm i pronës përfshin gjithashtu ndërhyrjen tek të dhënat; tek të tjerat ka nevojë të përshkruhet veçmas dëmtimi i të dhënave kompjuterike ose ndërhyrja tek të dhënat.  Kjo vepër penale tregon rritjen e madhe të të dhënave përkatëse (të dhënave kompjuterike) për jetën moderne. Të dhënat kompjuterike janë shumë të dobëta dhe mund të shkatërrohen ose manipulohen lehtësisht. Ky rregull penal mbron integritetin dhe disponueshmërinë e tyre.  Një nga rastet më të shpeshta të ndërhyrjes tek të dhënat është rezultati i veprimit të viruseve – që pa të drejtë vetë-instalohen në kompjuterin e viktimës dhe, për shembull, fshijnë të dhënat. | |
| Slajdet 14 dhe 15 | Ndërhyrja në një sistem është pengimi i funksionimit të sistemit kompjuterik – pengimi serioz: Neni 5 i Konventës së Budapestit nuk parashikon pengimin jo-serioz. Ky efekt mund të jetë rezultat i futjes, transmetimit, dëmtimit, fshirjes, shkatërrimit, ndryshimit ose prishjes së të dhënave kompjuterike, nëse kjo gjë kryhet qëllimisht dhe pa të drejtë. Në përgjithësi, ky aspekt i përgjithshëm përjashton, për shembull, testet e sigurisë të kryera nga administratori i rrjetit. Kjo vepër përfshin një gamë të gjerë veprimesh që ndërhyjnë në funksionimin normal dhe të duhur të një rrjeti. Në fakt, Konventa e Budapestit e njeh rëndësinë e sistemit të komunikimit dhe të teknologjisë kompjuterike në jetën e përditshme – disponueshmëria e këtyre sistemeve është thelbësore për funksionimin e rregullt të aktiviteteve sociale, ekonomike dhe publike. Por kjo lloj vepre penale nuk mbulon vetëm ndërhyrjet në shkallë të gjerë, si p.sh. sulmet e mohimit të shërbimit. Edhe veprimet e vogla, që përfshijnë një kompjuter, mund të përbëjnë ndërhyrje në sistemin kompjuterik – do të ishte rasti i një *mail bombing[[72]](#footnote-73)* me objektiv një adresë të vetme të postës elektronike. Në fakt, do të ishte gjithmonë një vepër penale e ndërhyrjes në sistem në rastin kur një keqbërës godet një sistem kompjuterik me më shumë kërkesa sesa mund të përballojë ai sistem.  Kjo vepër penale parashikon mbrojtjen e aksesit në rrjetet e komunikimit, duke mbrojtur edhe operatorët e sistemit edhe përdoruesin. | |
| Slajdet 16 deri 19 | Një nga shkeljet më komplekse të përshkruara në Konventën e Budapestit është vepra penale e shpërdorimit të pajisjeve kompjuterike – Neni 6.  Si me vepra të tjera penale, veprimi i keqbërësit duhet të jetë i qëllimshëm dhe pa të drejtë. Mbulon një gamë të gjerë aktesh, të gjithë të lidhura me pajisje, të cilat mund të keqpërdoren.  Kjo është një vepër penale “e re”, e papërfshirë në Rekomandimin e vitit 1989. Gjithashtu është shumë inovative – faktet e përshkruara aty nuk njiheshin më parë si vepër penale në shumë prej legjislacioneve kombëtare.  Në thelb, ajo ndalon prodhimin, shitjen, prokurimin për përdorim, importimin, shpërndarjen ose bërjen të disponueshme të pajisjeve, duke përfshirë programin kompjuterik, që dizenjohen ose përshtaten kryesisht për qëllimin e kryerjes së ndonjë prej veprave penale të përmendura në Konventë.    Po kështu, kriminalizon shitjen e fjalëkalimeve të kompjuterëve, kodeve të hyrjes, ose të dhënave të ngjashme me anë të të cilave mund të aksesohet çdo pjesë apo i gjithë sistemi kompjuterik. Me këtë dispozitë, Konventa njeh nevojën e inkriminimit të “tregut dytësor” lulëzues dhe gjithnjë e më shumë i rëndësishëm ekonomikisht i “pajisjeve për kryerjen e veprave penale”: shitja online nga hakerat e mjeteve të tyre të zanatit, paketave të gatshme të viruseve gjerësisht të disponueshme online dhe shpërndarja me shumicë e fjalëkalimeve të vjedhura me anë të përdorimit të Trojanëve ose pajisjeve të tjera. Kjo do të thotë se *hyrja e paautorizuar* në një sistem kompjuterik nuk është më ekskluzivitet i programuesve me aftësi të larta. Çdo keqbërës “i rregullt” lehtësisht mund të blejë mjetet e nevojshme, ose direkt fjalëkalimet e vjedhura – shumë shpesh keqbërësi shitës do të ofrojë gjithashtu edhe “shërbimin e klientit” dhe të ndihmojë klientin e tij të përgatisë kompjuterin e tij për kryerjen e krimit.  Një nga detajet më të diskutuara në Nenin 6 i referohet 1, b, që (përsëri me dashje dhe pa të drejtë), inkriminon posedimin e një *pajisjeje* me qëllimin e përdorimit të kryerjes së ndonjë prej veprave penale të parashikuara në Nenet 2 deri 5 të Konventës (aksesi i paligjshëm, kapja e paligjshme e të dhënave, ndërhyrja tek të dhënat dhe ndërhyrja në sistem).  Kjo alternativë është e ngjashme me ato që disa juridiksione quajnë “akte përgatitore” që, në këtë rast, janë tashmë të kriminalizuara dhe në mënyrë autonome. | |
| Slajdi 20 | Veprat penale të lidhura me kompjuterët janë krime të kryera nëpërmjet një sistemi kompjuterik. Këto shkelje janë forma të reja të krimeve tradicionale, por ato mund të kryhen brenda mjedisit virtual dhe nuk mund të ndodhin jashtë botës virtuale. | |
| Slajdi 21 | Falsifikimi me anë të kompjuterit, i përshkruar në Nenin 7 të Konventës së Budapestit është një formë e veçantë e falsifikimit. Në shumë vende, falsifikimi është një vepër penale tradicionale. Por zakonisht, i referohet objekteve të prekshme dhe nganjëherë nuk mund të përdoret për kriminalizimin e falsifikimit me anë të kompjuterit, ose falsifikimin e të dhënave kompjuterike. Kjo ishte arsyeja e futjes në Konventë në Nenin 7.  Në këtë pikë, Konventa synon të fusë një vepër penale paralele tek kategoria e falsifikimit tradicional të dokumenteve (dokumenteve të prekshëm). Por në këtë rast, objekti i veprës penale janë të dhënat kompjuterike. Kjo vepër penale kryhet nga ata që fusin, ndryshojnë, fshijnë, ose prishin të dhënat kompjuterike, të cilat bëhen të dhëna joautentike me qëllimin që këto të dhëna të konsiderohen ose me të cilat të veprohet për qëllime ligjore sikur të ishin autentike.  Sigurisht, kjo vepër penale kërkon veprim të qëllimshëm dhe pa të drejtë. | |
| Slajdi 22 | Mashtrimi i kryer nëpërmjet kompjuterit, i përcaktuar në Nenin 8 të Konventës së Budapestit, është një lloj vepre penale që, teorikisht, mund të dallohet me vështirësi nga mashtrimi tradicional, si një vepër penale. Megjithatë, në fakt është një formë e re dhe autonome e asaj vepre penale tradicionale. Vetëm se mund të kryhet brenda mjedisit dixhital.  Shumica e ligjeve të brendshme e kriminalizojnë mashtrimin tradicional, por zakonisht, është i papërdorshëm në situatat e lidhura me kompjuterët. Mashtrimi kërkon një mashtrim ose një gabim të qëllimshëm të kryer nga një person. Por shumicën e kohës, në mashtrimet kompjuterike, nuk ka një ndërhyrje të drejtpërdrejtë të një personi dhe është thjeshtë rezultat i manipulimit të një sistemi kompjuterik. Kjo është arsyeja se pse përshkrimi i llojit të veprës penale të mashtrimit kompjuterik, ndërhyrja e një personi, si keqbërës, është zëvendësuar nga manipulimi i të dhënave me qëllimin e pasjes, pa të drejtë, të një përfitimi ekonomik. Në këtë mënyrë, nuk është e nevojshme të kihet mashtrimi i mendjes së një personi tjetër si element i mashtrimit. | |
| **Slajdi 23** | Veprat penale të lidhura me përmbajtjen i referohen atyre krimeve që u bënë më të lehtë për tu kryer nëpërmjet përdorimit të kompjuterëve ose rrjeteve kompjuterike. Këto lloj veprash mund të kryhen me mjete të tjera por kompjuterët dhe rrjetet kompjuterike i bënë ato më të lehta. | |
| Slajdet 24 deri 26 | Neni 9 i Konventës së Budapestit zbulon një nga inovacionet më të mëdha të këtij traktati: ai krimininalizon aktet e pornografisë së fëmijëve të kryera nëpërmjet sistemit kompjuterik.    Tregtia me pornografinë e fëmijëve u rrit jashtëzakonisht shumë me ardhjen e Internetit. Rrjetet e komunikimit dhe informacionit ofrojnë një numër të madh avantazhesh dhe mundësish për ata që kërkojnë një lloj të tillë përmbajtjeje. Krahas kësaj, në Internet, përdoruesit mund të jenë anonimë, pa pasur akses tek materiali i abuzimit me fëmijë online.    Në lidhje me veprat penale të pornografisë së fëmijëve, duhet të diskutohet një aspekt në veçanti, sepse trajtohet gjerësisht në tekstin e Konventës: ndëshkimi i posedimit të thjeshtë të materialeve të pornografisë së fëmijëve. Neni 9, 1 e përcakton si shkelje posedimin e thjeshtë të këtij lloj materiali, brenda një sistemi kompjuterik dhe gjithashtu marrjen e imazheve të tillë thjesht për përdorim personal. Kjo qasje është miratuar nga *forumet* e tjera ndërkombëtare që e trajtojnë këtë temë.    Po kaq e diskutueshme është kriminalizimi i “pseudo imazheve”. Nenet e Konventës përfshijnë jo vetëm situatat e fotove ku një fëmijë i vërtetë fotografohet gjatë një aktiviteti seksual, por gjithashtu edhe përfaqësimet e rreme të fëmijëve – për shembull, piktura të fëmijëve të krijuara tërësisht nga kompjuterët (për shembull, vendosja e kokës së një fëmije në trupin e një të rrituri që kryen një akt seksual) ose foto të të rriturve (në mënyrë të bindshme) që pretendojnë (sillen ose vishen) si fëmijë.    Kriminalizimi i posedimit të thjeshtë të materialeve të pornografisë së fëmijëve e bën shumë më të lehtë kryerjen e hetimeve penale për këtë çështje, përderisa në bazë të kësaj dispozite kushdo që ka në posedim këtë lloj materiali mund të ndiqet ligjërisht, dhe qëllimi specifik i përdorimit të fotove në një farë mënyre (për shembull shitja e tyre) ose pjesëmarrja në prodhimin e tyre nuk ka nevojë të provohet. Kjo do të thotë se pedofilët e dyshuar mund të ndëshkohen pa ndonjë provë se kanë vepruar si pasojë e impulseve të tyre drejt një fëmije. Dhe sigurisht, policia dhe gjykatat mund të hetojnë dhe dënojnë furnizuesit e dyshuar të pornografisë së fëmijëve (edhe sikur të jetë thjesht posedim i këtyre materialeve), me ose pa prova që shitblerja ndodhi vërtet.    Në këtë drejtim është e rëndësishme gjithashtu të merret në konsideratë opsioni ligjor nga Bashkimi Evropian. Për shumë vite, Bashkimi Evropian vendosi të kriminalizojë posedimin e thjeshtë të materialeve pornografike të fëmijëve – që nga Vendimi nga Këshilli i 29 Majit 2000. Kohët e fundit, Direktiva 2011/92/EU e Parlamentit Evropian dhe e Këshillit e 13 Dhjetorit 2011, për luftën kundër abuzimit dhe shfrytëzimit seksual të fëmijëve dhe pornografisë së fëmijëve, dhe zëvendësimi i Vendimit Kuadër të Këshillit 2004/68/JHA, thotë se Shtetet Anëtare nga Bashkimi Evropian duhet të kriminalizojnë, ndër sjelljet e tjera kriminale, blerjen ose posedimin e pornografisë së fëmijëve (Neni 5, 2). Megjithatë, i njëjti dokument i jep liri vendimmarrjeje secilit prej Shteteve Anëtare të vendosin nëse ky inkriminim zbatohet për çështje ku materiali pornografik është poseduar nga prodhuesi vetëm për përdorimin e tij privat (përsa kohë që asnjë material pornografik nuk është përdorur për qëllimin e prodhimit të tij dhe me kusht që veprimi nuk përfshin përhapjen e materialit).    Ky opsion nga Bashkimi Evropian është absolutisht në linjë me Nenin 9 të Konventës së Budapestit që inkriminon prodhimin, ofrimin ose bërjen të disponueshme, shpërndarjen ose transmetimin, prokurimin ose thjesht posedimin e pornografisë së fëmijëve në një sistem kompjuterik ose në një pajisje kompjuterike ose pajisje për mbajtjen e të dhënave. Megjithatë, përfshirja e “prokurimit” ose “posedimit” lejon rezervim për Palët në Konventë.  Ky opsion u përforcua nga Konventa për Mbrojtjen e Fëmijëve (CETS 201), e nxjerrë nga Këshilli i Evropës dhe e hapur për nënshkrim në vitin 2007. Synimi i këtij traktati është harmonizimi i dispozitave të ligjit penal, brenda Palëve, me synimin e mbrojtjes së fëmijëve nga shfrytëzimi seksual. Sipas Nenit 20, ndër të tjera “*prokurimi i pornografisë së fëmijëve për vete ose për një person tjetër”* dhe “*posedimi i pornografisë së fëmijëve*” duhet të kriminalizohet. | |
| Slajdet 27 dhe 28 | Konventa e Budapestit nuk përfshin ndonjë dispozitë me vepra penale specifike për çështjet e të drejtave të autorit.  Megjithatë, Neni 10 i Konventës i referohet asaj, edhe pse nuk krijon rregulla të reja konceptuale për këtë tematikë. Por, Konventa thekson se rregullat e mëparshme për të drejtat e njeriut në botën reale duhet të zbatohen në mjedisin online: ajo që ndalohet në jetën reale duhet gjithashtu të ndalohet online. Shkeljet e të drejtave të njeriut online, ose të kryera me anë të një sistemi kompjuterik, duhet të ndëshkohen sikur të kryheshin në botën reale. Për këtë arsye, Konventa i referohet marrëveshjeve dhe traktateve ekzistuese për këtë çështje (Marrëveshja e Parisit nga 24 Korriku i vitit 1971, Konventa e Bernës dhe Traktatet e WIPO-s). | |
| Slajdi 29 | Dy çështje përfundimtare, që i referohen ligjit penal material, duhet të konsiderohet në këtë pikë: ndëshkimi i bashkëpunimit në vepër penale, nga njëra anë, dhe përgjegjësia penale e personave juridikë nga ana tjetër.    Neni 11 i Konventës së Budapestit përshkruan aktet e bashkëpunimit që të gjitha Palët në Konventë duhet të marrin në konsideratë në ligjin e brendshëm. Megjithatë, ajo pranon se krimi në Internet është shpesh një aktivitet “me shumë palë”, dhe shpesh me nivele kontributesh nga palë të ndryshme, duke e bërë ndjekjen ligjore potencialisht të vështirë. | |
| Slajdi 30 | Së fundi Neni 12 i Konventës i kërkon të gjithë Palëve kriminalizimin e veprave të personave juridikë. Kjo është një çështje e rëndësishme. Në fakt, brenda Bashkimit Evropian, kriminalizimi i akteve të personave juridikë është një tematikë e rëndësishme dhe shumë e debatueshme, dhe për rrjedhim është në kuadër të Këshillit të Evropës.  Të dy perspektivat, edhe ajo e Bashkimit Evropian edhe ajo e Këshillit të Evropës përfshijnë çdo lloj përgjegjësie (kriminale ose jo) të kompanive dhe personave të tjerë juridikë me akte kriminale të përfaqësuesve të tyre, që veprojnë në përfaqësimin dhe interesin e tyre. Krahas kësaj, Konventa deklaron se përgjegjësia e personave juridikë ndodh gjithashtu në rast të mungesës së mbikëqyrjes ose kontrollit të një përfaqësuesi ligjor të kompanisë ose personave të tjerë juridik mbi dikë që është nën mbikëqyrje.  Disa vende në Evropë preferojnë mjetet juridike civile, dhe jo zgjidhjet penale, për të rregulluar përgjegjësinë e personit juridik. | |
| Slajdi 32 | Pjesa e Dytë – Ligji Penal Material Kombëtar | |
| **Slajdet 33 deri 43** | Trajnerët do të fusin këtu referencat për dispozitat ligjore kombëtare. | |
| Slajdet 44 | Pjesa e Tretë – Rastet Praktike | |
| Slajdi 45 | 1. **Rast Praktik 1**  * **Faktet / skenari**   Bobi është një Oficer i Policisë. Një natë ai është në shërbim dhe shikon një Mercedes që parkon jashtë shtëpisë së tij. Ai nuk e njeh makinën por dyshon se i përket gruas së shefit të tij. I telefonon stacionit të policisë dhe pyet Merin, operatoren e kompjuterit, t’i thotë se kush e ka në pronësi Mercedesin duke i thënë se makina sapo kishte kaluar me të kuqe. Meri konfirmon se vërtet makina i përket gruas së shefit të tij.  *A ka kryer Bobi ndonjë vepër penale?*   * **Çështjet**   *A ka aksesuar Bobi ndonjë sistem kompjuterik?*  *A ishte ky akses pa të drejtë?*   * **Pikat për diskutim**   Kompjuteri u aksesua nga Meri dhe jo nga Bobi. Ajo është e autorizuar të hyjë tek të dhënat në kompjuter, ajo është e pafajshme. Ishte Bobi ai që duke vepruar nëpërmjet një përfaqësuesi të pafajshëm bëri që të dhënat të aksesoheshin. Ai e gënjeu Merin (një ilustrim i inxhinjerisë sociale), a përbën kjo akses të padrejtë sipas ligjit?  Edhe Bobi edhe Meri kanë të drejtën për të aksesuar kompjuterin e Policisë por në varësi të kushteve strikte që lidhen me ndonjë pyetësor legjitim në lidhje me aktivitetin e policisë. Aty ku aksesi e tejkalon këtë autorizim, a përbën kjo vepër të paligjshme?  Po sikur Bobi të shkojë në rajonin e policisë dhe të arrijë të shohë nga mbrapa mbi supet e Merit ndërsa ajo është duke bërë një kërkim të ligjshëm në lidhje me pronësinë e Mercedesit?  Teknika e quajtur “shoulder surfing”[[73]](#footnote-74) ka bërë që Bobi të përfitojë aksesin tek të dhënat kompjuterike. Mund të jetë çështja në lidhje me “qëllimin” e tij dhe sigurisht ai nuk e ka manipuluar sistemin kompjuterik për të hyrë tek të dhënat, por megjithatë ai e pati aksesin pa të drejtë (megjithëse do të ishte shumë e vështirë të provohej kjo).  Ky rast praktik është hartuar që pjesëmarrësit të shqyrtojnë çështjen e autorizimit (aksesi pa të drejtë).  Pjesëmarrësit gjithashtu mund të pyeten të marrin në shqyrtim situatën: a kishte shkuar Bobi në rajonin e policisë dhe kishte kërkuar informacionin në lidhje me pronësinë e Mercedesit në sistemin e indeksit të kartave – informacioni është i njëjti me atë që mbahet në kompjuter? Çështja këtu është se nuk janë vetë të dhënat që mbrohen (megjithëse ato mund të mbrohen nga legjislacion tjetër për mbrojtjen e të dhënave ndërkohë që sjellja e Bobit gjithashtu mund të përbëjë vepër të paligjshme) por është mjeti në të cilin ruhen të dhënat që është nën mbrojtje.  Sistemet kompjuterike të policisë mbajnë sasi jashtëzakonisht të mëdha të dhënash personale që lidhen me individë së bashku me shumë të dhëna delikate. Aksesi tek të dhëna të tilla duhet t’ju lejohet vetëm atyre që kanë një interes legjitim për to. Në Mbretërinë e Bashkuar, oficerët e policisë dhe operatorët e kompjuterëve të policisë shpesh gjenden që kanë aksesuar në mënyrë të paligjshme sistemet për qëllimet e tyre p.sh. për gjetjen e informacionit që mund të jetë me interes për Median ose në rastin e oficerëve të korruptuar për të zbuluar se çfarë informacioni mbahet për një person të caktuar ose nëse një person i caktuar ose grup është nën hetim aktiv. | |
| Slajdi 46 | 1. **Rast Praktik 2**  * **Faktet / skenari**   Një rojeje sigurie në një bankë i kërkohet nga një grup keqbërësish të vendosë një pajisje, të njohur si “key logger”[[74]](#footnote-75) mbrapa një numri kompjuterësh terminal në bankë. Regjistruesi i të dhënave regjistron shtypjen në tastierë dhe kap fjalëkalimet dhe të dhënat e tjera që i mundësojnë dikujt që ka akses në terminal të hyjë në llogaritë e përdoruesve të stafit të bankës.  Një karakteristikë shtesë e kësaj pajisjeje mundëson që të regjistrohen telefonatat e realizuara me programin Skype të bëra nga përdoruesi i terminalit.  Keqbërësit vendosën gjithashtu dhe një përgjues në një tavolinë pune, i cili kapte zërin, duke përfshirë të gjitha telefonatat e bëra dhe të marra nga përdoruesi i terminalit.  *A ka pasur një kapje të paligjshme të të dhënave?*   * **Çështja**   *A ka pasur ndonjë kapje të të dhënave?*  *A është arritur kapja e të dhënave me mjete teknike?*  *A janë transmetuar të dhënat për ose nga sistemi kompjuterik?*   * **Pikat për diskutim**   “Key logger” është një pajisje teknike që kap të dhënat e transmetuara nga terminali. Kjo përbën kapje të të dhënave dhe është e dukshme që bëhet pa të drejtë.  Po telefonatat e bëra me programin Skype? Në këtë skenar duket që të dhënat udhëtojnë në të njëjtën linjë si të dhënat e tjera të transmetuara nga kompjuteri, por po sikur përdoruesi të kishte vetëm një telefon me programin Skype? A do të përbënte një sistem kompjuterik një telefon i tillë? Konventa e përkufizon “sistemin kompjuterik” si *çdo pajisje ose grup pajisjesh të lidhura ose të ndërlidhura, një ose më shumë prej të cilave, në përputhje me një program, realizon përpunimin e të dhënave; dhe “të dhëna kompjuterike” si çdo paraqitje faktesh, informacioni ose konceptesh në formë të përshtatshme për përpunimin në një sistem kompjuterik, duke përfshirë një program të përshtatshëm për të shkaktuar që një sistem kompjuterik të kryejë funksionin e tij.*  Përdorimi i pajisjes audio mund të jetë pak më i vështirë? A është “përgjim”? Në Mbretërinë e Bashkuar gjykatat kanë vendosur se që të ndodhë një përgjim duhet të ketë një farë ndërhyrjeje ose abstragim të sinjalit ndërkohë që është duke u transmetuar në rrjet; këtu regjistrimi ndodh në mënyrë të pavarur pavarësisht se i njëjti informacion do të merrej sikur pajisja të kishte qenë vendosur në “linjë”.  Po sikur pajisja “key logger” të vendosej në sistem nga Kompania, që të garantonte se punonjësit e saj nuk e përdorin Internetin për qëllime të papërshtatshme?  Shumica e sistemeve të telekomunikacionit janë edhe në rrjetet private edhe në ato publike. Në momentin që komunikimi largohet nga posedimi yt, ai zhvendoset nga një sistem privat tek një publik. Kontrollori i një sistemi privat ka të drejtën të aksesojë komunikimin duke përdorur atë sistem; kështu për shembull, ti do të ishe në gjendje të monitoroje bisedat në linjën e telefonit të shtëpisë me kusht që çfarëdo pajisje që do të përdorje të ishte e lidhur me anën private të sistemit.  Ky skenar është hartuar që pjesëmarrësit të shqyrtojnë secilin prej elementëve të kapjes së të dhënave, se ekziston kapja e të dhënave kompjuterike gjatë transmetimit të saj me mjete teknike dhe pa të drejtë.  Pjesëmarrësit duhet të jenë të qartë se kjo dispozitë është hartuar të mbrojë përmbajtjen e komunikimeve dhe jo informacionin e lidhur me adresimin e mesazhit ose koston e shërbimit. | |
| Slajdi 47 | 1. **Rasti Praktik 3**  * **Faktet / skenari**   Anëtarët e një bande kriminale komunikojnë ndërmjet tyre me anë të përdorimit të një sistemi të postës elektronike në Internet që mund të aksesohet kudo në botë. Në vend që t’i dërgojnë njëri tjetrit mesazhe që mund të kapen nga policia ose të cilat mund t’i inkriminonin ata nëse do të gjendeshin në kompjuterin e tyre, ata përdorin sistemin e mesazheve të përgatitura por të padërguara. Ajo që bëjnë ata është se i shkruajnë mesazhet dhe i ruajnë në folderin “Draft”, më pas pjesëtarët e tjerë të bandës kanë fjalëkalimin e asaj llogarie, me anë të të cilës futen në llogari dhe lexojnë mesazhin e lënë, dhe i kthejnë përgjigje duke përsëritur procedurën.  Sikur policia të ishte në gjendje të hynte në atë llogari dhe lexonte mesazhin, a do të përbënte kjo një kapje të paligjshme të të dhënave?   * **Çështjet**   *A po dërgohet mesazhi?*   * **Pikat për diskutim**   Shumica e shteteve i kërkojnë policisë të vendosë një kufi të lartë dyshimi përpara se të autorizojë kapjen e përmbajtjes së një komunikimi. Marrja e provave pa autoritetin e kërkuar mund të rezultojë në pushimin e çështjes ose papranueshmërinë e provave.  Kompjuterët dhe Interneti lehtësojnë një numër formash të ndryshme të komunikimit, p.sh. postën elektronike, mesazhet e menjëhershme, twitter, etj. Mesazhet do të ruhen shpesh përpara se të tërhiqen nga marrësi i synuar. A duhet të konsiderohet një mesazh i padërguar, i ruajtur në folderin “Drafts”, sikur është duke u transmetuar? Nuk ka asnjë mënyrë për të kuptuar nëse mesazhi i përgatitur është lexuar nga marrësi i synuar. A duhet ligji të ofrojë të njëjtën mbrojtje për ata që qëllimisht shkatërrojnë mjetet normale të komunikimit me postë elektronike si e ofron për ata që e përdorin postën elektronike siç u krijua të përdoret?  Kjo është një mënyrë mjaft e zakonshme për keqbërësit që të komunikojnë me njëri tjetrin. Nëse aksesimi i këtyre mesazheve është kapje të dhënash ose jo do të varet nga legjislacioni i brendshëm dhe/ose qëndrimi i gjykatave të brendshme por do të ishte me vlerë që pjesëmarrësit të kuptonin se nëse ata do të mbështeteshin tek Ndihma Juridike e Ndërsjellë për marrjen e këtyre të dhënave, shteti i kërkuar mund ta konsideronte atë një kapje të dhënash për arsye se kërkimi i aksesit në përmbajtjen e komunikimit do të kishte një prag më të lartë që do të duhej të përcaktohej me qëllim marrjen e autorizimit të nevojshëm gjyqësor. | |
| Slajdi 48 | 1. **Rast Praktik 4**  * **Faktet / skenari**   Oficeri i Policisë Bobi ka marrë telefonin e bashkëshortes së tij, ka gjetur fjalëkalimin dhe ka dëgjuar një mesazh zanor të ruajtur që ajo akoma nuk e ka tërhequr.  *A është kjo një kapje të dhënash?*   * **Çështjet**   A është mesazhi zanor duke u dërguar?  A ka ndodhur ndonjë kapje e të dhënave kompjuterike?   * **Pikat për diskutim**   Derisa mesazhi të mbërrijë në destinacion, është në fazën e dërgimit edhe pse është i ruajtur brenda sistemit. Mesazhi ka shumë mundësi të jetë i ruajtur në mënyrë dixhitale në serverin e kompanisë së telefonave dhe Bobi ka aksesuar të dhënat kompjuterike. A është telefoni një kompjuter? Me shumë mundësi, po, sepse realizon përpunimin e automatizuar të të dhënave. Oficerët e Policisë që kryejnë kontrolle, dhe që gjejnë telefona duhet të kenë parasysh këtë me qëllim që të sigurohen se e kanë autoritetin e nevojshëm për të aksesuar mesazhe të tilla. Do të ishte ndryshe sikur marrësi ta kishte dëgjuar mesazhin dhe të kishte zgjedhur ta ruante atë.  Ky skenar ngriti disa çështje të ngjashme me skenarin e mëparshëm. Ai shërben për të ilustruar se çfarë mund të ishte një situatë e zakonshme që mund të zbatohet njësoj për oficerët që ekzekutojnë një urdhër kontrolli, sekuestrojnë një kompjuter, që përmban mesazhe elektronike të lexuara dhe të palexuara. Ai shërben gjithashtu për të ilustruar se vepra penale e parashikuar nga Neni 3 zbatohet për të gjitha format e transferimit të të dhënave elektronike, pavarësisht nëse bëhet me telefon, faks, email ose transferim skedarësh. | |
| **Slajdi 49** | 1. **Rast Praktik 5**  * **Faktet / skenari**   Bobi është i interesuar për UFO-t dhe ai beson se Qeveria Ruse ka kapur një anije kozmike aliene që ka zbritur në Siberi në fillim të Shekullit 20. Ai viziton një uebsajt rekrutimi të Ushtrisë Ruse, i cili mban një link të një uebsajti të Forcave Ajrore Ruse. Uebsajti i Forcave Ajrore kërkon një fjalëkalim por duke përdorur një program për gjetjen e fjalëkalimit ai arrin të hyjë në uebsajt. Ai kalon pak kohë duke eksploruar sistemin dhe kopjon një numër skedarësh. Ai gjithashtu përpiqet të fshijë të gjithë skedarët e regjistruar të aktivitetit të tij me qëllim që mos identifikohet nga Rusët. Më pas ai modifikon faqen kryesore të uebsajtit në mënyrë që të shfaqë foton e një UFO-je në vend të Stemës së Forcave Ajrore.  *A ka kryer Bobi vepër të paligjshme?*   * **Çështjet**   A mund të jetë aksesi i paautorizuar vepër penale e Ndërhyrjes në Sistem ose tek të Dhënat?  A është vepër penale fshirja e provave të aksesit të paautorizuar?  A duhet të shkaktohet dëmtim i rëndë tek funksionimi i kompjuterit përpara se të ngarkohet përgjegjësia penale?   * **Pikat për diskutim**   Synimi i këtyre dispozitave është ofrimi i mbrojtjes për të dhënat dhe programet kompjuterike njësoj si mbrojtja që i ofrohet pronës fizike kundër shkaktimit të qëllimshëm të dëmit.    Bobi nuk ishte i autorizuar të hynte në uebsajtin e Forcave Ajrore, se ishte i mbrojtur me fjalëkalim. Për rrjedhojë aksesi do të përbënte veprën penale të aksesit të paligjshëm.    Bobi fshiu të dhënat, skedarët e regjistruar dhe stemën e Forcave Ajrore. Megjithëse ai ndoshta gjeneroi skedarë regjistrimi që nuk janë të tij, sistemi ishte i konfiguruar ta regjistronte një aktivitet të tillë. Ai nuk ka asnjë të drejtë t’i fshijë ato. Forcat Ajrore mund të duan të dinë se kush ka hyrë në sistemin e tyre.    Duke ndryshuar imazhin në faqen kryesore, ai edhe ka fshirë edhe ka shtuar të dhëna në sistem, gjë e cila, megjithëse nuk ka të ngjarë të ketë rezultuar në ndonjë humbje informacioni të rëndësishëm, do të ishte e sikletshme për Forcat Ajrore. Megjithatë, megjithëse Bobi mund të pretendojë se ai u fut në sistem për të gjetur informacion, dhe se ai i fshiu të regjistrimet ose të dhëna të tjera pa rëndësi, a mundet që administratori i sistemit të besojë tek integriteti i të dhënave pas një aksesi kaq të paligjshëm?  Nëse është kryer një vepër penale në këto rrethana do të jetë një çështje interpretimi. Mund të jetë që një prag serioz nuk është përcaktuar. Megjithatë, administratori i sistemit me siguri do të ndjehej i detyruar ta bënte të padisponueshëm uebsajtin me qëllim që të përcaktonte efektin e hyrjes së paautorizuar, veçanërisht nëse uebsajti i aksesuar përmbante të dhëna konfidenciale ose delikate ose është përdorur për veprime, të cilat nëse do të ishin të këqija do të rrezikonin publikun, si p.sh. sistemet përgjegjëse për funksionimin e një stacioni nuklear.  Nëse për hir të argumentit të themi se sistemi që Bobi aksesoi do të ishte ai i përdorur për të drejtuar një Stacion Nuklear, a do të ishin të mjaftueshme veprat penale të përcaktuara në Nenet 4 dhe 5 për të reflektuar seriozitetin e një ndërhyrjeje të tillë, e cila përbën një sulm kundër Infrastrukturës Kritike Kombëtare? | |
| Slajdi 50 | 1. **Rast Praktik 6**  * **Faktet/ skenari**   Një program automatik për spam-et dërgon mesazhe elektronike të pakërkuara për mijëra përdorues në të gjithë botën çdo ditë. Nëse mesazhi elektronik hapet, ai shkarkon programe kompjuterike në kompjuterin e përdoruesit që hap mesazhin. Programi nuk bën gjë që të prekë funksionimin e kompjuterit të përdoruesit, nuk merr të dhëna dhe as nuk i fshin ato e as nuk shkakton ndonjë dëmtim tjetër; megjithatë kjo gjë do të thotë se kompjuteri i përdoruesit tashmë është një “Zombi” dhe bën pjesë në një “Botnet”[[75]](#footnote-76), dhe që “kontrolluesi i rrjetit” mund ta përdorë atë për të bërë veprime të ndryshme.  *A është kryer ndonjë vepër penale në kundërshtim me Nenet 4 ose 5 nga personi përgjegjës për dërgimin e mesazheve elektronike spam?*   * **Çështjet**   A ka ndodhur ndonjë akses i paautorizuar në kompjuterin e përdoruesit?  A janë modifikuar të dhënat në kompjuterin e përdoruesit?  A i është shkaktuar ndonjë dëm kompjuterit të përdoruesit?   * **Pikat për diskutim**   Edhe pse nuk është shkaktuar asnjë dëmtim, programi kompjuterik i instaluar automatikisht shkakton modifikim të të dhënave në kompjuterin e përdoruesit. Ky modifikim nuk u autorizua sepse përdoruesit nuk iu dha asnjë paralajmërim ose nuk iu kërkua pëlqimi në ndonjë mënyrë për modifikimin e kompjuterit të tij. A është dërgimi i mesazheve elektronike Spam në vetvete i paligjshëm apo është thjesht bezdisje? A bëhet i paligjshëm vetëm kur ka një impakt negativ?  Po sikur mesazhi elektronik spam të përmbante një skedar bashkëngjitur dhe një ftesë për ta hapur skedarin me fjalët “Kjo do të të pëlqejë” ?  Do të ishte i diskutueshëm fakti se marrësi ka zgjedhur dhe ka dhënë pëlqimin për shkarkimin e të dhënave në kompjuterin e tij. Megjithatë realiteti është se çdo pëlqim që mund të jetë dhënë nuk ka qenë pëlqim i informuar. Megjithatë mund të thuhet se të gjithë ata që zgjedhin të hapin skedarë bashkëngjitur mesazheve elektronike nga dërgues të panjohur e marrin përsipër rrezikun vetë.  A përbën ndonjë ndryshim që përdoruesi nuk do t’ia dijë nëse kompjuteri i tij u bë pjesë e një Botnet-i ose jo ?    Ndërsa navigojmë në Internet, vizitojmë faqe interneti dhe shkarkojmë të dhëna pa i kushtuar shumë vëmendje natyrës së materialit që mund të futet në kompjuterin tonë por i besojmë emrave që uebsajtet i vënë vetes, emrave të skedarëve ose rezultateve të kërkimeve për të marrë vendimet tona. Të klikuarit mbi imazhin e zvogëluar të një fotoje për të nxjerrë imazhin e plotë të saj tregon një ndërgjegjësim për të dhënat që po kërkojmë të marrim dhe një aprovim të plotë të informuar në lidhje me natyrën e këtyre të dhënave. Nëse klikojmë në imazhin e zvogëluar të një makine dhe më pas shohim se imazhi i plotë që del është ai i një avioni, nuk do të thotë se kemi dhënë pëlqimin për marrjen e këtij rezultati të dhënash.    Zgjedhja për të hapur një link që të çon në një uebsajt do të rezultojë në shkarkimin e shumë të dhënave. Nëse uebsajti është i ligjshëm, të dhënat ka shumë të ngjarë të lidhen me përmbajtjen e uebsajtit, megjithëse një pjesë e tyre mund të jenë reklama të vendosura nga palë të treta. Përsëri kemi bërë një zgjedhje të informuar dhe kemi dhënë pëlqimin e nënkuptuar për marrjen e reklamave duke ditur se kjo është praktikë e zakonshme në Internet. Një praktikë e zakonshme në industrinë e Internetit është shkarkimi i të dhënave tek programi navigator i përdoruesit, si skedarët “cookies”[[76]](#footnote-77).  Skedarët Cookies kryejnë një shumëllojshmëri funksionesh duke përfshirë regjistrimin e historisë së navigimit në Internet të përdoruesit. Një përdoruesi i jepet opsioni të çaktivizojë funksionin e cookies në programin navigues të Internetit, a është një opsion i tillë i mjaftueshëm të nënkuptojë se përdoruesi e ka dhënë pëlqimin e tij për shkarkimin e të dhënave të tilla? | |
| Slajdi 51 | 1. **Rast Praktik 7**  * **Faktet / skenari**   Bobi është një ish oficer i policisë, i cili u pushua nga puna për përdorim të papërshtatshëm të sistemit kompjuterik të policisë. Ai vendos të hakmerret ndaj departamentit të policisë. Ai përdor një program për mesazhet elektronike, i cili i mundëson atij të dërgojë 70,000 mesazhe elektronike në orë në ish-departamentin e tij. Ai modifikon kokën e mesazhit elektronik që të duket sikur vjen nga një oficer drejtues i policisë, duke e gënjyer serverin e mesazheve elektronike të policisë të besojë se mesazhet vijnë nga një burim legjitim. Serveri i policisë nuk ishte në gjendje të përballonte volumin e trafikut dhe pushoi së funksionuari.  *A përbën kjo një vepër të ndërhyrjes në sistem?*   * **Çështjet**   *Dërgimi i një mesazhi elektronik ka të bëjë me aksesin ose tentativën për të hyrë në një sistem kompjuterik, në serverin e mesazheve elektronike*. Deri në çfarë niveli pronari i një serveri të tillë e autorizon një akses të tillë?  Nëse keni një adresë emaili, a nuk do të thotë kjo se i ftoni të tjerët t’ju dërgojnë mesazhe elektronike ?   * **Pikat për diskutim**   Çështja ka të bëjë me të drejtën. Bobi ka aksesuar një sistem dhe ka shkaktuar prishjen e sistemit me anë të futjes së të dhënave të shumta. Duke krijuar një adresë email-i, e cila është e aksesueshme nga publiku, pronari i adresës në mënyrë të nënkuptuar jep pëlqimin e tij për marrjen e mesazheve elektronike. Bobi mund të argumentojë se policia ka dhënë pëlqimin për marrjen e mesazheve. Bobi mund të argumentojë se policia ka dhënë pëlqimin për marrjen e secilin mesazh elektronik individual dhe se nuk është faji i tij që sistemit i mungon kapaciteti të përballojë kaq shumë mesazhe elektronike. Por a ka pasur pëlqim të dhënë? Pronari i një shtëpie i jep pëlqimin e nënkuptuar një postieri të sjellë letrat nëpërmjet kutisë së tij të postës, që i janë adresuar pronarit. Ka gjithashtu një pëlqim të nënkuptuar për marrjen e “junk mail”[[77]](#footnote-78) të tilla si fletushkat e picerive. Megjithatë, pronari nuk jep pëlqimin e marrjes së kaq shumë fletushkave saqë ai të mos jetë në gjendje të hapë derën e tij të jashtme.    A nuk mund të thuhet gjithashtu se duke ndryshuar detajet e dërguesit të mesazhit elektronik, është përfituar aksesi në serverin e email-eve me anë të mashtrimit? Pëlqimi nuk është dhënë për marrjen e këtyre “spoofed emails”[[78]](#footnote-79).  Megjithëse ky skenar ka të bëjë me mesazhet elektronike, parimi vlen për ata që tentojnë të shkaktojnë mosfunksionimin e uebsajteve nëpërmjet sulmit të mohimit të shërbimit, ku uebsajti nuk është në gjendje të përballojë volumin e trafikut të drejtuar tek ai. Lidhja me një uebsajt ka të bëjë me shkëmbimin e të dhënave ndërmjet kompjuterit të përdoruesit dhe uebsajtit. Çështje të ngjashme në lidhje me pëlqimin e nënkuptuar për tu lidhur me uebsajtet dalin gjatë diskutimeve në lidhje me mesazhet elektronike. | |
| Slajdi 52 | 1. **Rast Praktik 8**  * **Faktet / skenari**   Bobi dërgon një mesazh elektronik bashkëshortes së tij të zemëruar në vendin e saj të punës. Ai ndryshon kokën e mesazhit për ta bërë të duket sikur i ka ardhur mesazhi nga njëri prej miqve të saj. Mesazhi elektronik përmban një program të quajtur “akses në të gjitha zonat”, i cili i lejon Bobit të marrë kontrollin e kompjuterit të bashkëshortes së tij. Përpara se Bobi të ketë mundësi të përdorë programin, prezenca e programit kapet nga administratori i sistemit, i cili e mbyll sistemin me qëllimin për të bërë një vlerësim të nivelit të ndërhyrjes në të.    *A ka kryer vepër penale Bobi në kundërshtim me Nenin 5?*   * **Çështjet**   A ka shkaktuar Bobi një prishje të të dhënave të mbajtura në sistem?  A ka penguar Bobi funksionimin e sistemit kompjuterik?  A ishte prishja e të dhënave ose bllokimi i funksionimit të sistemit pa të drejtë?   * **Pikat për diskutim**   Reagimi i administratorit të sistemit ndaj mesazhit elektronik të Bobit do të thotë se shërbimi iu është mohuar përdoruesve të sistemit. Aksesi tek të dhënat e ruajtura në sistem për rrjedhim është ndërprerë, megjithëse kufizimi i aksesit ka të ngjarë të jetë i përkohshëm. Vepra nuk kërkon që të dhënat të jenë të padisponueshme në mënyrë permanente.    Kemi diskutuar shkallën në të cilën pronari i një adrese email-i jep pëlqimin për marrjen e të dhënave nga të tjerët.    Neni 5 ka të bëjë me sistemet kompjuterike, d.m.th një ose më shumë kompjuterë të lidhur së bashku. A është një kompjuter i vetëm i lidhur me Internetin pjesë e një sistemi?    Ka shumë të ngjarë se kompjuteri i punës i bashkëshortes së Bobit është pjesë e një sistemi, ajo ka të ngjarë të jetë pjesë e rrjetit LAN ose rrjetit WAN ose Intranetit. A e ka bllokuar Bobi funksionimin e sistemit?    Bobi mund të argumentojë se nuk është përgjegjës për mohimin e shërbimit dhe se nuk kishte aspak për qëllim të shkaktonte diçka të tillë, në fakt krejt e kundërta, ai dëshironte që sistemi të vazhdonte funksionimin në mënyrë që ai të mund të zbulonte se ç’po kurdiste bashkëshortja e tij. Shpesh sulmet e mohimit të shërbimit janë të pamjaftueshme për ta nxjerrë offline një uebsajt, megjithatë ofruesit e shërbimit të Internetit do ta nxjerrin uebsajtin offline me qëllim që të minimizojnë efektin e sulmit mbi sistemet dhe të minimizojnë problemet për klientët e tjerë.  Në këtë skenar Bobi nuk duket të ketë qëllimin e kërkuar për një vepër penale sipas Nenit 5, por kjo sigurisht nuk do të thotë se ai shpëton nga përgjegjësia penale.  Ky është një shembull i një virusi Trojan, i cili është një mënyrë e zakonshme që keqbërësit kibernetikë të hyjnë në kompjuterët e të tjerëve. | |
| Slajdi 53 | 1. **Rast Praktik 9**  * **Faktet / skenari**   Një grup ”hacktivist”[[79]](#footnote-80) në Internet që po proteston kundër përdorimit të kafshëve për testimin e produkteve të kozmetike ndërmarrin sulme të “Mohimit të Përhapur të Shërbimit” (DDOS) kundër uebsajteve të kompanive kozmetike dhe revistave “glamour”. Nëpërmjet uebsajtit të tyre, grupi shpërndan programe kompjuterike të quajtura ‘Supergun’, që i mundësojnë grupit të koordinojë sulmet mbi uebsajtet dhe të maksimizojë sasinë e trafikut që kërkon të aksesojë uebsajtet në një kohë të caktuar. Programi kompjuterik ‘Supergun’ u zhvillua fillimisht si mjet nga administratorët e sistemit për testimin e sigurisë së sistemeve të tyre. Megjithatë, megjithëse programi kompjuterik akoma funksionon në të njëjtën mënyrë, ndërfaqja e përdoruesit është bërë më e lehtë për tu përdorur dhe tani mban logon e grupit.  *A është vepër penale bërja e disponueshme e programit “Supergun” për tu shkarkuar?*  *A është vepër penale të kesh në posedim programin “Supergun”?*   * **Çështjet**   A do të thotë fakti që programi Supergun përdoret për një qëllim legjitim se ndjekja ligjore nuk mund të fillohet?  A përbën shpërndarje bërja e disponueshme e programit Supergun?   * **Pikat për diskutim**   Veprat penale të lidhura me këtë Nen janë: aksesi i paautorizuar, kapja e paligjshme e të dhënave, ndërhyrja tek të dhënat dhe në sistem.    Megjithëse programi kompjuterik në fillim ishte me përdorim të dyfishtë, d.m.th pati një funksion legjitim, tani që ndërfaqja e përdoruesit është modifikuar, a do të thotë kjo se posedimi i tij etj. është vepër penale?  Duke iu kthyer rasteve tona të mëparshme praktike, programi kompjuterik “akses në të gjitha zonat”, i përdorur nga Bobi për të përfituar aksesin në kompjuterin e bashkëshortes së tij ka një përdorim legjitim. Programe të tilla i lejojnë përdoruesve të aksesojnë kompjuterët e tyre nga larg.  Po posedimi nga Bobi i programit për gjetjen e fjalëkalimeve: a do ishte kjo një vepër penale? Mund të jetë çështje qëllimi, çfarë arsyeje legjitime mund të ketë ai që të posedojë një program të tillë? A ka ndonjë provë të tregojë se ai ka kërkuar të përdorë këtë program për të kryer vepër penale?  Kjo vepër penale nuk është krijuar të përdoret për të kriminalizuar përdoruesit dhe ofruesit e programeve legjitime. Me prova, siç ka këtu, të synimeve të këqija, problemi ndoshta nuk lind. Megjithatë ata që përfshihen në krimin kibernetik shpesh janë të përfshirë në aktivitete legjitime në Internet dhe shumë mirë mund të jenë profesionistë që përdorin dhe zhvillojnë programe të tilla, por kur shfaqet mundësia janë të përgatitur ta përdorin atë në mbështetje të aktivitetit të paligjshëm. Po pronarët e dyqaneve? Si mund ta dinë ata se çfarë qëllimesh mund të kenë klientët në lidhje me pajisje fizike ose programe kompjuterike? A mos është fusha e veprës penale shumë e vagullt? | |
| Slajdi 54 | 1. **Rast Praktik 10**  * **Faktet / skenari**   Një ofrues i programeve kompjuterike ka prodhuar programe për kodim. Programi e ndan përmbajtjen e njësisë së diskut të kompjuterit në dy volume, secila ka nevojë për fjalëkalim për akses në të, megjithatë vetëm një volum është i dukshëm për përdoruesin e zakonshëm dhe ekzistenca e volumit të fshehur nuk mund të zbulohet duke përdorur programe nga kriminalistika dixhitale që janë të disponueshme aktualisht.  Prodhuesit pretendojnë se ky program do të ishte i dobishëm për ata që mund ta gjejë veten në një situatë kur janë të detyruar ta tregojnë fjalëkalimin e tyre. Kjo do të thotë se të dhënat në volumin e fshehur mund të mbahen të sigurta edhe sikur fjalëkalimi i folderit të dukshëm të tregohet.   * **Çështjet**   A përbën vepër penale prodhimi, shpërndarja, përdorimi ose posedimi i një programi të tillë kompjuterik?   * **Pikat për diskutim**   Të gjithë vazhdimisht nxitemi që të mbajmë të sigurta të dhënat tona. Megjithëse një program i tillë në mënyrë të dukshme është i dobishëm për ata që përfshihen në vepra penale dhe në veçanti ata që kanë frikë se përmbajtja e kompjuterit të tyre mund t’i inkriminojë, programi nuk po përdoret për të kryer një vepër penale por po përdoret për të fshehur provat.  Kriminelët kibernetikë mund të shfrytëzojnë programet dhe sistemet e tjera për të evituar zbulimin duke përfshirë anonymizers[[80]](#footnote-81), të cilët iu mundësojnë atyre të navigojnë në Internet pa e zbuluar adresën IP të tyre ose programet e quajtura “evidence eliminator”, të cilat fshijnë të gjithë përmbajtjen e diskut të ngurtë të kompjuterit. | |
| Slajdi 55 | 1. **Rasti Praktik 11**  * **Faktet / skenari 3**   Niku punon në departamentin IT të një kompanie të madhe, e cila ka intranetin e saj. Politika e kompanisë i ndalon punonjësve të saj të përdorin kompjuterin e kompanisë dhe lidhjen e Internetit për të bërë blerje online. Në kohën e lirë, Niku fillon të zhvillojë programe kompjuterike, që do t’i mundësojnë atij të identifikojë ata punonjës që bëjnë blerje online dhe ta kapë atë informacion në mënyrë që të përdoret si provë në procedimet disiplinore për ata punonjës. Nikut i mungojnë aftësitë e nevojshme dhe kontakton online “Jupiterin”. Së bashku ata bëjnë një program kompjuterik, që kur është i instaluar në kompjuterin e përdoruesit do të aktivizohet kur ai përdorues do të fillojë të plotësojë një formular online si ata që përdoren për të realizuar pagesat online dhe do të kapë të dhënat e futura nga përdoruesi. Kompania e Nikut është shumë e kënaqur ndërsa Jupiteri fillon të shpërndajë programin duke përdorur një program Trojan.  *A ka kryer Niku vepër penale?*  *A ka kryer kompania vepër penale?*  *A ka kryer Jupiteri vepër penale?*   * **Çështjet**   A është krijuar ose përshtatur pajisja kryesisht për qëllime të kryerjes së veprave penale të përcaktuara?   * **Pikat për diskutim**   Kriminelët kibernetikë janë në gjendje të përdorin një shumëllojshmëri mjetesh që i mundësojnë atyre kryerjen e veprave penale ose që do t’i ndihmojnë ata në kryerjen e tyre. Është plotësisht e mundur të blihet kodi, që do të mundësojë ndërtimin e “bot-it” tënd ose të blihet një “botnet” ose të blihet aksesi në një botnet, që do t’i mundësojë përdoruesit të ndërmarrë një sërë veprash të paligjshme të tilla si “phishing”.  Jupiteri do ta përdorë këtë program për të marrë të dhëna financiare nga përdoruesit, që më pas mund të shfrytëzohen ose nga vetë Jupiteri ose të tjerët. Kompania mendoi se Niku e kishte prodhuar këtë gjatë kohës së tij të punës. Niku është i pafajshëm dhe pa dashje ka ndihmuar Jupiterin të krijojë një mjet të fuqishëm kriminal. As Niku e as Kompania nuk e kanë qëllimin kriminal të kërkuar. A do të ishte ndryshe sikur Jupiteri të hidhte në treg programin për kompani të tjera, që do të dëshironin të monitoronin aktivitetin në Internet të punonjësve të tyre? A mund të argumentojë Jupiteri se programi kompjuterik ka një qëllim legjitim pavarësisht se është tërheqës për keqbërësit? | |
| Slajdi 56 | 1. **Rast Praktik 12**  * **Fakt / Skenari**   Stefani përdor një program kompjuterik për fotografitë të disponueshëm në treg për të prodhuar çeqe bankare reale në kompjuterin e tij të shtëpisë. Ai e çon çekun në bankë. Banka e pranon atë si të vërtetë dhe transferon fonde në llogarinë e tij.  *Çfarë vepre penale ka kryer Stefani?*   * **Çështjet**   A është prodhimi i çeqeve bankare të rreme një falsifikim kompjuterik?  A është vepra penale e kryer sapo nëpunësi i bankës e pranon çekun si të vërtetë?   * **Pikat për diskutim**   Krijimi i çeqeve bankare ka të bëjë me futjen e të dhënave joautentike në kompjuter, d.m.th. që çeku është bërë në emër të Stefanit. Megjithatë, a është bërë kjo pa të drejtë apo ka të drejtë Stefani të prodhojë një dokument të tillë në kompjuterin e tij? Stefani mund të ketë qëllimin të përdorë çekun të mashtrojë bankën, por për njëfarë arsyeje nuk mund ta printojë çekun. A ka ndonjë ndryshim përsa i takon përgjegjësisë së Stefanit nëse dokumenti i përgatitur në kompjuter printohet në letër?  Kjo vepër nuk u krijua të trajtojë këtë skenar por mund të shërbejë nëse legjislacioni i brendshëm nuk do ta kriminalizonte prodhimin e çeqeve bankare të falsifikuara. Këto vepra penale mund të shqyrtohen më mirë në drejtim të përgjegjësisë sekondare, si p.sh. tentativa.  Kjo vepër penale është në fakt për ata që përdorin kompjuterin si mekanizëm për të kryer një vepër të paligjshme, pra, kur vepron në mirëbesim punonjësi i bankës fut të dhënat e dhëna nga Stefani duke pranuar se ato janë autentike. | |
| Slajdi 53 | 1. **Rast Praktik 13**  * **Faktet / skenari**   Stefani është mburrur gjithmonë tek miqtë e tij për aftësitë e tij si atlet kur ishte adoleshent. Miqtë e tij janë skeptikë. Ai arrin të hyjë në bazën e të dhënave të shkollës së tij të vjetër dhe të ndryshojë rekordet për ta treguar atë kapiten të skuadrës atletike të shkollës dhe atë që fiton një numër medaljesh.  *A është kjo vepra penale e falsifikimit me anë të kompjuterit?*   * **Çështjet**   Të dhënat e modifikuara nuk do të përdoren për ndonjë qëllim ligjor.   * **Pikat për diskutim**   Stefani ka ndryshuar të dhënat dhe ka futur të dhëna jo autentike. Është e qartë se ky akses dhe modifikimet janë pa të drejtë. Duke lënë mënjanë veprat e tjera që mund të ketë kryer Stefani, nuk është e sigurt nëse ai ka kryer mashtrim me anë të kompjuterit sepse këto të dhëna nuk do të përdoren për qëllime ligjore.  Vepra e mashtrimit me anë të kompjuterit nuk ka të bëjë me përfitime financiare ose përfitime të tjera; këto vepra janë të përfshira në fushën e mashtrimit të lidhur me kompjuterin. Ky Nen kërkon të garantojë sigurinë dhe qëndrueshmërinë e të dhënave elektronike, të cilat mund të kenë pasojë për marrëdhëniet ligjore. Termi “për qëllime ligjore” tregon transaksionet dhe dokumentet, që kanë lidhje nga ana ligjore. | |
| Slajdi 58 | 1. **Rast Praktik 14**  * **Faktet / skenari**   Tani që ka humbur punën në Forcat e Policisë dhe i duhet të paguajë detyrimin ushqimor për bashkëshorten e tij, që nga divorci Bobi po kërkon një mënyrë tjetër sesi të bëjë para. Ai gjithmonë ka pasur interes për tu marrë me aksionet dhe blen 100 aksione të Kompanisë Flanders Mining Inc, e cila është një kompani me një të drejtë ekskluzive për nxjerrjen e uraniumit në Belgjikë për 1 euro copa. Bobi është anëtar i një forumi në Internet, anëtarët e të cilit, si Bobi, janë të interesuar në tregun e aksioneve. Bobi poston një mesazh ku thotë se një mik i tij në qeverinë Belge i ka thënë se janë zbuluar në Belgjikë sasi të konsiderueshme të uraniumit. Pas këtij mesazhi, çmimi i aksioneve për kompaninë Flanders Mining rritet, nga fundi i javës secili aksion ka kapur vlerën e 1000 eurove. Bobi më pas i shet aksionet e tij.  *A ka kryer Bobi ndonjë vepër të paligjshme?*   * **Çështjet**   A është i pavërtetë mesazhi i Bobit?  Nëse mesazhi ishte i pavërtetë, a ka humbur ndonjë njeri pasurinë për këtë shkak?    A ka fituar Bobi ndonjë avantazh ekonomik?   * **Pikat për diskutim**   Nëse mesazhi i postuar nga Bobi është i pavërtetë, atëherë ai mund të ketë kryer një vepër të paligjshme. Ai ka futur të dhëna të rreme në një kompjuter dhe ka pasur një përfitim ekonomik për vete në rritjen e çmimit të aksioneve.  A është lidhja shkakësore ndërmjet futjes së të dhënave dhe efektit shumë e largët?  A i ka shkaktuar Bobi humbje ndonjë njeriu? Ndoshta po, në faktin se aksionet janë të vlerësuara në mënyrë jo korrekte dhe në njëfarë pike do të bien. Megjithatë, duhet të pranohet se tregu i aksioneve është jashtëzakonisht i paqëndrueshëm, a nuk është vlera e një aksioni çmimi që kushdo është i gatshëm të paguajë në çdo kohë?? A është mashtruar vërtet ndonjë njeri, a nuk është Interneti i mbushur me këto lloj thashethemesh dhe mesazhesh? A do t’i besojë vërtet ndonjë njeri atij mesazhi apo nuk do të arrijë ta shohë si përpjekje e trashë për të manipuluar çmimin e aksioneve? A do të thotë kjo se nuk mund të themi gënjeshtra në Internet? | |
| Slajdi 59 | 1. **Rasti Praktik 15**  * **Faktet / skenari**   Stefani shkon në bankë me makinë. Tek parkimi ai mëson se nuk ka para të holla. Ai vendos një rondele në makinën automatike të parkimit dhe merr një biletë.  *A ka kryer Stefani një vepër të paligjshme?*   * **Çështjet**   A është makina automatike e parkimit një kompjuter?  A ka rëndësi që makina automatike e parkimit prodhon bileta automatikisht dhe asnjë njëri nuk është mashtruar?  Cili është statusi i biletës së parkimit?   * **Pikat për diskutim**   Makina automatike e parkimit është kompjuter, ajo përpunon të dhënat duke llogaritur shumën e parave përkundrejt tarifës së parkimit dhe lëshon një biletë për një periudhë të përshtatshme kohe. Stefani ka futur të dhëna jo autentike, rondelën në vend të monedhës së përshtatshme. Neni 7 nuk kërkon që personi të ketë vepruar mbi të dhënat e futura.  Bileta e parkimit është falsifikim, të dhënat e përdorura për ta krijuar atë ishin false dhe ajo u prodhua me qëllim që një person, një punonjës i parkimit të makinave ta konsideronte atë si autentike dhe të mos i jepte Stefanit një biletë parkimi. | |
| Slajdi 60 | 1. **Rast Praktik 16**  * **Faktet / Skenari**   Mbas arrestimit të tij policia zbuloi se Stefani është në posedim të të dhënave të kartave të kreditit që i përkasin një numri të madh të palëve të treta.  *A është posedimi i këtyre të dhënave vepër penale?*   * **Çështjet**   Çfarë statusi kanë skedarët e kompjuterit? A janë ato “sende” në ligj pavarësisht nga fakti se ato përbëhen nga një varg kodesh binar?   * **Pikat për diskutim**   Në Mbretërinë e Bashkuar është vepër penale materiale të jesh në posedim të një sendi për ta përdorur për mashtrim. Sendi e përfshin një skedar kompjuteri. Sigurisht që është e nevojshme të provohet qëllimi por është e vështirë të argumentosh se ke pasur një arsye legjitime të kesh në posedim të dhëna të këtij lloji.  Mund të jetë që kjo mund të konsiderohet si një fazë përgatitore e veprës penale. | |
| Slajdi 61 | 1. **Rasti Praktik 17**  * **Faktet / skenari**   Adami është anëtar i një grupi ekskluziv online, i cili shkëmben fotografi të fëmijëve që abuzohen seksualisht. Adami është gjithashtu anëtar i një grupi “peer to peer” që shkëmben skedarë, ai vendos foto të fëmijëve që abuzohen që ka marrë nga grupi online në folderat e tij të ndarë me përdorues të tjerë të grupit “peer to peer”, për t’i bërë të aksesueshme për të tjerët.  *Çfarë vepre penale ka kryer Adami?*   * **Çështjet**   Përkufizimet e prodhimit, gjetjes dhe shpërndarjes.  Adami ka shkarkuar skedarë imazhesh nga Interneti. A është i barabartë shkarkimi me prodhimin e një imazhi të tillë? Shkarkimi, dhe veçanërisht ruajtja e një imazhi në një kompjuter nuk është si të shikuarit Televizor. Akti i shkarkimit krijon një gjë të re, një skedar kompjuteri, pra shikimi i imazheve në Internet do të thotë krijimi i imazheve të reja. Prokurorët mund ta gjejnë shumë të dobishëm këtë koncept.  Rrjetet Peer to Peer për shkëmbimin e dosjeve i lejojnë anëtarëve të tyre të kenë akses tek skedarët duke i bërë ato të disponueshëm nga anëtarë të tjerë të rrjetit. Duke vendosur imazhet në folderat e përbashkët, Adami po i bën të disponueshëm për shpërndarje. | |
| Slajdi 62 | 1. **Rasti Praktik 18**  * **Faktet / skenari**   Billi është arrestuar në aeroport në kthim nga Kamboxhia. Në Laptopin e tij u gjetën një numër i madh imazhesh të atij vetë të angazhuar në aktivitet seksual me fëmijë që duket të jenë nga Azia Juglindore.  *A mundet Billi të ndiqet ligjërisht në lidhje me imazhet?*   * **Çështjet**   Juridiksioni.  Zgjedhja e veprës penale materiale, posedimi i imazhit ose bërja e imazhit.   * **Pikat e diskutimit**   Mund të ketë çështje juridiksionale në lidhje me bërjen e imazheve se këto duken të jenë prodhuar jashtë shtetit.  Posedimi nuk duhet të jetë problem.  Cila do të ishte pozita sikur të gjitha imazhet të ishin gjetur në një vend të pacaktuar?  Posedimi kërkon edhe dijeninë edhe kontrollin. Billi mund të dijë ose mund të mos e dijë që imazhet që fshihen prapëseprapë mund të aksesohen në njësinë e diskut të kompjuterit, megjithatë po të mos ketë ekspertizën dhe mjetet teknike ai nuk do të jetë kurrë në gjendje ti rikuperojë ato. Megjithatë, (në varësi të çështjeve juridiksionale) i mbetet prokurorit ose ta procedojë për bërjen e imazhit ose për posedimin e imazheve në shkuarën.  Cili do të ishte pozicioni, nëse imazhet të ishin me fëmijë nudo të moshave 3-7 vjeç duke luajtur në plazh dhe Billi të shpjegonte se ai është një natyrist por pranon se ai merr kënaqësi seksuale nga shikimi i imazheve?  Nëse imazhe të tilla janë të paligjshme është çështje për interpretim lokal. Në Mbretërinë e Bashkuar zakonisht duhet që imazhet të kenë një element seksual dhe ne do ta konsideronim motivin e fotografuesit pa lidhje.  *Kush vendos se cili imazh është i paligjshëm? A është ambienti i veprës penale mjaftueshmërisht i qartë?* | |
| Slajdi 63 | 1. **Rasti Praktik 19**  * **Faktet / skenari**   WWW.Iuvfishin.com është një Uebsajt i kushtuar peshkimit. Uebsajti mbahet në serverat e ndodhur në SHBA. Pronarët e uebsajtit zbulojnë se uebsajti është aksesuar në mënyrë të paligjshme dhe se një mijë imazhe të abuzimit seksual me fëmijë janë futur dhe vendosur në uebsajt. Mënyra sesi është realizuar do të thotë se këto imazhe nuk do të ishin të dukshme për përdoruesit e zakonshëm të uebsajtit. Uebsajti regjistron adresat IP të atyre që i kanë aksesuar fotografitë.  Një adresë IP që i përket Xhonit i është dhënë policisë në vendin tuaj. Ata kontrollojnë adresën e Xhonit dhe sekuestrojnë kompjuterin e tij, i cili përmban mijëra imazhe të abuzimit të fëmijëve. Është e qartë nga historia e Internetit dhe të dhënave brenda këtyre skedarëve se shumica e imazheve janë shkarkuar nga Interneti.  Çfarë vepre penale ka kryer Xhoni?   * **Çështjet**   Si të provohet se Xhoni është përgjegjës për imazhet?  Impakti mbi të dyshuarit e akuzuar për vepra penale pedofilie**.**   * **Pikat për diskutim**   Kjo metodë e fshehjes së imazheve nuk është e pazakontë. Grupet postojnë linke për tek imazhet. Megjithatë, mund të jetë e rrezikshme të mbështetesh vetëm tek adresa IP për të marrë një urdhër arresti pa kuptuar se si ajo adresë IP është regjistruar në uebsajt. Ata mund të jenë futur në atë uebsajt në mënyrë krejt të pafajshme, duke u dërguar nga një uebsajt tjetër dhe të mos kenë shkuar për të aksesuar imazhet kur e kuptuan se çfarë ishin ato. Sigurisht ata mund ta kenë vizituar në më shumë se një rast, ose mund të kenë aksesuar një numër imazhesh.    Kjo mund të përdoret për të diskutuar kujdesin që duhet përpara akuzimit të një individi si pedofil. Ka një përqindje të lartë të vetëvrasjeve të personave që akuzohen për vepra të tilla penale. Si me të gjitha çështjet e krimit kibernetik, duhet që i dyshuari të ketë qenë në tastierë në kohën e duhur; një adresë IP mund të jetë përdorur nga një numër individësh në të njëjtën adresë ose rrjeti kompjuterik mund të ketë qenë rrëmbyer nga dikush tjetër. Akuzat e këtij lloji mund të kenë një efekt shkatërrues tek një individ i pafajshëm. | |
| Slajdi 64 | 1. **Rasti Praktik 20**  * **Faktet / skenari**   Policia në SHBA ka mbyllur një uebsajt që hostonte uebsajte që ofronin imazhe të abuzimit me fëmijët për ata që paguanin një tarifë mujore. Autoritetet amerikane kanë kapur të dhëna nga ata që kanë paguar për akses, duke përfshirë adresën IP, numrat e kartave të kreditit, adresat e postës elektronike, adresat bankare dhe fjalëkalimet. Një prej klientëve është Osvaldi. Me marrjen e urdhrit të kontrollit kompjuteri i tij u ekzaminua. Asgjë inkriminuese nuk u gjet sepse Osvaldi kishte përdorur një program të quajtur “Elimination of Evidence”  *A ka kryer vepër penale Osvaldi?*   * **Çështjet**   A ka kryer Osvaldi një vepër penale materiale apo një vepër me përgjegjësi dytësore? A ka çështje problematike me juridiksionin?    A ka rëndësi se uebsajti amerikan ishte plotësisht i automatizuar?    Çfarë mund të themi për përdorimin e programit “Evidence Elimination”?   * **Pikat për diskutim**   Osvaldi nuk është në posedim të ndonjë imazhi dhe ne nuk mund të provojmë se ai ka aksesuar ndonjëherë ndonjë uebsajt për të parë imazhe të tilla, megjithatë ne mund të provojmë se ai ka paguar një tarifë për ta bërë këtë. Megjithatë Osvaldi ka paguar para për të bindur një person tjetër, pronarin e uebsajtit në SHBA të shpërndante ose bënte të disponueshme imazhe të abuzimit seksual të fëmijëve për shpërndarje. Për rrjedhim a përbën kjo një vepër penale?  Që uebsajti amerikan është i automatizuar do të thotë se asnjë njeri nuk është angazhuar në përpunimin e detajeve të kartave të kreditit. Megjithatë, procesi është krijuar dhe administrohet e mirëmbahet nga një person, i cili përfiton financiarisht.  Përdorimi i një programi për eliminimin e provave nuk është në vetvete i paligjshëm. Përveç rastit kur Osvaldi mund të ketë qenë në gjendje ta aktivizonte programin gjatë hetimit të policisë, ai nuk ka të ngjarë të ketë kryer ndonjë vepër penale që lidhet me administrimin e drejtësisë. Megjithatë, nëse Osvaldi ndiqet ligjërisht, përdorimi i këtyre programeve mund të konsiderohet si rrethanë rënduese nga gjykata. | |
|  | Ushtrime Praktike **(sipas rastit)**  Për këtë sesion nuk është përgatitur asnjë ushtrim praktik. | |
|  | Kontrolli i njohurive  Trajneri duhet të kontrollojë njohuritë me anë të bërjes së pyetjeve përkatëse nga secili aspekt i sesionit. | |
| **Slajdet 65 dhe 66** | Përmbledhje    Trajneri duhet të bëjë përmbledhjen/testimin e njohurive për çështjet e mëposhtme:     * Dispozitat e ligjit penal material dhe disa prej faktorëve kyç të përdorur për përshkrimin e veprave penale, bazuar në Konventën e Budapestit. * Dispozitat e ligjit penal material dhe disa prej faktorëve kyç të përdorur për përshkrimin e veprave penale, bazuar në ligjin e brendshëm ekzistues. * Nevojat dhe avantazhet e harmonizimit ndërmjet legjislacionit të brendshëm dhe instrumenteve ndërkombëtarë, në veçanti Konventa e Budapestit. * Dispozitat përkatëse të ligjit material nga diskutimet e rasteve praktike | |

|  |  |  |
| --- | --- | --- |
| Mësimi 1.2.4 Ligji procedural i brendshëm | | **Kohëzgjatja: 90 Minuta** |
| **Burimet materiale të nevojshme:**   * Kompjuter Laptop ose Kompjuter Tavoline me Windows 7 dhe me Programin Office 2010 * Projektor * Prezantim me Power Point | | |
| **Synimi:**  Synimi i këtij sesioni është prezantimi i pjesëmarrësve të secilit vend me masat hetimore të parashikuara nga ligji i brendshëm dhe rregullat kombëtare për provat elektronike. | | |
| **Objektivat:**  Në përfundim të mësimit, pjesëmarrësit do të jenë në gjendje të:   * Identifikojnë rregullat kombëtare për provat elektronike * Identifikojnë masat hetimore të lejuara sipas ligjit kombëtar dhe vlerën dhe kriteret e mbledhjes dhe ruajtjes së provave elektronike * Identifikojnë disa specifika të procedimit kombëtar, përsa i takon provave elektronike, në kontekst të skenarit të kuadrit ligjor ndërkombëtar | | |
| **Hyrje**  Ky sesion është përgatitur t’ju japë pjesëmarrësve një shembull sesi konventa e Budapestit është integruar në legjislacionin e brendshëm të një vendi, në këtë rast të Portugalisë. Trajnerët do të duhet të zëvendësojnë të dhënat nga Portugalia me detajet legjislative përkatëse për vendin e tyre. | | |
| **Slajdi nr.** | **Përmbajtja:** | |
| Slajdet 1 deri 29 | Prezantim me PowerPoint (ose lloje të tjera prezantimesh)  Përmbajtja e slajdeve në këtë seksion është një shembull i asaj që mund të përshkruhet në secilin prej trajnimeve lokale.  Idealisht, sesioni për provat elektronike duhet të përmendë instrumentet ligjorë ndërkombëtarë të nënshkruar dhe të ratifikuar nga secili Shtet dhe rezultatin e transpozimit të tij në të drejtën e brendshme.  Krahas kësaj, duhet të jepet një përshkrim i llojeve të masave hetimore të parashikuara në ligjin e brendshëm, si dhe një shpjegim i rëndësisë dhe kritereve të mbledhjes dhe ruajtjes së provave elektronike.  Sipas rastit, në fund duhet të përmenden specifikat eventuale të procedimeve kombëtare në lidhje me provat elektronike. | |
| Slajdet 2 | Axhenda  Ky prezantim ka tre pjesë:   * Pjesa e Parë do t’i referohet dispozitave procedurale të Konventës së Budapestit; * Pjesa e Dytë do të japë një përshkrim të dispozitave procedurale sipas ligjit kombëtar; * Pjesa e Tretë do të japë një përmbledhje të dy pjesëve të mëparshme. | |
| Slajdi 3 | Në fund të këtij sesioni, pjesëmarrësit do të jenë në gjendje të shpjegojnë dispozitat procedurale të Konventës së Budapestit dhe të shpjegojnë dispozitat procedurale ekzistuese sipas ligjit të brendshëm. | |
| Slajdi 5 | Pjesa e Parë – Dispozitat procedurale të Konventës së Budapestit  Një nga aspektet më të rëndësishme të Konventës, që duhet të nënvizohet me forcë, është dimensioni i saj procedural. | |
| Slajdi 6 | Neni 14 i hap një fushëveprimi shumë të gjerë Konventës së Budapestit. Sipas ti, Konventa do të jetë e zbatueshme – në mënyrë evidente – kur vepra penale të jetë një nga ato të renditura në Konventë.  Megjithatë, ajo përfshin dy zgjatime jashtëzakonisht përfshirëse:     * Rregullat procedurale mund të përdoren në hetimin e veprave penale nëse janë kryer me anë të një sistemi kompjuterik; * Rregullat gjithashtu zbatohen për mbledhjen e provave elektronike në lidhje me çdo vepër penale. Kjo do të thotë se çdo vepër penale përfshihet në rregullat procedurale të Konventës për Krimin Kibernetik. | |
| Slajdet 7 deri 10 | Nenet 16 dhe 17 përshkruajnë ruajtjen e përshpejtuar të të dhënave kompjuterike dhe ruajtjen e përshpejtuar dhe zbulimin e të dhënave kompjuterike. Të dy dispozitat janë shumë inovative dhe jashtëzakonisht domethënëse.  Pjesët tradicionale të provave do të qëndrojnë në skenën e krimit, eventualisht, për periudha më të gjata kohe, por të dhënat dixhitale – provat elektronike – janë shumë të paqëndrueshme dhe mund të zhduken shumë shpejt.  Për rrjedhim, neni 16 e përcakton “ruajtjen e përshpejtuar” si një masë të menjëhershme provizore për mbajtjen e provave dhe jep kohë për marrjen e urdhrave gjyqësorë për sekuestrimin ose zbulimin e të dhënave. Këto mund të jenë të dhëna të trafikut të informacionit ose të dhëna për përmbajtjen.  Një komunikim në Internet mund të mos përfshijë një por disa shërbimofrues. Është e rëndësishme që zbatuesit e ligjit të jenë në gjendje të urdhërojnë çdo kompani shërbimofruese të Internetit përgjatë komunikimeve me të që ajo të ruajë të dhënat e dëshiruara. Për këtë arsye, sipas Nenit 17, një kompani shërbimofruese mund të urdhërohet të zbulojë një sasi të mjaftueshme për të dhënat e trafikut për përcaktimin e rrugës së komunikimit.  Nenet 16 dhe 17 tregojnë të dhëna specifike të nevojshme në një hetim specifik. Këto nuk duhet të ngatërrohen me rregullat e mbajtjes së të dhënave që i kërkojnë shërbimofruesve të Internetit të mbajnë të gjitha të dhënat e trafikut për një periudhë të caktuar kohe në rast se nevojiten nga autoritetet e zbatimit të ligjit. Konventa e Budapestit nuk ka një dispozitë të tillë për ruajtjen e të dhënave. | |
| Slajdet 11 deri 13 | Përcaktimet e Nenit 18 janë gjithashtu shumë interesante. Sipas tij, secila Palë duhet të miratojë masa legjislative për t’iu dhënë kompetenca autoriteteve të zbatimit të ligjit me mundësinë e dhënies së “urdhrave të prodhimit”. Ky urdhër gjyqësor mund të lëshohet nga organet e zbatimit të ligjit për qytetarët dhe për kompanitë shërbimofruese të Internetit, me anë të të cilit i urdhërojnë ata t’iu japin autoriteteve kompetente të dhënat e ruajtura në sistemin kompjuterik, në përgjegjësinë e tyre ose të japin të dhënat e abonimit.    Sipas Konventës, urdhri i prodhimit duhet të specifikojë natyrën dhe nivelin e të dhënave të kërkuara: është shumë e qartë se të dhënat e kërkuara nga hetimi duhet të përcaktohet paraprakisht; për këtë arsye janë të ndaluara *ekspeditat e peshkimit*. Qëllimi i këtij kufiri ligjor është parandalimi i abuzimit me këto kompetenca të reja investigative nga ana e punonjësve të zbatimit të ligjit. Në botën reale, një kontroll ose sekuestrim objektesh ose dokumentesh zakonisht i drejtohet vetëm objekteve ose dokumenteve që janë direkt të lidhura me një çështje në hetim. Në botën dixhitale, nëse rregulli ishte lejim i plotë i aksesit tek i gjithë informacioni që vjen me një pjesë fizike të kompjuterit, do të lejohej që të të aksesoheshin të gjitha llojet e informacionit të ruajtur në atë kompjuter, shpesh të palidhura me veprën penale në hetim dhe (p.sh. në rastin e komunikimit me postë elektronike) duke përfshirë gjithashtu edhe palë të treta.    Nëse Neni 16 është hapi i parë (ruajtja e të dhënave), Neni 18 është hapi i 2-të kur të dhënat e ruajtura duhet t’ju bëhen të ditura autoriteteve. | |
| Slajdet 14 deri 19 | Kontrolli dhe sekuestrimi përshkruhet në Nenin 19 të Konventës së Budapestit.  Shumica e rregullave procedurale kombëtare përfshijnë rregulla të përgjithshme për kontrollin dhe sekuestrimin, por jo të gjitha kanë rregulla specifike që rregullojnë kontrollin dhe sekuestrimin kompjuterik. Shumë juridiksione mund të ecin mirë vetëm me kontrollet dhe sekuestrimet tradicionale. Megjithatë, bota reale tregon se hetimet dixhitale përballen me sfida të panjohura më parë të shkaktuara, për shembull, nga ndërlidhja e sistemeve kompjuterike.  Duke pasur këto çështje të reja, Konventa e Budapestit krijoi rregulla specifike për të trajtuar kontrollet dhe sekuestrimet në botën dixhitale.  Për shembull, ka një rregull specifik në Nenin 19.2, që lidhet me shtrirjen hipotetike të një kontrolli kur, gjatë kontrollit të një sistemi kompjuterik, hetuesit konkludojnë se ka nevojë që ai kontroll të shtrihet edhe tek një sistem kompjuterik tjetër. Sipas Konventës, kur një autoritet fiton në mënyrë të ligjshme aksesin tek një sistem kompjuterik specifik ose pjesë e tij, dhe gjatë inspektimit të këtij sistemi formon një besim të arsyeshëm se të dhënat e kërkuara ruhen në një sistem kompjuterik tjetër në territorin e tij, ai autoritet mund ta shtrijë “në mënyrë të përshpejtuar” kontrollin edhe tek sistemi tjetër kompjuterik.    Më specifikisht në lidhje me sekuestrimet, ka disa çështje konkrete që duhet të nënvizohen sepse ato janë tipike për mjedisin e ri dixhital: mundësitë e sekuestrimit fizik të të dhënave kompjuterike.  Meqenëse shumica e legjislacioneve kanë rregullime specifike për kontrollet në botën fizike, ata nuk kanë rregulla të posaçme për mënyrat e reja dhe me efektive për sekuestrimin e të dhënave kompjuterike.  Në veçanti, Konventa e Budapestit kërkon që shtetet nënshkruese të miratojnë legjislacion që iu lejon atyre që gjatë procesit të një sekuestrimi ligjor të të dhënave kompjuterike të:   * 1. Sekuestrojnë fizikisht një sistem kompjuterik,   2. Bëjnë dhe ruajnë një kopje të të dhënave kompjuterike (që është e rëndësishme në rast se të dhënat ruhen në serverin kryesor, ku është e pamundur eliminimi fizik dhe gjithashtu ku sekuestrimi fizik do të ndërhynte në mënyrë të konsiderueshme tek të drejtat e njerëzve të tjerë që kanë të drejtën e aksesit në atë server – për shembull serveri i një kompanie të madhe)   3. Ruajtja e integritetit të të dhënave kompjuterike të ruajtura, dhe, së fundi, t’i   4. Bëjnë të paaksesueshme ose të eliminojnë ato të dhëna kompjuterike në sistemin kompjuterik të aksesuar.   Kjo dispozitë e fundit është për shembull për rastin kur sekuestrimi fizik është i pamundur, por do të ndodhte dëm real nëse një palë e tretë do të kishte akses në ato të dhëna.  Me përjashtim të sekuestrimit të thjeshtë të të dhënave kryesisht dhe regjistrimit origjinal, të gjitha këto mundësi procedurale janë masa specifike nga mjedisi dixhital. | |
| Slajdi 20 | Nganjëherë, hetuesi ka nevojë më tepër për informacionin më të fundit, sesa informacionin e ruajtur në një sistem kompjuterik. Mbledhja në *kohë reale* e të dhënave të trafikut mundëson hetimet me kompjuter të ndezur dhe është përshkruar në Nenin 20 të Konventës së Budapestit. Një lloj e tillë mase kërkon legjislacionin e duhur për të lejuar autoritetet e zbatimit të ligjit të mbledhin ose regjistrojnë, nëpërmjet mjeteve teknike, të dhëna në kohë reale, dhe gjithashtu kompetencën për të detyruar shërbimofruesit për të mbledhur ose regjistruar të dhënat e trafikut nga klientët, brenda aktivitetit normal, në kohë reale.  Ky lloj instrumenti investigativ mund të jetë, për shembull, shumë i rëndësishëm për përcaktimin e burimit të komunikimit, përsa i takon identifikimit të keqbërësit, në kohë reale. | |
| Slajdi 21 | Së fundi, Neni 21 përshkruan kapjen e të dhënave të përmbajtjes. Krahas të dhënave të trafikut, nganjëherë autoritetet e zbatimit të ligjit duhet të dinë përmbajtjen reale të komunikimeve ndërmjet të dyshuarve të një krimi. Disa vende kanë tashmë dispozita për interceptimin e telefonave, por jo të gjitha i lejojnë autoritetet të interceptojnë komunikimet, përveç telefonit.  Kjo është arsyeja pse në Nenin 21 specifikisht, Konventa e Budapestit përfshin dispozita që i mundësojnë hetuesve të kapin dhe regjistrojnë komunikimet e të dhënave.  Përveç të qënurit një instrument i fuqishëm investigativ, interceptimi i komunikimeve është gjithashtu dhe një masë shumë ndërhyrëse dhe lejohet vetëm sipas kushteve të Konventës për një disa vepra penale të rënda dhe përcaktohet nga ligjet e brendshme. | |
| Slajdi 23 | Pjesa e Dytë – Dispozitat procedurale sipas ligjit kombëtar | |
| Slajdet 24 deri 31 | Trajnerët do të fusin këtu referencat për dispozitat ligjore kombëtare. | |
|  | Ushtrime Praktike (sipas rastit)  Asnjë ushtrim praktik nuk është përgatitur për këtë sesion | |
|  | **Kontrolli i Njohurive**  Trajneri duhet të kontrollojë njohuritë duke bërë pyetjet përkatëse për secilin aspekt të sesionit. | |
| Slajdet 33 deri 34 | Përmbledhje  Trajneri duhet të përmbledhë / testojë njohuritë për pikat e mëposhtme:   * Të përshkruajë rregullat kombëtare për provat elektronike * Të përmendë kuadrin ndërkombëtar, sipas rastit * Të diskutojë llojet e masave investigative të lejuara sipas ligjit të brendshëm dhe vlerën dhe kriteret e mbledhjes dhe ruajtjes së provave elektronike * Të identifikojë disa specifika të procedimeve kombëtare në lidhje me provat elektronike, në kontekstin e skenarit të kuadrit ligjor ndërkombëtar. | |

|  |  |  |
| --- | --- | --- |
| Mësim 1.3.1 Rishikimi Ditor | | **Kohëzgjatja: 30 Minuta** |
| **Burimet materiale të nevojshme:**   * Kompjuter Laptop ose Kompjuter Tavoline me Windows 7 dhe me Programin Office 2010 * Projektor * Prezantimi me PowerPoint | | |
| **Synimi:**  Synimi i këtij sesioni është rishikimi i aktiviteteve të ditëve të mëparshme, marrja e vlerësimit nga pjesëmarrësit dhe kontrolli që objektivat e sesioneve janë arritur | | |
| **Objektivat:**  Në fund të mësimit, pjesëmarrësit do të jenë në gjendje të:   * Identifikojnë fushat e aktiviteteve të ditëve të mëparshme që kanë kuptuar * Identifikojnë fushat e tilla ku ata kanë nevojë të rishikojnë materialet për të rritur njohuritë në nivelin e kërkuar | | |
| **Hyrje**  Ky sesion është përgatitur për t’i lejuar pjesëmarrësve të kontrollojnë se e kanë kuptuar mësimin e ditëve të mëparshme dhe se janë në gjendje të përmbushin secilën prej objektivave për sesionet individuale. Është gjithashtu për t’i dhënë mundësinë trajnerit të kontrollojë nivelin e njohurive të pjesëmarrësve dhe të identifikojë fushat ku mund të përmirësohet materiali. | | |
| **Slajdet nr.** | **Përmbajtja:** | |
| **Slajdet**  **1 deri 12** | **Prezantim me PowerPoint** (ose lloj tjetër prezantimi)  Slajdet në këtë prezantim janë dhënë për të ndihmuar trajnerin dhe pjesëmarrësit me aktivitetet e ditëve të mëparshme. Trajneri duhet të bëjë përmbledhjen e atyre aktiviteteve duke përdorur axhendat dhe objektivat si pika kyç. | |
|  | Ushtrime Praktike (sipas rastit)  Asnjë ushtrim praktik nuk është përgatitur për këtë sesion | |
|  | **Kontrolli i Njohurive**  Trajneri duhet të kontrollojë njohuritë duke bërë pyetjet përkatëse për secilin aspekt të sesionit. | |
|  | Përmbledhje  I gjithë ky sesion është hartuar si një përmbledhje e aktiviteteve të ditëve të mëparshme dhe nuk kërkohet asnjë përmbledhje e veçantë. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mësimet 1.3.2 & 1.3.3 Provat Elektronike | | | | **Kohëzgjatja: 120 & 90 Minuta** |
| **Burimet Materiale të nevojshme:**   * Kompjuter Laptop ose Kompjuter Tavoline me Windows 7 dhe me Programin Office 2010 * Projektor * Akses në Internet (sipas rastit) * Prezantim me PowerPoint * Modele të pajisjeve fizike të kompjuterit (sipas rastit) * Kopje të guidës për provat elektronike të financuar nga Projekti OISIN i BE | | | | |
| **Synimi:** Synimi i këtij sesioni është pajisja e gjyqtarëve dhe prokurorëve me njohuri për çështjet që lidhen me provat elektronike të tilla si llojet e ndryshme të provave që mund të hasin, sesi t’i marrin dhe ti trajtojnë gjatë hetimeve dhe t’i paraqesin në proceset gjyqësore penale. Jepen gjithashtu njohuri të tjera për sfidat e marrjes së provave të tilla nga juridiksionet e tjera. | | | | |
| **Objektivat:**  Në fund të sesionit pjesëmarrësit do të jenë në gjendje të:   * Diskutojnë llojet e ndryshme të provave elektronike * Shpjegojnë parimet e praktikave më të mira në lidhje me sekuestrimin dhe trajtimin e provave elektronike * Identifikojnë sfidat e komunikimit me mënyrën “dead box”[[81]](#footnote-82), “live data”[[82]](#footnote-83) dhe burimet në Internet të provave elektronike * Identifikojnë sfidat e marrjes së provave nga një juridiksion tjetër * Diskutojnë çështjet e pranueshmërisë së provave elektronike në procedimet gjyqësore, përsa i takon autenticitetit, saktësisë, dhe plotësisë | | | | |
| **Koha** | **Përmbajtja:** | | | |
| 30 minuta  30 minuta  60 minuta  60 minuta  30 minuta | * Hyrja dhe hapja (Axhenda dhe objektivat e sesionit) * Pjesa 1 – Çfarë janë Provat Elektronike * Pjesa 2 – Procedurat dhe Praktika e Mirë * Pjesa 3 – Çështjet Ligjore * Përmbledhje | | | |
| **Hyrje**  Ky sesion synon të pajisë trajnerët me një kuadër për zhvillimin e materialeve të trajnimit për tu zhvilluar si pjesë e një programi më të gjerë. Nuk mund të jetë gjithëpërfshirës sepse teknologjia ndryshon kaq me shpejtësi saqë çdo specifikim teknik do të vjetrohej pothuaj në momentin që do të botohej dokumenti. Garantimi që Gjyqtarët dhe Prokurorët të kenë njohuri të mjaftueshme për çështje teknike sepse ato lidhen me çështjet që dalin përpara tyre, është thelbësore për funksionimin e drejtë të çdo sistemi gjyqësor. Ky sesion jep një vështrim të përgjithshëm të aspekteve përkatëse të teknologjisë dhe lidhjes së saj me sistemin e drejtësisë penale. Ofrohet një prezantim me PowerPoint si material për tu përdorur nga trajnerët nëse konsiderohet i përshtatshëm.    Ky sesion jep informacion për teknologjinë që do të haset nga Gjyqtarët dhe Prokurorët gjatë punës së tyre dhe që përdoret nga keqbërësit për kryerjen e veprave penale për tu zbuluar nga autoritetet e zbatimit të ligjit.  Ky sesion është mbështetur në dokumentin “seizure of e-evidence”[[83]](#footnote-84) për shumicën e materialeve të tij burimore. Ky dokument u hartua me financimin e Komisionit Evropian me anë të Programit OISIN me referencë 2002/OIS/014[[84]](#footnote-85). Ky dokument është hartuar disa vjet më parë dhe pjesë të tij, për këtë arsye, janë të vjetruara. Aty ku duhet informacioni është azhurnuar për tu përfshirë në këtë kurs trajnimi. Dokumenti u prezantua fillimisht në komunitetin e autoriteteve të zbatimit të ligjit; megjithatë të tjerë mund të zbatojnë parimet dhe procedurat në sistemin e drejtësisë penale. Ky dokument mund të zbatohet në të gjitha çështjet në të cilat duhet të sekuestrohen prova elektronike.    Secili Shtet Anëtar duhet të marrë në konsideratë rregulloret dhe dokumentacionin e tij ligjor kur të bëjë interpretimin e masave të propozuara në këtë dokument. Krahas kësaj, secili Shtet Anëtar duhet të shtojë informacionin e kontaktit për njësitë e tij të ekspertëve.    Një organizatë ose agjenci që dëshiron të zbatojë procedurat e rekomanduara duhet të përcaktojë përgjegjësitë për veprime/hapa individuale në përputhje me strukturën e saj të brendshme. | | | | |
| **Slajdet nr.** | **Përmbajtja:** | | | |
| Slajde 1 | **Prezantimi me PowerPoint** (ose lloje të tjera të prezantimeve) | | | |
| **Slajdi 2** | Axhenda  Slajdi i axhendës rendit pjesët e sesionit dhe trajneri duhet t’i kalojë këto duke shpjeguar ku është e nevojshme aspekte specifike që duhen nënvizuar për grupe të caktuara të studentëve. Trajneri duhet të shpjegojë sesi do trajtohen materialet dhe kohën e caktuar për ndërveprim dhe pyetje. Trajneri duhet të theksojë se ky trajnim është hartuar të jetë interaktiv dhe se pjesëmarrësit duhet të jenë aktivë gjatë gjithë trajnimit. Trajneri duhet të shpjegojë nëse ka vlerësim dhe se çfarë forme ka ai, duke përfshirë detaje të çdo vlerësimi që zbatohet. (Për këtë program pilot, nuk është përfshirë asnjë vlerësim). | | | |
| **Slajdi 3** | Është e rëndësishme që pjesëmarrësit të kuptojnë se cilat janë objektivat e mësimit. Këto duhet të jenë në formën e objektivave “SMART” dhe të shpjegohen në detaje për pjesëmarrësit përpara se të fillojë sesioni, duke përdorur informacionin në slajd. | | | |
| Slajdi 6 | Pjesa e Parë – Çfarë janë Provat Elektronike | | | |
|  | Llojet dhe burimet e provave elektronike    Shembuj  Trajneri duhet të fillojë një diskutim me pjesëmarrësit duke identifikuar llojet e provave elektronike dhe duke i inkurajuar pjesëmarrësit të japin detaje nga njohuritë e tyre për këtë çështje. Trajneri më pas duhet të rendisë llojet e provave të vendosura në një tabelë me letër ose tabelë të bardhë. Trajneri duhet të plotësojë listën nëse pjesëmarrësit nuk i vendosin llojet e ndryshme të provave. Lista duhet të përfshijë të dy llojet e provave p.sh. me kompjuter fikur, me kompjuter ndezur, memoria, Interneti, si dhe burime të provave si ato të trajtuara në seksionin e teknologjisë. | | | |
| Slajdi 8 | Përkufizimi  Përkufizimi i provave zakonisht përshkruhet në legjislacionin e brendshëm. Meqë ky është një kurs ndërkombëtar është përdorur një përkufizim i përgjithshëm. Përkufizimi është marrë nga fjalori Black’s Law. Trajnerët duhet ta zëvendësojnë këtë me përkufizime kombëtare sipas vendit ku do të zhvillohet kursi.  “Prova si koncept juridik është çdo lloje prove ose lënde provuese, e paraqitur ligjërisht në gjykimin e një çështjeje, nga palët dhe nëpërmjet dëshmitarëve, shënimeve, dokumenteve, objekteve konkrete, etj. me qëllimin e nxitjes së besimit në mendjet e gjyqtarëve ose të jurisë për argumentimin e çështjes.' Informacioni elektronik është zakonisht i pranueshëm si provë në procedimet gjyqësore”. | | | |
| Slajdet 9 dhe 10 | Nuk ka një përkufizim të pranuar ndërkombëtarisht të provave elektronike. Megjithatë në shumë vende ka rregulla që përmbajnë urdhra, të cilat në njëfarë mënyre i referohen provave elektronike*.*  Një shembull i dobishëm i një “përkufizimi” është:  Informacion ose të dhëna me vlerë investigative që ruhen ose transmetohen nga një pajisje elektronike.  [www.nij.gov](http://www.nij.gov)[/topics/forensics/evidence/digital/digital-glossary.htm](http://www.nij.gov/topics/forensics/evidence/digital/digital-glossary.htm)  Edhe njëherë, është përgjegjësia e trajnerit të garantojë që çdo përkufizim kombëtar që mund të ekzistojë të përfshihet në trajnimin e një vendi.  Lufta kundër formave moderne të kriminalitetit kërkon mbështetjen e ekspertëve dhe oficerëve të specializuar   * Për analizën e provave dhe interpretimin e saktë të tyre * Gjatë fazave të hetimit dhe të gjykimit | | | |
| Slajdi 12 | Burimet dhe llojet e provave elektronike  Nuk është e nevojshme të rishikohet e gjithë lista e llojeve dhe burimeve të provave që u identifikuan në seksionin e teknologjisë në këtë kurs. Trajneri duhet të bëjë përmbledhjen duke përdorur listën që u krijua në fillim të këtij sesioni.  Burimet mbulojnë çdo pajisje elektronike. Trajneri mund të dëshirojë të nxjerrë në pah rëndësinë e provave elektronike nga pajisje të ndryshme dhe rolin që luajnë ato në çështjen gjyqësore.    Llojet e provave për tu trajtuar janë ato që kanë të bëjnë:   * Të dhënat statike * Të dhënat e marra me kompjuter ndezur * Të dhënat në Internet | | | |
| Slajdi 13 | Karakteristikat e provave elektronike  Ka shumë karakteristika të provave elektronike që krijojnë sfida shtesë për pranueshmërinë sesa provat tradicionale. Në shumë raste, ato trajtohen dhe administrohen në të njëjtën mënyrë si provat e tjera dhe është kuptimi i çështjeve dhe aftësia e gjyqtarëve dhe prokurorëve për të lidhur natyrën elektronike të provave që është faktori kyç.    Siç mund të shihet nga shembujt e dhënë në kurs, shumë prej çështjeve të renditura lidhen edhe me provat elektronike edhe me ato tradicionale; megjithatë ekzistojnë disa diferenca dhe këto duhet të theksohen në këtë fazë.  Çështjet janë:   * **Paqëndrueshmëria** * Mund të ndryshohen lehtësisht * Mund të mos jenë të disponueshme për shumë kohë      * **Natyra** * Mund të kërkojnë aftësi të specializuara për tu vlerësuar * Mund të kërkojnë prova të specializuara për tu interpretuar * Mund të nevojitet ushtrimi i kompetencave për marrjen dhe aksesin tek to, ose përdorimi mund të jetë i kufizuar      * **Vendndodhja** * Mund të jetë të lidhura pazgjidhshmërisht me materiale jo provuese * Mund të jenë jashtë juridiksionit      * **Volumi** * Identifikimi i materialit provues * Identifikimi i materialit të papërdorur | | | |
| Slajdi 14 | Çështje të provave  Karakteristikat e provave elektronike çojnë drejt disa çështjeve që duhet të nënvizohen. Trajneri duhet t’i shpjegojnë këto me ndihmën e shembujve.    Çështjet janë:     * Indicie * Të dhënat e biznesit * Proceset e automatizuara * Provat e përziera * Volumi i të dhënave * Provat e specializuara      * **Të brishta.** Disa të dhëna dixhitale të përpunuara nga një sistem kompjuterik janë jashtëzakonisht të brishta dhe lehtësisht mund të fshihen ose modifikohen. Ky aspekt jo vetëm që lidhet me vlerësimin e provave elektronike por gjithashtu edhe me procesin e mbledhjes së provave. Të dhënat e ruajtura vetëm në memorien RAM zakonisht humbasin nëse sistemi fiket me përjashtim të rastit kur aplikohen masa teknike të posaçme për ta parandaluar këtë proces. Meqë informacioni i ruajtur në memorien e sistemit mund të jetë me rëndësi të madhe për hetimin, teknika e mbledhjes së këtyre provave mund të jetë e ndryshme nga proceset e mbledhjes së provave tradicionale.      * **Të ndryshueshme.** Të dhënat dixhitale janë të ndryshueshme. Një nga parimet themelore të kriminalistikës dixhitale është nevoja për ruajtjen e integritetit të provave elektronike. Garantimi i dokumentimit të plotë të procesit dhe zbatimi i metodave për ruajtjen e integritetit të të dhënave kompjuterike është esenciale për evitimin e pretendimeve të të dyshuarit për falsifikim të provave. Si rezultat, ekspertët e kriminalistikës dixhitale kërkojnë të zëvendësojnë proceset e hetimit që çojnë drejt ndryshimit të skedarëve në kompjuterët e të dyshuarve me procese më të sofistikuara.      * **Ruajtja e decentralizuar e të dhënave.** Disponueshmëria e aksesit me gjerësi të madhe vale në Internet dhe serverëve të largët për ruajtjen e informacionit ka influencuar mënyrën në të cilën ruhet informacioni sot. Megjithëse në të kaluarën hetuesit përqendroheshin në ambientet e të dyshuarit për të kontrolluar për të dhëna kompjuterike, sot ata duhet të marrin konsideratë se informacioni dixhital mund të ruhet fizikisht jashtë shtetit dhe mund të aksesohet nga larg nga i dyshuari nëse është e nevojshme.      * **Shpejtësia e zhvillimit teknik.** Zhvillimi teknik po vazhdon me ritëm të shpejtë. Një numër i konsiderueshëm zhvillimesh përbëjnë sfida të reja në lidhje me ekzaminimin kriminalistik. K zhvillim kërkon trajnim të vazhdueshëm të atyre që janë të përfshirë në mbledhjen e provave, si dhe mbajtjen e pajisjeve të azhurnuara. Versione të reja të sistemeve të operimit dhe produkteve të tjera të programeve kompjuterike mund të gjenerojnë të dhëna të ndryshme që mund të jenë të lidhura me hetimet. Zhvillime të ngjashme ndodhin edhe me pajisjet fizike kompjuterike. Ndërkohë që në të kaluarën të dhënat ruheshin në disketa, hetuesit sot duhet të marrin në konsideratë se informacioni mund të ruhet në pajisje MP3 ose ora dore që përfshijnë pajisje USB. | | | |
| Slajdet 18 dhe 19 | Pjesa e Dytë – Procedurat dhe Praktikat e Mira | | | |
|  | Kjo pjesë e mësimit mbështetet shumë në çështjet e trajtuara në guidën për provat elektronike. Shumë detaje janë ofruar për të ndihmuar trajnerin të krijojë mësimin. Këto janë të detajuara në guidën e trajnerit dhe janë përmbledhur me pika të zeza në slajdet shoqëruese. Trajneri duhet të konsiderojë se sa detaje janë të nevojshme bazuar në kriteret e pjesëmarrësve për të mundësuar objektivat që duhet të arrihen.  Guida mund të zbatohet në të gjitha rastet në të cilat duhet të sekuestrohen prova elektronike.  Secili Shtet Anëtar duhet të marrë në konsideratë rregullat dhe dokumentet e tij ligjore gjatë interpretimit të masave të propozuara në këtë dokument. Krahas kësaj, secili Shtet Anëtar duhet të shtojë informacionet e kontaktit për ekspertët e tij.  Një organizatë apo agjenci që duhet të aplikojë procedurat e rekomanduara duhet të përcaktojë përgjegjësitë për hapat/veprimet individuale në përputhje me strukturën e tij të brendshme. | | | |
| Slajdi 20 | PARIME TË PËRGJITHSHME  Në trajtimin e provave elektronike, është e rëndësishme të ndiqen parimet e përgjithshme, d.m.th,   1. Dëshmitë në vendngjarje, 2. Integriteti i të dhënave, 3. Lista e kontrolleve, 4. Mbështetja e ekspertëve, 5. Trajnimi i oficerëve, dhe 6. Ligjshmëria dhe mbështetja tek parimet.   Parimet shpjegohen në seksionet e mëposhtme. | | | |
| Slajdi 21 | 1. **Dëshmitë në vendngjarje**   Parimi: *Oficeri përgjegjës nuk duhet të shkojë kurrë në vendngjarje i vetëm*  Të paktën dy oficerë duhet të jenë përfshirë në këtë lloj aktiviteti. Kjo ofron vetë-mbrojtje nga njëra anë, dhe ndihmon në kapjen e më shumë detajeve në vendngjarje. Oficerët duhet t’i planifikojnë dhe koordinojnë veprimet e tyre. Nëse hasen probleme të papritura, është më e lehtë të zgjidhen sepse “dy mendje janë më mirë se një”. | | | |
| Slajdi 22 | 1. **Integriteti i të Dhënave**   Parimi: *Asnjë veprim nuk duhet të kryhet nga oficerët apo punonjësit e zbatimit të ligjit për të ndryshuar mjetet apo pajisjet elektronike, të cilat më pas duhet të përdoren në gjykatë gjatë procesit gjyqësor*  Gjatë administrimi të të dhënave dhe pajisjeve elektronike, ato nuk duhet të ndryshohen, ose në lidhje me pajisjet fizike ose programet kompjuterike. Oficeri është përgjegjës për integritetin e materialit të mbledhur nga vendngjarja dhe për fillimin e zinxhirit të ruajtjes së provave elektronike. | | | |
| Slajdi 23 | 1. **Lista e Kontrolleve**   Parimi: Duhet të krijohet dhe ruhet një listë kontrollesh apo të dhëna të tjera të të gjitha veprimeve të ndërmarra gjatë administrimit të provave elektronike. Një palë e tretë e pavarur duhet të jetë në gjendje të ekzaminojë këto veprime dhe të arrijë të njëjtin rezultat*.*  Është imperative të regjistrohen me saktësi të gjitha aktivitetet për t’i mundësuar një pale të tretë të rindërtojë veprimet e hetuesit të parë në vendngjarje me qëllim që të sigurohet vlera e tyre provuese në gjykatë. I gjithë aktiviteti në lidhje me sekuestrimin, aksesin, ruajtjen ose transferimin e provave elektronike duhet të dokumentohet plotësisht, të ruhet dhe të bëhet i disponueshëm për rishikim. | | | |
| Slajdi 24 | 1. **Mbështetja nga Ekspertë të Fushës**   Parim: *Nëse supozohet se gjatë një operacioni policie do të gjenden prova elektronike, oficeri përgjegjës duhet të njoftojë ekspertët/konsulentët e jashtëm në kohë*  Për hetimet që kanë të bëjnë me kontroll dhe sekuestrim të provave elektronike, mund të jetë e nevojshme konsultimi me ekspertët e jashtëm. Të gjithë ekspertët e jashtëm duhet të njohin parimet e përcaktuara në këtë ose dokumente të tjerë të ngjashëm. Një ekspert duhet të ketë:   * Ekspertizën e nevojshme dhe përvojën në fushë, * Njohuritë ligjore dhe investigative të nevojshme, * Njohuritë ligjore dhe kontekstuale të nevojshme, dhe * Aftësitë e përshtatshme të komunikimit (për shpjegimet edhe me gojë edhe me shkrim). | | | |
| Slajdi 25 | 1. **Trajnimi i Oficerëve**   Parimi: *Hetuesit e parë në vendngjarje duhet të jenë të trajnuar në mënyrë të përshtatshme për të kontrolluar dhe sekuestruar provat elektronike nëse nuk janë të disponueshëm ekspertët në vendngjarje*  Në rrethana përjashtimore kur është e domosdoshme që një hetues në vendngjarje të mbledhë prova elektronike dhe/ose të aksesojë të dhëna origjinale të ruajtura në një pajisje elektronike ose pajisje dixhitale të ruajtjes së të dhënave, ai/ajo duhet të jetë i trajnuar për ta realizuar atë siç duhet dhe të shpjegojë lidhjen dhe implikimet e veprimeve të tij/saj. | | | |
| Slajdi 26 | 1. **Ligjshmëria dhe Përmbajtja tek Rregullat**   Parimi: *Oficeri dhe agjencia përgjegjëse për garantimin e ligjit duhet t’i përmbahet parimeve procedurale dhe kriminalistike të përgjithshme, dhe parimeve të sipërpërmendura. Kjo zbatohet edhe për posedimin dhe aksesin tek provat elektronike.*  Secili Shtet Anëtar duhet të marrë në konsideratë rregullat dhe dokumentet e tij ligjore kur të bëjë interpretimin e masave të propozuara në këtë dokument.  Një nga dokumentet ligjorë më të rëndësishëm ndërkombëtarë, Konventa për Krimin Kibernetik e Këshillit të Evropës, aktualisht është e hapur për nënshkrim nga Shtetet Anëtare dhe Shtetet që kanë marrë pjesë në trajtimin dhe aderimin në të nga shtetet e tjera. | | | |
| Slajdi 28 | Llojet e sekuestrimit  Alternativat e ndryshme për sekuestrimin e provave elektronike janë një aspekt i rëndësishëm i këtij kursi trajnimi dhe të gjitha kanë karakteristika, risqe dhe rezultate të ndryshme. Trajneri duhet të garantojë që të gjitha të shpjegohen në detaje në mënyrë që pjesëmarrësit të jenë në gjendje të kuptojnë impaktin e këtyre në rolin e tyre si gjyqtarë dhe prokurorë. Informacioni që pason jepet për t’iu lejuar trajnerëve të zhvillojnë material të përshtatshëm.  Ka katër lloje të përgjithshme të sekuestrimit të provave elektronike:   1. Sekuestrimi me anë të konfiskimit të pajisjeve elektronike dhe pajisjeve të ruajtjes së të dhënave; 2. Sekuestrimi me anë të kopjimit të të gjithë përmbajtjes së memories (me anë të kopjimit të imazheve dhe të dhënave); 3. Sekuestrimi me anë të konfiskimit të pajisjeve rezerve të ruajtjes së të dhënave 4. Sekuestrimi me anë të kopjimit të të dhënave të përzgjedhura; dhe 5. Sekuestrimi i provave nga Interneti   Llojet e ndryshme të sekuestrimit diskutohen në seksionet e mëposhtme. Ju lutem vini re se është e mundur që të kombinohen lloje të ndryshme të sekuestrimit brenda një procedure sekuestrimi. Për shembull, mund të jetë e nevojshme të konfiskohen edhe pajisjet elektronike edhe pajisjet rezervë të ruajtjes së të dhënave. | | | |
| Slajdi 29 | 1. **Sekuestrimi i pajisjeve elektronike dhe pajisjeve të ruajtjes së të dhënave**   Ky lloj sekuestrimi mund të jetë i përshtatshëm në rastet e mëposhtme:   * Nuk ka shumë pajisje për tu konfiskuar, p.sh. një kompjuter tavoline ose një rrjet i vogël (p.sh., në apartamentin e një të dyshuari); * Nuk ka rrezik për humbje të madhe financiare ose humbje të tjera që mund të shkaktohen nga mosfunksionimi/mosdisponueshmëria e pajisjeve të konfiskuara; * Konfiskimi është absolutisht i nevojshëm për shkak të natyrës së veprës së caktuar; * Është e nevojshme të ndalohen aktivitetet e mbështetura nga pajisjet që do të konfiskohen.   Avantazhet e këtij lloji sekuestrimi janë si më poshtë:   * Mund të kryhet pa mbështetjen e ekspertit në vendngjarje; * Procedura e sekuestrimit zakonisht nuk konsumon shumë kohë; * Provat elektronike merren në kontroll; dhe * Provat elektronike mund të analizohen në një mjedis të kontrolluar.   Disavantazhet e këtij lloji sekuestrimi janë si më poshtë:   * Ka rrezik të dëmtimit të pajisjeve; * Ka rrezik të dëmtimit të personave të palidhur me veprën penale në fjalë; dhe * Ka rrezik të ndërhyrjes me aktivitete të palidhura me veprën penale në fjalë.  1. **Kopjimi i të gjithë përmbajtjes së memories**   Për këtë lloj sekuestrimi, nganjëherë të quajtur edhe “imaging”[[85]](#footnote-86) ose “mirroring”[[86]](#footnote-87), përdoren pajisje të posaçme për të krijuar një dublikatë ekzakte të përmbajtjes së memories së pajisjes elektronike (ose pajisjeve dixhitale për ruajtjen e të dhënave) ose një mjeti/pajisjeje të jashtme për ruajtjen e të dhënave.  Ky lloj sekuestrimi mund të jetë i përshtatshëm për rastet e mëposhtme:   * Ka një sasi të konsiderueshme të pajisjeve për tu marrë në konsideratë (p.sh., ndërmarrje të vogla ose të mesme); * Ka rrezik për humbje të mëdha financiare ose humbje të tjera që mund të shkaktohen nga mosfunksionimi/mosdisponueshmëria e pajisjeve (p.sh. sistemi i teknologjisë së informacionit mund të konsiderohet vital për një të dyshuar ose një palë të tretë); dhe * Konfiskimi nuk konsiderohet i nevojshëm për shkak të natyrës së veprës së caktuar.   Avantazhet e këtij lloji sekuestrimi janë si më poshtë:   * Rrezik i vogël për dëmtimin e pajisjeve; * Rrezik i vogël për dëmtimin e personave që nuk lidhen me veprën penale në fjalë; * Risk i vogël i ndërhyrjes me aktivitete të palidhura me veprën penale në fjalë; * Provat elektronike mund të analizohen në një mjedis të kontrolluar.   Disavantazhet e këtij lloji sekuestrimi janë si më poshtë:   * Nevojiten pajisje të posaçme në vendngjarje; * Mbështetja e ekspertit është zakonisht e nevojshme në vendngjarje; * Ekziston risku i mosvënies re të një pjese të provave; * Procedura e sekuestrimit konsumon kohë; dhe * Pajisja përkatëse vihet nën kontroll.      1. **Sekuestrimi me anë të konfiskimit të pajisjes rezervë për ruajtjen e të dhënave**   Ky lloj sekuestrimi mund të jetë i përshtatshëm në raste të ngjashme me anë të kopjimit të të gjithë përmbajtjes së memories veçanërisht nëse ka një sasi të madhe të pajisjeve dhe të dhënave për tu marrë parasysh (p.sh. rrjete të mëdha, mjedise me kompjuterë mainframe).  Avantazhet janë të ngjashme me ato të sekuestrimit me anë të kopjimit të përshkruara në Seksionin 2 (nuk ka asnjë risk për dëmtim ose veprime të dëmshme). Avantazhe të tjera janë se   * Asnjë pajisje e posaçme nuk kërkohet në vendngjarje; dhe * Nuk ka nevojë të kryhet asnjë veprim që merr kohë në vendngjarje.   Disavantazhet e këtij lloji sekuestrimi janë si më poshtë:   * Mbështetja e ekspertit është zakonisht e nevojshme në vendngjarje; * Zakonisht është e nevojshme mbështetja e administratorit të sistemit lokal; * Ekziston risku i mosvënies re të një pjese të provave (për shkak se tërësia e të dhënave rezervë zakonisht nuk mund të dihet përpara); dhe * Pajisja përkatëse nuk vihet nën kontroll.  1. **Sekuestrimi duke kopjuar të dhëna të përzgjedhura**   Ky lloj sekuestrimi duhet të përdoret vetëm në rrethana të jashtëzakonshme nëse nuk është i mundur të realizohet asnjë prej llojeve të tjera të sekuestrimeve, i.e., vetëm të dhëna të përzgjedhura (d.m.th, të dhënat më relevante) mund të kopjohen dhe analizohen më vonë. Mbështetja e ekspertit zakonisht është e detyrueshme në vendngjarje.  Avantazhet dhe disavantazhet janë të ngjashme me ato të sekuestrimit me anë të konfiskimit të pajisjes rezervë për ruajtjen e të dhënave. Një disavantazh tjetër do të ishte se do të ishte i pamundur çdo rikonstruktim historik i sistemit kompjuterik. Kjo do ta kufizonte efektivisht vlerën e hetimit. Krahas kësaj, vëmendje e posaçme duhet t’i kushtohet vlerës provuese të informacionit të sekuestruar në këtë mënyrë.   1. **Sekuestrimi i provave nga Interneti**   Sekuestrimi i provave nga Interneti është thelbësor për shumë lloje të hetimit dhe kërkon njohuri, aftësi dhe burime të specializuara që të arrihet të realizohet me efektivitet. Ky kurs nuk do të trajtojë specifikat e mbledhjes së të dhënave të tilla përveçse do të përforcojë se parimet e përgjithshme zbatohen për këtë njësoj si për llojet e tjera që janë përfshirë në këtë kurs. Ka lloje të ndryshme të mbledhjes së provave nga Interneti dhe këto mund të ndahen në 1) mbledhja e të dhënave me burim të hapur dhe 2) mbledhja me mjete te fshehura. Ka çështje procedurale dhe ligjore që lidhen me këtë aspekt dhe nuk janë trajtuar këtu gjerësisht. Është parashikuar që kjo temë të trajtohet në një modul trajnimi më të avancuar. | | | |
| Slajdet 30 deri 40 | PROCEDURA E SEKUESTRIMIT TË PROVAVE ELEKTRONIKE  Siç u përmend në hyrje, ky dokument fokusohet tek procedura e sekuestrimit të provave elektronike që ka të bëjë me kontrollin, njohjen, mbledhjen dhe dokumentimin e provave elektronike. Procedura konsiston në fazat e mëposhtme që janë përshkruar në seksionet e mëposhtme:   1. Përgatitja për sekuestrim (Seksioni [1](#_Lesson_No:_1.3.2)), 2. Sigurimi i vendngjarjes (Seksioni 2), 3. Dokumentimi i vendngjarjes (Seksioni ), 4. Mbledhja e provave (Seksioni 4), dhe 5. Paketimi, transportimi dhe ruajtja (Seksioni ).   Parimet kryesore për kontrollin e një mjedisi IT të rekomanduara nga Këshilli i Bashkimit Evropian janë marrë të gjitha në konsideratë gjatë zhvillimit të procedurave të përshkruara në seksionet e mëposhtme.   1. **Përgatitja për sekuestrim**   Gjatë hetimeve të mëparshme të synuara për marrjen e një urdhri kontrolli, duhet të përcaktohet nëse ka të ngjarë të gjenden prova elektronike që mund të kenë lidhje me çështjen. Në një rast të tillë, oficeri përgjegjës duhet të informojë njësinë lokale të rikuperimit të të dhënave dhe/ose ekspertët e jashtëm sa më shpejt që të jetë e mundur. Vendimi i parë për tu marrë është se cili lloj sekuestrimi duhet të kryhet (llojet e sekuestrimeve janë të përshkruara në slajdin 28). I gjithë informacioni i mundur për tu sekuestruar për sistemin kompjuterik duhet të grumbullohet paraprakisht dhe me mbështetjen e ekspertit, si për shembull:   * Informacion për pjesët fizike të kompjuterëve/sistemet e operimit/programet kompjuterike/aplikacionet dhe informacion tjetër i lidhur me ruajtjen e të dhënave, * Informacion për rrjetin dhe komunikimet (ISP[[87]](#footnote-88), telefon, faks, modem, LAN[[88]](#footnote-89), pajisje të rrjetit, etj.), * Kush është përgjegjës për sistemin kompjuterik dhe/ose rrjetin (p.sh., nëse ka administrator lokal ose nëse administrohet nga një kompani e jashtme), * Sa pajisje pritet të sekuestrohen (lidhet me llojin e sekuestrimit nga Seksioni ), * Sa të dhëna duhet të kopjohen (lidhet me llojet e sekuestrimit nga Seksionet 2 dhe 4), dhe * A ka të disponueshëm ndonjë kopje rezervë të të dhënave të disponueshme në ndonjë pajisje (lidhet me llojin e sekuestrimit nga Seksioni 3).   Faza përgatitore përfshin hapat e mëposhtëm:   * Të garantohet se sekuestrimi i provave elektronike është i autorizuar siç duhet (p.sh., marrja e urdhrit të kontrollit në përputhje me legjislacionin në fuqi); * Marrja e sa më shumë të dhënave që të jetë e mundur për sistemin kompjuterik që do të sekuestrohet (shih më lart); * Zgjedhja e anëtarëve të grupit (duke përfshirë ekspertët e jashtëm nëse është e nevojshme); * Caktimi i detyrave individuale për anëtarët e grupit; * Informimi i anëtarëve të grupit sesi të kryejnë detyrat e tyre (anëtarët duhet të kenë kryer trajnimin e duhur bazë); dhe * Sigurimi i mjeteve dhe pajisjeve të nevojshme të sekuestrimit (logjistika).   Siç u përmend më lart, të gjitha aktivitetet duhet të jenë në përputhje me politikat e institucionit dhe të BE-së, të Shtetit dhe të legjislacionit të brendshëm.  Anëtarët e Grupit të Sekuestrimit  Nëse dihet se mund të gjenden prova elektronike në vendngjarje, grupi i sekuestrimit duhet të përfshijë oficerë posaçërisht të trajnuar për detyrat e kontrollit dhe sekuestrimit të pajisjeve të teknologjisë së komunikimit dhe provave elektronike. Në disa raste, mund të jetë madje e nevojshme të konsultohet një ekspert i pavarur (shih gjithashtu Seksionin 4). Për shembull, nëse sistemi administrohet nga një kompani e jashtme ose administrator i jashtëm, mund të merrni parasysh që ta përfshini atë si një ekspert dëshmitar (nëse ai/ajo nuk konsiderohet i/e dyshuar). Kriteri minimal është që punonjësit që shkojnë të parët në vendngjarje të kenë trajnimin bazë për mbledhjen e provave elektronike.  Anëtarët e grupi duhet të përzgjidhen dhe detyrat duhet t’iu caktohen nga një oficer përgjegjës që i korrespondon fazave procedurale të sekuestrimit (shih gjithashtu fillimin e slajdit 30). Fazat dhe detyrat korresponduese janë përshkruar në seksionet e mëposhtme (Seksionet -).  Të gjithë anëtarët e grupit duhet të jenë të udhëzuar sesi të kryejnë detyrat e tyre. Për shembull, ata duhet ta dinë kur duhet të zbatojnë parimet në administrimin e provave elektronike njësoj si në administrimin e provave të tjera fizike tradicionale, dhe kur duhet të marrin masa të posaçme (p.sh., nuk duhet të përdoret pluhuri i aluminit për të marrë shenjat e gishtave nga pajisjet elektronike). Ata duhet ta dinë gjithashtu se në disa raste, ata duhet të kontaktojnë një njësi ekspertësh dhe ta marrin këtë informacion paraprakisht.  Pajisjet dhe mjetet e sekuestrimit  Për mbledhjen e provave elektronike mund të nevojiten mjete dhe pajisje të posaçme. Përparimet në teknologji mund të diktojnë ndryshime tek mjetet dhe pajisjet e kërkuara.    Pajisjet e mëposhtme mund të jenë të vlefshme gjatë kontrollit dhe sekuestrimit dhe duhet të jenë të disponueshme për grupin e sekuestrimit nga logjistika:   * Mjetet e zbërthimit dhe heqjes: * Kaçavida (petë dhe kryq, dhe forma të tjera, p.sh., Compaq, Macintosh); * Sete të ndryshme kaçavidash (gjashtëkëndore, në formë ylli dhe të modeleve “secure-bit”); * Pinca (standarde dhe me majë të hollë); * Pinca prerëse për tela (për heqjen e lidhëseve të kabllove); * Piskatore të vogla; * Dokumentacioni: * Regjistri i kontrollit dhe sekuestrimit (regjistri i sendeve në pronësi); * Etiketa dhe ngjitëse ( për të shënuar dhe identifikuar pjesët përbërëse të sistemit, duke përfshirë edhe zgjatueset dhe prizat); * Etiketat për kabllot; * Etiketat për të shënuar objektet (lidhëse dhe ngjitëse); * Formularë të tjerë të nevojshëm * Markera me ngjyrë që nuk hiqet (për të shënuar dhe identifikuar sendet e hequra); * Aparat fotografik dhe/ose videokamera (për të fotografuar skenën dhe ekspozimet në ekran); * Pajisjet e paketimit dhe transportimit: * Qese antistatike (për mbrojtjen e pajisjeve të hequra si p.sh qarqet; materiale që mund të prodhojnë elektricitet statik si qeset me politen); * Qese paketuese me flluska ajri; * Lidhëse për kabllot (për sigurimin e kabllove); * Ngjitëse dhe qese për provat; * Kuti për paketimin e disketave, fishekë JAZ/ZIP, DVD, ose CD; * Materiale paketimi (duhet të evitohen materiale që mund të prodhojnë elektricitet statik të tillë si polisteroli ose polisterol me copa); * Kuti ambalazhimi prej kartoni të madhësive të ndryshme (duhet të përdoret paketim origjinal sa herë që të jetë e mundur); * Mjetet e komunikimit * Telefona celularë ose pajisje të tjera komunikimi për marrjen e këshillave (nuk duhet të përdoren në afërsi të kompjuterëve); * Informacion kontakti për asistencë (p.sh., numra telefoni për njësinë e ekspertëve) * Mjete të tjera: * Elektrik dore me kapëse; * Doreza; * Karrocë dore; * Shirita të mëdha kauçuku; * Lente zmadhuese; * Letër për printim; * CD/disk sekuestrimi (nëse jeni të trajnuar ta përdorni për qëllime të mbledhjes së provave); * Disketa të papërdorura; * Transportimi (për në vendngjarje dhe nga vendngjarja, për anëtarët e grupit të sekuestrimit, pajisjet dhe mjetet e sekuestrimit, dhe provat e sekuestruara).  1. **Sigurimi i vendngjarjes**   Punonjësi i parë në vendngjarje duhet të garantojë sigurinë e të gjithë personave në vendngjarje dhe integritetin e të gjitha provave, edhe tradicionale edhe elektronike.  Kjo fazë përfshin hapat e mëposhtme:   * Ndjekja e politikave juridiksionale për sigurimin e vendngjarjes: * Largimi i të gjithë personave nga zona në të cilën do të merret provat (pajisjet dhe furnizimi me energji); * Mbrojtja nga ana fizike dhe elektronike e të dhënave që mund të prishen: * Identifikoni, siguroni, dokumentoni dhe fotografoni secilën pajisje që përmban të dhëna që mund të prishen; * Vëzhgoni të dyshuarit e mundshëm dhe persona të tjerë për t’i parandaluar që ata të modifikojnë ose shkatërrojnë provat; * Vëzhgoni pajisjet IT për të parandaluar modifikimin ose shkatërrimin e provave. * Identifikimi dhe dokumentimi i komponentëve elektronikë që nuk do të mblidhen; * Identifikimi i linjave telefonike dhe linjave të rrjetit bashkëngjitur me pajisjet, dokumentimi dhe etiketimi i tyre; * Vendosni nëse kërkoni ndonjë provë tjetër nga pajisja që do të sekuestrohet (p.sh., DNA, shenja gishtash, droga, përshpejtuesit); * Nëse po, ndiqni procedurat e përgjithshme të trajtimit për llojet e provave të përcaktuara në manualin përkatës; * Shtyni për më vonë teknikat e shkatërrimit derisa të përfundojë rikuperimi i provave elektronike; * Mblidhni shenja të fshehura mbasi të rikuperohen provat elektronike (sepse tastierat, mausi i kompjuterit, disketat, CD-të, ose komponentët e tjerë mund të kenë shenja gishtash të fshehura ose prova të tjera fizike që duhet të ruhen); * Mos përdorni pluhur alumini për marrjen e shenjave të gishtave nga vendngjarja sepse kjo mund të dëmtojë pajisjet dhe të dhënat. * Kontrolloni vendngjarjen për prova jo elektronike por që lidhen me çështjen, të tilla si: * Fjalëkalime të shkruara dhe shënime të tjera me shkrim, * Letra bosh me shkrim të shtypur, * Manuale për pjesët fizike të kompjuterit apo programe kompjuterike, * Kalendarë ose ditarë, * Letra të printuara me imazhe apo me tekste, * Fotografi, ose * Informacion për interesat personale që mund të jenë të dobishme për gjetjen e fjalëkalimit (shumica e fjalëkalimeve janë direkt të lidhur me mjedisin personal, të tilla si p.sh., targat, bashkëshortët/fëmijët, numrat e telefonit, hobit, etj.) * Zhvilloni intervista paraprake: * Veçoni dhe identifikoni të gjithë personat (dëshmitarë, subjekte, ose të tjerë) në vendngjarje dhe regjistroni vendndodhjen e tyre në kohën e hyrjes; * Përdorni formular/listë ose diçka të ngjashme për të mbledhur ose regjistruar të dhëna nga këto individë; * Në përputhje me politikat e institucionit dhe legjislacionin në fuqi, merrni nga këta individë të dhëna të tilla si: * Qëllimin e pajisjes/sistemit (p.sh., kontabilitet); * Pronarët dhe/ose përdoruesit e pajisjeve/sistemeve të gjetura në vendngjarje, si dhe fjalëkalimet (shih më poshtë), emrat e përdoruesve, dhe Kompaninë Shërbimofruese të Internetit; * Çdo fjalëkalim për tu futur në sistem, program kompjuterik ose të dhëna. (Një individ mund të ketë disa fjalëkalime, p.sh., për BIOS-in, hyrjen në sistem, për hyrjen në rrjet ose ISP, skedarë aplikacionesh, fraza për kodimin të tilla si PGP, postën elektronike, të dhënat e aksesit, axhendë, ose listë kontaktesh.); * Çdo skemë unike të sigurisë ose pajisje destruktive; * Çdo ruajtje të dhënash jashtë sistemit; dhe * Çdo dokumentacion që shpjegon pjesët fizike ose programet kompjuterike të instaluara në sistem.  1. **Dokumentimi i vendngjarjes**   Dokumentimi i vendngjarjes është një proces gjatë gjithë procedurës së sekuestrimit. Është me rëndësi thelbësore të dokumentohet me saktësi vendndodhja dhe gjendja e kompjuterëve, pajisjeve të ruajtjes së të dhënave, pajisjeve të tjera elektronike, dhe pajisjeve të tjera tradicionale. Në seksionet e mëparshme dhe të ardhshme të Kapitullit 0 jepen udhëzime më të detajuara në lidhje me çfarë duhet të dokumentohet. Ky seksion jep vetëm një përmbledhje të këtyre udhëzimeve.  Në përgjithësi, të mëposhtmet duhen dokumentuar por mund të krijohet dokumentacion shtesë gjatë fazës së mbledhjes:   * Vendngjarja fizike * Bëni një skicë të sistemit duke përfshirë, p.sh., pozicioni i mausit dhe vendndodhja e komponentëve të tjerë të kompjuterit; * Fotografoni/regjistroni me video/dokumentoni të gjithë skenën[[89]](#footnote-90) (mbulim 360 gradë nëse është e mundur); * Sistemet kompjuterike dhe komponentët/pajisjet/mjetet elektronike * Dokumentoni të mëposhtmet: * Detajet e të gjitha pajisjeve përkatëse të gjetura, p.sh. marka, modeli, numri serial; * Gjendja dhe vendndodhja e secilit sistem kompjuterik që përmban ose paraqet prova elektronike, duke përfshirë gjendjen e kompjuterit (i ndezur, i fikur, ose në gatishmëri); * Dokumentoni të gjitha lidhjet (me kabull ose pa kabull) në drejtim të ose që dalin nga sistemi kompjuterik ose pajisjet e tjera; * Etiketoni të gjitha portat dhe kabllot (duke përfshirë lidhjet me pajisjet e jashtme periferike) për të realizuar montimin në një kohë të mëvonshme; * Etiketoni portat e lidhjes që nuk përdoret me fjalët “i/e papërdorur”. Identifikoni docking stations[[90]](#footnote-91) për kompjuterët laptop me qëllimin për të identifikuar pajisje të tjera të ruajtjes së të dhënave * Dokumentoni detajet e monitorit në kohën e ndërhyrjes. * Fotografoni pjesën ballore të kompjuterit si dhe ekranin e monitorit dhe komponentët e tjerë; * Mbani shënim se çfarë shfaqet në ekranin e monitorit; * Regjistroni me video programet aktive ose krijoni dokumentacion më të zgjeruar të aktivitetit të ekranit të monitorit. * Dokumentoni komponentët përkatës elektronik që do të sekuestrohen; * Informacioni nga personat e gjendur në vendngjarje * Intervistoni personat dhe dokumentoni përgjigjet/plotësoni formularët * Dokumentoni sa më poshtë: * Detajoni të gjithë personat e pranishëm në ambientet e kontrollit; * Detajoni të gjithë personat që kanë përdorur pajisjet/sistemin kompjuterik përkatës; * Shënime, komente dhe informacion të marrë nga përdoruesit/pronarët e sistemit kompjuterik si dhe dëshmitarët. * Veprimet e ndërmarra në vendngjarje * Krijoni një listë me kontrollet/regjistër sekuestrimi me përshkrimin e veprimeve të ndërmarra dhe datën dhe kohën e saktë.      1. **Mbledhja e Provave**   Një sistem kompjuterik nuk duhet të sekuestrohet vetëm sepse rastis të gjendet ne vendngjarje. Një masë e tillë mund të justifikohet dhe në proporcion me veprën korresponduese, për këtë arsye, personi që urdhëroi kontrollin duhet të marrë një vendim të ndërgjegjshëm nëse një objekt duhet të merret nga autoriteti investigues.  Si me çdo provë tjetër, provat elektronike duhet të trajtohen me kujdes dhe në një mënyrë që të ruhet vlera e tyre provuese. Kjo ka të bëjë jo vetëm me integritetin fizik të një objekti ose pajisjeje, por gjithashtu edhe me të dhënat elektronike që përmban. Disa lloje të caktuara të provave elektronike kërkojnë mbledhje, paketim dhe transportim të posaçëm. Provat elektronike që mund të jenë të ndjeshme ndaj dëmtimit ose modifikimit nga fushat elektromagnetike (si ato të gjeneruara nga elektriciteti statik, magnetet, transmetuesit radio dhe pajisjet e tjera) duhet të jenë të mbrojtura në mënyrë adekuate. Provat elektronike duhet të sekuestrohen në përputhje me udhëzimet e institucionit dhe legjislacionin në fuqi. Llojet e mëposhtme të provave elektronike do të diskutohen më vonë:     * Sistemi kompjuterik * Pajisje të tjera elektronike * Mjete dixhitale të ruajtjes së të dhënave * Informacion për rrjetet (konfigurimi dhe shërbimet/aplikacionet)   Mbledhja e provave jo-elektronike (ose provave tradicionale) mund të jetë gjithashtu thelbësore për hetimin e veprave penale kompjuterike/elektronike. Kujdes i veçantë duhet treguar për të garantuar që prova të tilla të rikuperohen dhe të ruhen. Objektet që lidhen me hetimin pasues të provave elektronike mund të ekzistojnë në forma të tjera (p.sh., fjalëkalime të shkruara dhe shënime të tjera, fletë të bardha letre me shkrime të shtypura, manuale për programet kompjuterike ose komponentët fizikë të kompjuterëve, kalendarët, literatura, printimet e teksteve ose imazheve, dhe fotografitë) dhe duhet të sigurohen dhe ruhen për analizë të mëtejshme. Këto objekte shpesh janë në afërsi të kompjuterit apo komponentëve të tjerë fizikë të lidhur me të. Të gjitha provat duhet të identifikohen, sigurohen, dhe ruhen në përputhje me politikat e institucionit dhe legjislacionin në fuqi.   1. **Paketimi, transportimi dhe ruajtja**   Kompjuterët dhe pajisjet e lidhura me to janë instrumente elektronikë të brishtë që janë të ndjeshëm ndaj temperaturës, goditjeve fizike, elektricitetit, burimeve magnetike, dhe madje disa veprimeve (p.sh. ndezja/fikja). Për këtë arsye, duhet të bëhet shumë kujdes gjatë paketimit, transportimit dhe ruajtjes së provave elektronike. Për të ruajtur zinxhirin e ruajtjes së provave duhet të regjistrohet procesi i paketimit, transportimit, dhe ruajtjes së tyre.  Përgjithësisht, të gjithë komponentët e kompjuterit dhe pajisjet e ruajtjes së të dhënave duhet të trajtohen me kujdesin më të madh sepse trajtimi i pakujdesshëm mund të shkaktojë dëmtimin ose shkatërrimin e provave elektronike.     * Paketimi * Sigurohuni që të gjitha provat elektronike të mbledhura të jenë të dokumentuara siç duhet dhe të etiketuara përpara paketimit. * Sa herë që të jetë e mundur, transportoni provat elektronike të mbledhura në paketim origjinal. * Nëse nuk është i disponueshëm asnjë paketim origjinal, përdorni paketimin antistatik (p.sh., çanta prej letre ose qese plastike antistatike). Evitoni përdorimin e materialeve që mund të prodhojnë elektricitet statik, të tilla si qeset plastike standarde. * Mos i palosni, përkulni ose gërvishtni njësitë e ruajtjes së të dhënave si disketat, CD-të dhe kasetat. * Mos ngjisni etiketa me ngjitëse në sipërfaqe të disqeve apo pajisjeve të ruajtjes së të dhënave. Përdorni kuti ose zarfa për paketimin e tyre kurdoherë që është e mundur. * Sigurohuni që të gjithë kutitë që mbajnë provat të jenë me etiketat përkatëse siç duhet. * Nëse sekuestrohen disa sisteme kompjuterike, etiketojini secilin prej tyre qe më pas pastaj të jetë e mundur rimontimi i tyre siç u gjetën në vendngjarje * Transportimi * Mbajini provat elektronike larg prej burimeve magnetike. Transmetuesit radio, altoparlantët, dhe sediljet me rezistenca ngrohjeje janë shembuj të objekteve që mund të dëmtojnë provat elektronike. * Sigurohuni që pajisjet të mbrohen nga goditjet (dëmtim mekanik), nxehtësia dhe lagështia. * Sigurohuni që kompjuterët dhe pajisjet e tjera që nuk janë paketuar në kontenierë të jenë të siguruar në automjet për të evituar goditjet dhe lëkundjet e tepërta. Për shembull, kompjuterët duhet të vendosen në dyshemenë e automjetit dhe monitorët të vendosen në sedilje me ekranin poshtë dhe të siguruar me rrip sigurimi. * Mos vendosni objekte të rënda mbi pjesë të vogla të pajisjeve për ruajtjen e të dhënave. * Sa herë që është e mundur, mos i lini në automjet provat elektronike për periudha të gjata kohe. * Depozitimi * Sigurohuni që provat të inventarizohen në përputhje me rregullat përkatëse. * Ruajini provat në një zonë të sigurt, larg prej temperaturave dhe lagështisë ekstreme. * Mbrojeni atë nga burimet magnetike, lagështia, pluhuri dhe ndotës të tjerë të dëmshëm. * Përdorni një depo/magazinë të sigurt e të përshtatshme me: * Kontroll të hyrjes së saj, * Mbrojtje nga zjarri (p.sh., alarm, bombola për shuarjen e zjarrit, ndalim të duhanit në zonën e depozitimit ose në afërsi të saj), * Temperatura dhe lagështia, dhe * Mbrojtja nga burimet magnetike (p.sh., larg prej pajisjeve të drejtimit me radio). * Mos depozitoni sende të djegshme në të njëjtën dhomë ose në afërsi (p.sh. lëndë kimike për pastrim, ose grumbuj me letër). * Përdorni mbulesa të përshtatshme dyshemeje për të evituar ngarkesat statike. * Mos depozitoni prova elektronike në dhomë me tubacione uji, veçanërisht përgjatë tavanit. * Kini kujdes se provat potenciale të tilla si data, koha dhe konfigurimi i sistemit mund të humbasin si rezultat i magazinimit të gjatë. Përderisa bateritë kanë jetëgjatësi të kufizuar, të dhënat mund të humbasin nëse mbarojnë ato. Për rrjedhim stafi i përshtatshëm duhet të informohet që një pajisje me bateri ka nevojë për vëmendje të menjëhershme (p.sh. një PDA, ose PC/CMOS). | | | |
| Slajdet 42 deri 51 | Investigimi dhe analizimi i provave elektronike  Kriminalistika dixhitale  Termi kriminalistika dixhitale përdoret për përshkrimin e analizës sistematike të pajisjeve të teknologjisë së informacionit me qëllimin e kontrollit për prova elektronike. Analiza kriminalistike zakonisht ndodh mbasi është kryer vepra penale. Krahasuar me hetimet e rregullta, kryerja e një analize të tillë sjell sfida unike sepse teknologjia kompjuterike është gjithmonë në ndryshim dhe gjithnjë e më shumë informacion ruhet në formate dixhitale, gjë e cila rrit sasinë e provave potenciale elektronike. Fokusi për rrjedhim është në aftësinë për t’i përdorur provat në procesin gjyqësor. Kjo kufizon deri në një farë limiti aftësinë për të kryer ekzaminime, sepse ato duhet të kryhen sipas standardeve ligjore. Edhe sikur zhvillime të reja teknike të bënin të mundur hetime të reja kriminalistike, zbatimi i tyre është i kufizuar nga kushti që këto instrumente të reja të mbulohen nga kuadri ligjor ekzistues.  **Fazat e angazhimit të ekspertëve të kriminalistikës**  Ekspertët e kriminalistikës nuk janë të angazhuar vetëm në procedime penale por gjithashtu luajnë një rol të rëndësishëm në procedimet civile, në zhvillimin e strategjive të mbrojtjes dhe edukimit. Përsa i takon procedimeve penale, angazhimi i tyre ndodh në katër faza:   * Identifikimi i provave përkatëse. Ekspertët e kriminalistikës luajnë një rol të rëndësishëm në hartimin e strategjive të hetimit. Ata mund të mbështesin institucionet e zbatimit të ligjit në përcaktimin e teknikës më të mirë të hetimit përpara zbatimit të saj. Krahas kësaj, ekspertët konsulentë mund të luajnë një rol aktiv në hetimin për shembull me anë të analizës së infrastrukturës së rrjetit në ambientet e të dyshuarit, me qëllim identifikimin e vendndodhjeve të mundshme të pajisjeve të ruajtjes së të dhënave. * Ruajtja/sekuestrimi/mbledhja e provave. Mbledhja e provave elektronike mund të ndodhë në vendndodhjen fizike ku janë ruajtur po ashtu edhe në vendndodhjen e largët. Hetuesit që fillojnë të bëjnë mbledhjen e provave (hetuesit e parë në vendngjarje) kanë një përgjegjësi të konsiderueshme për të gjithë procesin e hetimit. Nëse marrin vendime të këqija në lidhje me ruajtjen e të dhënave, gjurmë të rëndësishme mund të humbasin. Një shembull i sfidës së kësaj detyre është çështja sesi të trajtohen kompjuterët e ndezur të të dyshuarit. Zakonisht procedura e sugjeruar është shkëputja e energjisë elektrike nga kompjuteri në vend të fikjes së tij me anë të komandave të sistemit të operimit. Por në ato raste kur keqbërësi ka përdorur teknologjinë e kodimit, shkëputja e energjisë elektrike mund të çojë në ç’kodimin e skedarëve. Për këtë arsye hetuesi i parë në vendngjarje duhet të marrë një vendim në varësi të fokusit të hetimit.     Ekspertiza kriminalistike nuk është vetëm e disponueshme përsa i takon hetimeve në vendngjarje ku ruhen të dhënat përkatëse. Ekspertët e kriminalistikës mund të mbështesin gjithashtu një hetim duke përgatitur një kërkesë që i dërgohet kompanive shërbimofruese të Internetit dhe t’i ndihmojnë hetuesit në paraqitjen e historive adekuate të çështjeve, të cilat janë të nevojshme për të provuar besueshmërinë e provave të mbledhura .   * Analiza e teknologjisë kompjuterike dhe provave dixhitale. Faza tjetër trajton të gjitha aspektet e lidhura me analizën e provave dixhitale si dhe pjesëve fizike kompjuterike të sekuestruara. Në përgjithësi është faza më komplekse në të gjithë procesin e hetimit. Hetuesit e parë në vendngjarje shpesh sekuestrojnë disa pajisje dixhitale të ruajtjes së të dhënave. Secila prej këtyre pajisjeve përmban mijëra skedarë. Sasia e të dhënave që nevojitet të analizohet sjell sfida të mëdha për hetuesit. Identifikimi i informacionit përkatës për hetimin dhe lidhja e tij është një nga detyrat më të mëdha të ekspertëve të kriminalistikës dixhitale. Puna e tyre varion që nga kontrolli për përmbajtje të paligjshme në sistemin kompjuterik e deri tek analiza e skedarëve regjistrues. Jo të gjitha proceset e ndërmarra nga një keqbërës në kryerjen e krimeve kibernetike lënë gjurmë. Duke analizuar të gjitha provat e disponueshme, ekspertët kriminalistikë mund të rindërtojnë mënyrën sesi u krye një vepër penale. Faza e tretë përfshin gjithashtu prodhimin e një raporti të plotë, i cili përfshin ndër të tjera dhe hapat e hetimit dhe metodat e përdorura për të marrë provat.   **Shembuj të ekzaminimeve kriminalistike**  Brenda katër fazave (dhe veçanërisht brenda fazës së tretë) janë të mundura shumë ekzaminime kriminalistike. Zgjedhja e teknikës së duhur varet nga faktorë të ndryshëm – në veçanti, lloji i veprës penale që është në fokus të hetimit.  Ndër teknikat më të zakonshme janë të mëposhtmet:   * Analiza e komponentëve fizikë të sistemit kompjuterik. Nëse hetuesit sekuestrojnë pjesët fizike të kompjuterit, më pas ekspertët mund t’i analizojnë këto pjesë për të mbledhur informacion në lidhje me sistemin. Një hetim i tillë mund të jetë i lidhur me të provuarin nëse një keqbërës kishte mundësinë të lidhte sistemin kompjuterik në Internet. Analiza e komponentëve fizikë mund të ketë lidhje nëse – për shkak të transferimit të informacionit të sistemit gjatë një procesi regjistrimi – mësohet se i dyshuari përdori një konfigurim specifik të pjesëve fizike të kompjuterit. * Analiza e funksionimit të programeve kompjuterike. Përveç pjesëve fizike, programet kompjuterike luajnë një rol të rëndësishëm në funksionimin e një sistemi kompjuterik. Ekspertët e kriminalistikës dixhitale mund të përcaktojnë funksionet e një virusi ose një forme tjetër të programeve të dëmshme kompjuterike. Krahas kësaj, ata mund të rindërtojnë proceset e funksionimit të programeve. Më tej, analiza e programeve kompjuterike mund të jetë me rëndësi për përcaktimin nëse janë të kriminalizuara prodhimi ose shitja e programeve që mund të përdoren në mënyrë legjitime si dhe për qëllime të paligjshme (përdorim i dyfishtë). * Analiza e programit kompjuterik të instaluar në sistemin kompjuterik të të dyshuarit. Analiza e programit të instaluar në sistemin kompjuterik mund t’ju japë hetuesve informacion të vlefshëm për hetim të mëtejshëm. Kështu ndodh veçanërisht në lidhje me programet e kodimit dhe mjetet e përdorura për të fshirë skedarët në mënyrë të sigurt. Nëse një program i tillë është i instaluar në kompjuterin e të dyshuarit, hetime të mëtejshme mund t’i kenë në fokus këto çështje. * Identifikimi i informacionit dixhital që lidhet me çështjen. Të dhënat kompjuterike mund të ruhen në lloje të ndryshme pajisjesh dixhitale. Madje edhe brenda një disku ka mundësi të ndryshme se ku mund të ruhet një skedar. Identifikimi i vendit të ruajtjes së provave përkatëse është i vështirë.   Një prej tendencave të reja që paraqet sfida të tjera në identifikimin e informacionit dixhital është përdorimi në rritje i ruajtjes së largët të të dhënave. Siç u theksua më lart, disponueshmëria e aksesit broadband dhe e serverëve të largët për ruajtjen e të dhënave ka influencuar mënyrën e ruajtjes së informacionit. Duke shfrytëzuar një ruajtje të tillë të largët të të dhënave, i dyshuari mund të parandalojë sekuestrimin e pjesëve fizike të kompjuterit duke i mundësuar punonjësve të zbatimit të ligjit aksesin tek informacioni që ndodhet i ruajtur në pajisje të largëta. Analiza kriminalistike në këtë rast mund të përdoret për të verifikuar nëse i dyshuari ka përdorur pajisje të ruajtjes së të dhënave në largësi.  Identifikimi i informacionit përkatës dixhital nuk është i kufizuar vetëm tek skedarët. Bazat e të dhënave me programe kompjuterike të përdorura nga i dyshuari për gjetjen e informacionit në kompjuterin e tij mund të përmbajnë gjithashtu informacion. Madje edhe skedarët e përkohshëm të gjeneruar nga sistemi mund të përmbajnë prova për procedimet penale.   * Identifikimi i skedarëve të fshehur. Keqbërësit mund të përdorin teknika për fshehjen e skedarëve në një pajisje dixhitale me qëllim që të pengojnë institucionet e zbatimit të ligjit të analizojnë përmbajtjen e skedarëve. Ky është veçanërisht rasti me hetimet që kanë të bëjnë me përmbajtje të paligjshme. Hetimet kriminalistike mund të identifikojnë dosje të fshehura dhe t’i bëjnë ato të aksesueshme brenda analizës. * Rikuperimi i skedarëve të fshirë. Nëse keqbërësit përdorin instrumente për tu siguruar se skedarët janë të fshirë në mënyrë të sigurt, rikuperimi i këtij informacioni zakonisht nuk është i mundur. Por në rastet kur keqbërësit nuk janë në dijeni të këtyre mjeteve, fshirja e informacionit dixhital nuk i bën ata të padisponueshëm ndaj autoriteteve të zbatimit të ligjit sepse të dhënat mund të rikuperohen me anë të përdorimit të programeve të posaçme kompjuterike. * Ç’kodimi i skedarëve dhe volumeve të koduara dhe rikuperimi i fjalëkalimeve. Kriminelët janë duke e përdorur gjithnjë e më shumë teknologjinë e kodimit. Kjo teknologji krijon sfida të konsiderueshme për autoritetet e zbatimit të ligjit sepse ato nuk janë në gjendje të aksesojnë dhe ekzaminojnë informacionin e koduar. Gjatë analizës kriminalistike mund të ndërmerren veprime për të ç’koduar skedarët e koduar dhe pajisjet e ruajtjes së të dhënave. Krahas kësaj, ekspertët e kriminalistikës mund të mbështesin autoritetet në zhvillimin e strategjive për të hyrë tek skedarët e koduar – për shembull duke përdorur një program kompjuterik të quajtur key-logger.   Keqbërësit janë në gjendje jo vetëm të pengojnë aksesin tek të dhënat duke përdorur kodimin, por gjithashtu edhe të përdorin sistemet e mbrojtjes me fjalëkalime. Analiza kriminalistike mund të përdorë metodën e rikuperimit të fjalëkalimeve për të mundësuar aksesin e autoriteteve të zbatimit të ligjit në sistemet e mbrojtjes me fjalëkalime.   * Analiza e skedarëve të ruajtur. Skedarët e ruajtur në një pajisje dixhitale mund të analizohen në mënyra të ndryshme. Për shembull, ekzaminimet kriminalistike mund të fokusohen tek përmbajtja e skedarëve. Përveç ekzaminimit manual të skedarëve të dyshimtë, hetimet mund të përfshijnë kërkime automatike me fjalë kyçe për skedarë në formë tekstesh dhe mjete që kontrollojnë automatikisht imazhe të njohura në kompjuterin e të dyshuarit.   Siç u theksua më lart, të dhënat kompjuterike mund të manipulohen mjaft lehtë. Hetimet mund të provojnë se janë kryer ndryshime dhe falsifikime të dokumenteve dixhitale.  Krahas kësaj, hetimet mund të marrin në konsideratë të dhënat që përshkruajnë të dhëna të tjera. Këto lloj analizash mund të përcaktojnë kohën se kur është hapur ose modifikuar për herë të fundit dokumenti. Krahas asaj, analiza e këtyre të dhënave mund të përdoret për identifikimin e autorit të skedarit me një mesazh kërcënues ose numrin serial të aparatit fotografik që është përdorur për të prodhuar imazhin e pornografisë së të miturve.   * Analiza e autorësisë. Nëse tekstet kërcënuese ose fjalimet e urrejtjes janë postuar në blogje ose forume në Internet, analiza e skedarëve regjistrues mund të mos i çojë hetuesit tek autori i tekstit nëse i dyshuari vepron nga një Internet Cafe ose shfrytëzon shërbimet anonime të komunikimit. Analiza linguistike e sofistikuar mund të ndihmojë në përcaktimin nëse i dyshuari e shkroi tekstin përpara dhe e la informacionin që mund të ndihmojë në identifikimin e individit në këtë kontekst. * Ruajtja e integritetit të të dhënave. Siç u theksua më lart, mbrojtja e integritetit të provave dixhitale është thelbësore për pranueshmërinë në gjykatë. Ekspertët e kriminalistikës mund të garantojnë mbrojtjen e integritetit të skedarëve gjatë mbledhjes së provave. Kjo iu mundëson autoriteteve të zbatimit të ligjit në disa raste të evitojnë sekuestrimin e pjesëve fizike kompjuterike dhe të bëjnë kopjimin e skedarëve përkatës duke mbrojtur integritetin e tyre kundër çdo lloj modifikimi gjatë procesit të hetimit. Kjo përfshin në veçanti krijimin e imazheve të pajisjes dixhitale ku janë ruajtur të dhënat. * Gjurmimi i IP-së. Keqbërësit që përdorin Internetin për kryerjen e veprave penale (për shembull, shkarkimi i imazheve të pornografisë së të miturve ose sulmimi i sistemeve kompjuterike) lënë gjurmë. Analiza e të dhënave të trafikut, të tilla si ekzaminimi i skedarëve të regjistrimit të mbajtura nga serverët e Internetit, mund të çojë hetuesit në lidhjen e përdorur nga keqbërësit për tu futur në Internet. Hetime të tilla mund të jetë të vështira nëse keqbërësit përdorin teknologji Komunikimi anonime. Por edhe në ato raste hetimet nuk janë të pamundura. Një shembull është programi CIPAV (Computer and Internet Protocol Address Verifier[[91]](#footnote-92)) që është përdorur në Shtetet e Bashkuara të Amerikës për identifikimin e një të dyshuari që përdorte shërbime Komunikimi anonime. * Analiza e postës elektronike. E-mail-i është bërë një formë shumë popullore e komunikimit dhe për rrjedhojë luan një rol të rëndësishëm në kriminalistikën dixhitale. Meqë është relativisht e lehtë të identifikohet dërguesi i një email-i kërcënues ose me përmbajte të paligjshme bashkëngjitur, keqbërësit shumë shpesh përdorin adresa pa pagesë të postës elektronike të regjistruara me informacion të rremë. Edhe në ato raste, ekzaminimi i informacionit të kreut të mesazhit dhe skedarëve regjistrues të shërbimofruesit të Internetit në disa raste mund të mundësojë identifikimin e të dyshuarit. * Gjurmimi i transaksioneve financiare. Një numër krimesh – duke përfshirë shitjen e pornografisë së fëmijëve – përfshijnë transaksione financiare. Duke përdorur të dhënat nga sistemet dhe institucionet tregtare të përfshira në transaksionet financiare është e mundur të identifikohet keqbërësi. Një shembull i tillë është një hetim në Gjermani ku keqbërësit, të cilët shkarkuan pornografi të miturisht nga një uebsajt tregtar, u identifikuan nga kompanitë e tyre të kartave të kreditit që analizuan të dhënat e klientëve të tyre për identifikimin e klientëve që përdorën kartat e tyre të kreditit për blerjen e pornografisë së miturve në uebsajtin specifik. Hetime të tilla janë më të vështira nëse keqbërësit shfrytëzojnë metoda pagese anonime. * Mbledhja në kohë reale e të dhënave të trafikut dhe interceptimi i të dhënave të përmbajtjes. Hetimet financiare mund të përfshijnë monitorimin në kohë reale të të dhënave të transferuara që janë përpunuar. Ky Projekt i Këshillit të Evropës për Krimin Kibernetik [www.coe.int/cybercrime](http://www.coe.int/cybercrime) i mundëson hetuesve të reagojnë për procese në kohën e veprimit të të dyshuarit të hetimit. * Aktivitetet e monitorimit në lidhje me shërbimet e disponueshme për publikun. Shërbimet e disponueshme publikisht mund të përdoren për shkëmbimin e materialit të mbrojtur nga e drejta e autorit ose e materialeve të paligjshme. Shërbime të tilla brenda një hetimi mund të monitorohen nga ekspertët e kriminalistikës. Kjo përfshin për shembull vëzhgimin e forumeve me shërbimin e Chat-it. * Mbledhja e të dhënave nga distanca. Aktualisht është diskutuar nevoja për instrumente/mjete të mbledhjes së provave në distancë, pa e marrë vesh i dyshuari për hetimin që po kryhet në sistemin e tij.   Kryerja e hetimeve të tilla kërkon trajnim specifik dhe procedura të mirë përcaktuara që bazohen në metodologji dhe standarde të pranuara gjerësisht.  Si kryhen ekzaminimet kriminalistike  Ka dy mënyra në të cilat mund të kryhen hetimet për mbledhjen e provave:     * Operacionet manuale. Pavarësisht nga disponueshmëria e teknologjisë për automatizimin e proceseve hetimore, kriminalistika dixhitale mbetet në një shkallë të madhe punë manuale. Veçanërisht në ato hetime që kanë të bëjnë me sasi të mëdha të të dhënave, operacione të tilla manuale mund të ecin me vështirësi. * Mjetet e analizës. Disa prej proceseve – veçanërisht kërkimet me fjalë kyç, rindërtimi i skedarëve të fshirë ose ç’kodimi i materialeve të koduara – mund të automatizohet duke përdorur mjetet e sofistikuara të analizës kriminalistike.     Shumica e hetimeve kombinojnë operacionet manuale me përdorimin e programeve kompjuterike që automatizojnë proceset.     * Paraqitja/prezantimi i provave në gjykatë. Në përgjithësi, ekspertët kriminalistë nuk paraqesin prova në gjykatë, megjithatë ata mund të luajnë një rol të rëndësishëm në procedimet penale. Ekspertët mund të dalin në gjykim si dëshmitarë që ndihmojnë njerëzit e përfshirë në procedimin gjyqësor për të kuptuar proceset sesi u krijuan provat, procedurat e përdorura për mbledhjen e provave dhe vlerësimin e tyre. | | | |
| Slajdet 52 dhe 59 | Pjesa e Tretë – Çështjet Ligjore | | | |
|  | ÇËSHTJE SPECIFIKE NË LIDHJE ME MBLEDHJEN E PROVAVE DIXHITALE    Format moderne të kriminalitetit në rrjetet kompjuterike, kundër rrjeteve, ose brenda tyre kërkon mbështetjen e ekspertëve dhe oficerëve të specializuar për mbledhjen dhe analizimin e provave dhe realizimin e një paraqitjeje korrekte të tyre në gjykatë.    Sigurisht kjo nuk është gjë e re: ka shumë shekuj që ekspertët ndihmojnë gjyqtarët, prokurorët dhe avokatët të kuptojnë çështjet teknike. Për shembull, për shekuj me radhë, doktorët kanë qenë faktor thelbësor në përcaktimin, sqarimin dhe vlerësimin në gjykatë të shkakut të mundshëm të një vrasjeje me dashje nga aspekti mjekësor. Por çështja është se mjedisi dixhital nxjerr probleme të ndryshme dhe të vështira për tu zgjidhur.  Në fakt, zhvillimi i vazhdueshëm i teknikës nuk pasohet gjithmonë nga një rishikim i vazhduar dhe azhornim i instrumenteve ligjore dhe jo gjithmonë mjetet ligjore procedurale i legjitimojnë teknikat e mbledhjes së provave elektronike.  Nga ana tjetër, zakonisht, trajnimi fillestar dhe i vazhduar i agjentëve të zbatimit të ligjit, prokurorëve dhe gjyqtarëve, nuk ndjek evolucionin teknik pa vonesë.  Në këtë skenar, ka një paraqitje në rritje të veprave të reja penale, kuptimi i të cilave varet nga njohuritë specifike. Ekspertiza teknike nuk nevojitet thjesht të provojë aktivitetin kriminal; ajo nevojitet për të kuptuar me saktësi se cila është vepra penale në fokus. Megjithëse të gjithë e kuptojmë se ç’do të thotë “murder”[[92]](#footnote-93), dhe mjekët ekspertë na nevojiten të përcaktojnë shkakun e vdekjes, “Denial of service”[[93]](#footnote-94) është një vepër penale që përcaktohet nga të kuptuarit teknik të rrjeteve kompjuterike.  Në botë, shumica e vendeve nuk kanë rregulla specifike për provat elektronike. Disa prej tyre kanë rregulla të posaçme që rregullojnë, për shembull, interceptimin e komunikimeve. Por në përgjithësi, sistemet ligjore e bazojnë mbledhjen e provave elektronike në rregullat paraekzistuese, të aplikueshme në botën jashtë Internetit. Në disa raste, gjykata pranon realitetet e reja të provave, duke miratuar rregulla klasike; dhe në disa raste të tjera gjykata nuk i pranon. Në këto lloje situatash, duhet të shtohen dispozita të reja në kornizën ekzistuese ligjore.  Shumica e vendeve Evropiane nuk e kanë futur akoma legjislacionin në lidhje me provat elektronike dhe kriteret që gjykatat duhet të përdorin në ekzaminimin dhe vlerësimin e provave elektronike.  Mbledhja dhe vlerësimi i provave elektronike është aktivitet delikat, sepse zakonisht prek të drejtat themelore, të tilla si jeta private dhe fshehtësia e telekomunikimeve. Dhe nganjëherë nuk është e qartë për gjyqtarët nëse këto të drejta respektohen.  Krimi kibernetik është global. Faktet kriminale mund të ndodhin njëkohësisht në më shumë se një shtet dhe juridiksion. Për vetë natyrën e tij, krimi kibernetik është transnacional. Veprat penale të kryera brenda rrjeteve të komunikimit dhe informacionit krijonin probleme serioze për të sqaruar vendin se ku u krye vepra, dhe autoritetin kompetent të zbatimit të ligjit për zgjidhjen e çështjes. Konventa e Budapestit për Krimin Kibernetik nuk mund të zgjidhte të gjitha problemet që lidhen me këtë, por u përpoq të gjente zgjidhje për disa situata të vështira.  Palët në Konventë, si zakonisht dhe në çështjet e tjera, do të hetojnë veprat penale të kryera në territorin e tyre. Krahas kësaj, Konventa thotë se Palët duhet të deklarohen vetë kompetente për ndjekjen ligjore dhe gjykimin e çështjeve që kanë të bëjnë me qytetarët e tyre kur vepra penale është kryer jashtë vendit, me kusht që aktiviteti në fjalë të jetë i ndëshkueshëm sipas ligjit të brendshëm kur ndodhi vepra.  Kjo është një çështje praktike e rëndësishme. Megjithëse disa vende kanë dispozita që përcaktojnë juridiksionin e tyre universal, ky nuk është parim i njohur universalisht ose përgjithësisht.  Megjithatë, në shumë situata mund të jetë e vështirë të sqarohet se cila gjykatë ka juridiksion në përputhje me rregullat e përgjithshme. Për shembull, një vepër penale kompjuterike mund të kryhet në të njëjtën kohë në shumë vende mbi shumë viktima, ose mund të kryhet nga disa autorë nga vendndodhje të ndryshme.  Përderisa rregullat juridiksionale penale nuk janë harmonizuar në të gjitha vendet, mund të ndodhë fare mirë që dy gjykata në vende të ndryshme, të pretendojnë se kanë juridiksionin mbi një vepër të vetme, pavarësisht nga rregullat e përmbajtura në Konventën për Krimin Kibernetik.  Në nivelin e Bashkimit Evropian, është lëshuar një Direktivë e rëndësishme, në lidhje ekskluzivisht me mbledhjen e provave dixhitale: Direktiva 2006/24/EC, e Parlamentit Evropian dhe e Këshillit, e 15 Marsit 2006 ishte dokumenti i parë detyrues brenda Bashkimit Evropian në lidhje me ruajtjen e të dhënave të gjeneruara ose të përpunuara në lidhje me ofrimin e shërbimeve të komunikimeve elektronike të disponueshme për publikun ose me rrjetet publike të komunikimit. | | | |
|  | Ushtrime Praktike(sipas rastit)  Nuk është parashikuar ndonjë ushtrim praktik për këtë sesion të veçantë sepse nuk ka asnjë garanci se niveli i teknologjisë dhe aksesi në Internet për dhënien e ushtrimeve do të jetë i disponueshëm në të gjitha vendet.  Trajnerët në të ardhmen mund të kërkojnë të plotësojnë mësimin me futjen e ushtrimeve, ku trajnimi zhvillohet në një mjedis ku pajisjet janë të përshtatshme. | | | |
|  | **Kontrolli i Njohurive**  Për këtë kurs nuk është parashikuar ndonjë kontroll njohurish krahas atyre të renditura më lart. Nuk është kërkuar asnjë vlerësim zyrtar. | | | |
| Slajdet 63 dhe 64 | Përmbledhje  Trajneri duhet të përmbledhë dhe testojë njohuritë për objektivat e mëposhtëm për të garantuar se ato janë arritur gjatë sesionit:   * Të diskutojë llojet e ndryshme të provave elektronike * Të shpjegojë parimet e praktikave më të mira në lidhje me sekuestrimin dhe administrimin e provave elektronike * Të identifikojë vështirësitë e ofruara nga “mbledhja e provave me kompjuter të fikur”, “mbledhja e provave me kompjuter të ndezur” dhe burimet në Internet të provave elektronike * Të identifikojë vështirësitë e mbledhjes së provave nga një juridiksion tjetër * Të diskutojë çështjet e pranueshmërisë së provave elektronike në procedimet gjyqësore, përsa i takon autenticitetit, saktësisë, dhe plotësisë   Kjo mund të arrihet me anë të diskutimit në grup, pyetjes së pjesëmarrësve, një kuici apo metodave të tjera të njohura.  Ky mësim u përpoq të ofronte disa udhëzime në lidhje me llojin dhe nivelin e njohurive për provat elektronike që kërkohet nga Gjyqtarët dhe Prokurorët për përmbushjen e rolit të tyre me efektivitet. Nuk pretendon të jetë një analizë e plotë e çështjeve dhe sipas rastit tregon se ku mund të merret informacion i mëtejshëm.  Rekomandohet që hartuesit e trajnimi të garantojnë se materiali që përgatisin ata të jetë sa më i azhurnuar dhe të përfshijë çështjet më të fundit sepse ato kanë ndikim mbi sjelljen kriminale; impakti i tij mbi rregullat e provave, rregullat procedurale dhe ato ligjore brenda juridiksionit ku do të zhvillohet trajnimi. Ka ndryshime teknologjike që do të ndikojnë sistemin e drejtësisë penale, të tilla si ruajtja në gjendje solide e të dhënave dhe Web 2.0. Këto do të jenë çështje të rëndësishme për tu përfshirë në programet e trajnimit dhe kërkojnë përfshirje sepse bëhen më mbizotëruese. | | | |
| Mësimi 1.3.4 Bashkëpunimi Ndërkombëtar | | | **Kohëzgjatja: 90 Minuta** | |
| **Burimet material të nevojshme:**   * Kompjuter Laptop ose Kompjuter tavoline me Windows 7 dhe me Programin Office 2010 * Projektor * Prezantimi me PowerPoint | | | | |
| **Synimi:**  Ky sesion dëshiron të theksojë rëndësinë e bashkëpunimit ndërkombëtar dhe të paraqesë një vështrim të përgjithshëm për instrumentet e disponueshëm për bashkëpunimin ndërkombëtar në fushën e krimit kibernetik, kryesisht Konventa e Budapestit për Krimin Kibernetik – do të jetë një prezantim i instrumenteve të disponueshëm, mënyrave të përdorimit, afateve kohore dhe efektivitetit. | | | | |
| **Objektivat**  Në përfundim të sesionit, pjesëmarrësit do të jenë në gjendje të:   * Njohin dimensionin global të Internetit dhe dimensionin ndërkombëtar të krimit kibernetik * Shpjegojnë rëndësinë e bashkëpunimit ndërkombëtar dhe të njohin instrumentet e disponueshme për bashkëpunimin ndërkombëtar në fushën e krimit kibernetik * Identifikojnë nevojën për kanale efektive dhe shumë të shpejta për bashkëpunimin ndërkombëtar dhe instrumentet e disponueshme, mënyrat e përdorimit, afatet dhe efektivitetin * Përshkruajnë përpjekjet nga organizatat ndërkombëtare në lidhje me implementimin e modaliteteve të reja të bashkëpunimit ndërkombëtar * Diskutojnë Konventën e Budapestit për Krimin Kibernetik – të diskutojnë parimet e saj të përgjithshme, masat provizore dhe rrjetin 24/7 për ndihmën e ndërsjellë juridike | | | | |
| **Slajdet nr.** | | **Përmbajtja:** | | |
|  | | **Hyrja**  Ky sesion do të nënvizojë rëndësinë e bashkëpunimit ndërkombëtar për hetimin e çështjeve konkrete të krimeve kibernetike. Do të përshkruhen instrumentet e disponueshme për bashkëpunimin ndërkombëtar, kryesisht Konventa e Budapestit për Krimin Kibernetik. | | |
| **Slajdi 2** | | 1. Pjesa e Parë e prezantimit do të fokusohet në dimensionin ndërkombëtar të krimit kibernetik. Meqë kjo çështje u referua në sesionet e tjera, qasja këtu do të jetë shumë e shkurtër. 2. Në Pjesën e Dytë do të rendisim disa reagime ndaj krimit kibernetik në nivel ndërkombëtar. 3. Pjesa e Tretë, përsa i takon reagimit ndërkombëtar për krimin kibernetik, do të nënvizojë rolin e Konventës së Budapestit për Krimin Kibernetik. 4. Së fundi, Pjesa e Katërt do të fokusohet tek instrumentet e bashkëpunimit ndërkombëtar të përshkruara në Konventën e Budapestit. 5. Pjesa e Pestë do të rikuperojë temat kryesore të të gjithë prezantimit. | | |
| Slajdi 3 | | Objektivat e Sesionit  Qëllimi i këtij sesioni përgjithësisht është të njohë dimensionin global të Internetit dhe dimensionin ndërkombëtar dhe transnacional të krimit kibernetik.  Do të jenë si referencë bashkëpunimi ndërkombëtar dhe instrumentet e disponueshme për bashkëpunim ndërkombëtar në fushën e krimit kibernetik.  Do të nënvizohet nevoja për kanale efektive dhe shumë të shpejta të bashkëpunimit ndërkombëtar krahas dhënies së përshkrimit të instrumenteve të disponueshëm për një bashkëpunim të tillë.  Dhënia e një vështrimi të përgjithshëm të përpjekjeve nga organizatat ndërkombëtare në lidhje me implementimin e modaliteteve të reja të bashkëpunimit ndërkombëtar.  Në veçanti, do t’i referohemi Konventës së Budapestit për Krimin Kibernetik – duke identifikuar parimet e saj të përgjithshme, masat provizore dhe rrjetin 24/7 të ndihmës së ndërsjellë juridike. | | |
| Slajdi 4 | | Pjesa e Parë – Dimensioni ndërkombëtar i krimit kibernetik  Në një qasje shumë të shkurtër do të rishihet dimensioni ndërkombëtar i krimit kibernetik. | | |
| Slajdi 5 | | Është fakt i dukshëm se Interneti është shtrirë në të gjithë globin dhe mund të aksesohet dhe përdoret nga pothuaj të gjithë në botë.  Brenda rrjeteve, krimet po rriten. Dhe për pasojë, krimi kibernetik duhet të trajtohet si fenomen global. Realiteti i plotë i krimit kibernetik nuk mund te kuptohet pa njohur dimensionin ndërkombëtar. | | |
| Slajdi 6 | | Në këtë kontekst, krimi kibernetik është më transnacionali ndërmjet të gjitha krimeve. Dhe ata që duan të hetojnë krimin kibernetik duhet të jenë të ndërgjegjshëm se detyra e tyre kërkon bashkëpunim ndërkombëtar efiçent. Në fakt, duke qenë global në natyrë, pa bashkëpunim ndërkombëtar, hetimet për krimin kibernetik nuk kanë të ngjarë të jenë të suksesshme. | | |
| Slajdi 7 | | Konkretisht kur një vepër penale kryhet në hapësirën kibernetike, autoritetet e drejtësisë penale përballen me çështje të vështira, të cilat duhet të zgjidhen përpara të gjitha gjerave të tjera.  Duke ditur se Interneti është kudo, është gjithnjë e lehtë të përcaktohet vendndodhja ligjore relevante e veprës penale. Nëse, për shembull, keqbërësi vepron në vendndodhjen A dhe kompjuteri i viktimës së synuar është në vendndodhjen B, por komunikimi i paligjshëm i përdorur nga keqbërësi i realizuar nga shërbimofruesi me vendndodhje në C, dhe të gjitha këto vendndodhje i përkasin juridiksioneve të ndryshme, çështja e parë që autoritetet e zbatimit të ligjit duhet të zgjidhin është vendndodhja relevante ligjore e veprës penale përsa i takon juridiksionit. Duhet të jetë e qartë se ku është vendi i kryerjes së veprës penale, në mënyrë që të mund të përcaktohet se cili është ligji material dhe cili është juridiksioni kompetent (polici, prokurori, gjyqtari).  Hetuesi duhet të respektojë juridiksionin e tij – kompetencën e tij territoriale. Në përputhje me këndvështrimin e tij, juridiksioni do të jetë një kufi detyrues për hetimet penale.  Ky realitet ngre dy lloj çështjesh të pazgjidhura.   * E para ka të bëjë me hetimet ndërkufitare: si mundet të investigojë në mënyrë të ligjshme një punonjës i zbatimit të ligjit jashtë vendit të tij, nëse i nevojitet të veprojë me urgjencë? Si mund të marrë dhe mbledhë prova të ruajtura “në derën tjetër”, në një shtet tjetër nëse e ndjen se provat mund të zhduken shumë shpejt? * Çështja e dytë ka të bëjë me hetimin në “re”. askush nuk e di se ku mund të ruhen (fizikisht) të dhënat; supozohet të jenë ruajtur në “re”. Është e mundur që askush mos ta dijë se cili është juridiksioni kombëtar për disa të dhëna, në “re”. Si mund të marrë dhe mbledhë të dhënat e ruajtura në “re” një punonjës i zbatimit të ligjit, kudo që të jenë të ruajtura fizikisht? | | |
| Slajdet 9 dhe 10 | | Pjesa e Dytë – Reagimi ndërkombëtar ndaj krimit kibernetik  Meqë Interneti është shtrirë në të gjithë globin dhe përdoret sot nga potencialisht të gjithë në planet, krimi kibernetik duhet të trajtohet si një fenomen botëror. Qëllimi i Pjesës së Dytë është përshkrimi i disa prej hapave më të rëndësishëm si përgjigje ndaj krimit kibernetik brenda Evropës si një qasje praktike. | | |
| Slajdet 11 deri 13 | | Interpoli është një organizatë ndërkombëtare shumë e njohur, anëtarët e të cilit janë organe të zbatimit të ligjit nga e gjithë bota. Deri në Janar 2012, Interpoli numëron 190 anëtarë nga të gjitha kontinentet. Objektivi i tij është përmirësimi dhe lehtësimi i bashkëpunimit ndërkombëtar policor. Për këtë qëllim, Interpoli organizoi një sistem global komunikimi për policinë dhe zhvilloi databaza specifike dhe analiza të të dhënave të policisë.  Interpoli ishte një prej institucionet të para ndërkombëtare që tregoi preokupim për çështjet e krimit kibernetik, dhe një prej të parëve që organizoi grupet e diskutimit të ekspertëve për këtë çështje në vitin 1995. Që atëherë Interpoli zhvilloi përpjekjet e tij për të ndihmuar policinë dhe agjencitë e tjera të zbatimit të ligjit në të gjithë botën për forcimin e aftësisë së tyre për të luftuar krimin kibernetik.  Për të arritur këtë qëllim, Interpoli ndërtoi një rrjet pikash kontakti (Interpol National Central Reference Points - NCRP), i cili kërkon të japë asistencë tek anëtarët e tij në mënyrë të vazhdueshme. Deri në shtator 2011, NCRP kishte rreth 120 pika reference në të gjithë botën. Këto pika reference miratuan planin e pikave të kontaktit 24/7 të krijuara nga Neni 35 i Konventës së Budapestit për Krimin Kibernetik. Në disa prej vendeve që janë Palë në Konventë, pika e referencës së Interpolit u caktua edhe pika e kontaktit për G8-n. Të gjitha pikat e kontaktit të G8 u përfshinë në këtë rrjet. Objektivi i kësaj strukture ishte mundësimi i policisë të identifikojë menjëherë ekspertët në vendet e tjera dhe të marrë menjëherë asistencën për hetimet që lidhen me sistemet kompjuterike dhe mbledhjen e provave. Ky rrjet është i disponueshëm 24 orë në ditë, dhe shtatë ditë në javë.  Synimi i NCRP-s është realizimi i shkëmbimit të të dhënave dhe informacionit të policisë ndërmjet anëtarëve të saj dhe ofrimi i mbështetjes teknike dhe operacionale. Në fakt, synimi kryesor i NCRP-s është garantimi që të dhënat tipike të policisë të mund të shkëmbehen sa më shpejt që të jetë e mundur, nëpërmjet kanaleve specifike dhe të përshtatshme të Interpolit; kjo përfshin informacionin për terroristët e dyshuar, personat në kërkim, gjurmët e gishtërinjve, profilet e DNA-së, dokumentet e udhëtimit të humbura ose të vjedhura, automjetet e vjedhura, veprat e artit të vjedhura, etj. Ky lloj informacioni potencialisht i rëndësishëm është shumë i dobishëm për hetime konkrete. Megjithatë, për shkak të synimit të rrjetit, ai nuk mund të përdoret, për shembull, të kërkojë me urgjencë ruajtjen e të dhënave kompjuterike, ose ruajtjen e të dhënave të trafikut, apo ndonjë masë për marrjen ose ruajtjen e provave. Me fjalë të tjera, lloji i bashkëpunimit që mund të jepet nga ky rrjet specifik i Interpolit bazohet në të njëjtat parime që zbatohen për bashkëpunimin e përgjithshëm të Interpolit. | | |
| Slajdi 14 | | Bashkimi Evropian është mbështetës i Konventës së Budapestit – ai madje ka marrë pjesë, si vëzhgues, në hartimin e saj. Që atëherë, Bashkimi Evropian ka inkurajuar Shtetet Anëtare ta ratifikojnë atë. Në fakt, një numër i madh Shtetesh Anëtare e kanë ratifikuar atë dhe të gjithë e kanë nënshkruar.  Sigurisht, brenda Bashkimit Evropian, janë të disponueshme një sërë instrumentesh për bashkëpunim ndërkombëtar, edhe jashtë metodave më të fundit, bazuar në parimin e njohjes reciproke. Shumica e avantazheve të sistemit Evropian bazohen në mundësinë e kontakteve të drejtpërdrejta ndërmjet autoriteteve gjyqësore të secilit Shtet Anëtar. Në përputhje me këtë mundësi, secili gjyqtar ose prokuror mund të paraqesë direkt një kërkesë për një gjyqtar ose prokuror tjetër. Ky është një mjet shumë i fortë në lidhje me hetimin, gjithashtu i përshtatshëm në çështjet e krimit kibernetik. | | |
| Slajd 15 | | Krahas kësaj, në vitin 2005, Bashkimi Evropian miratoi një instrument detyrues në lidhje me një rrjet pikash kontakti 24/7, në lidhje me hetimet për krimin kibernetik – Vendimi Kuadër i Këshillit 2005/222/JHA i 24 Shkurtit 2005 për sulmet kundër sistemeve të informacionit. Ky Vendim Kuadër përfshin, në veçanti, rregulla që i referohen “rrjetit ekzistues të pikave të kontaktit” – Neni 11, 1, thotë se të gjithë Shtetet Anëtare të Bashkimit Evropian duhet të garantojnë se do të përdorin rrjetin ekzistues të pikave operacionale të kontaktit të disponueshme 24 orë në ditë dhe shtatë ditë në javë. Kjo është një dispozitë në lidhje me shkëmbimin e informacionit në lidhje me disa vepra penale të renditura (aksesi i paligjshëm në sistemet e informacionit, ndërhyrja e paligjshme në sistem, nxitja dhe ndërhyrja e paligjshme tek të dhënat, bashkëpunimi dhe tentativa).  Nuk thuhet shprehimisht në vendimin kuadër por është e qartë se *rrjeti ekzistues* është rrjeti i Këshillit të Evropës/G8. | | |
| Slajdi 16 | | Europoli është një organizatë autonome e Bashkimit Evropian, synimi i të cilës është përmirësimi i efektivitetit të bashkëpunimit ndërmjet autoriteteve të zbatimit të ligjit nga secili Shtet Anëtar i Bashkimit Evropian. Aktivitetet e tij, që nga viti 1999, përfshijnë lehtësimin e analizës së informacionit penal dhe ndarjen e të dhënave ndërmjet Shteteve Anëtare. Krimi Kibernetik është një prej fushave më të rëndësishme të aktivitetit të Europolit. Ndër mundësitë e tjera, Europoli mund të jetë një kanal i shkëlqyer për rritjen e efiçencës së dispozitave të Nenit 26 të Konventës së Budapestit, në lidhje me informacionet spontane.  Në Janar 2013 u themelua Qendra Evropiane për Krimin Kibernetik (EC3). | | |
| Slajdi 17 | | Asnjë nuk e di se ku do të arrijë në të ardhmen Eurojust-i por aktualisht është një agjenci e rëndësishme e Bashkimit Evropian, e dedikuar për bashkëpunimin gjyqësor (në prokurori dhe në gjyqësor), ndërmjet Shteteve Anëtare të Bashkimit Evropian. Synimi i Eurojust është bashkëpunimi ndërkombëtar në luftën kundër krimit me anë të koordinimit të aktiviteteve të kryera nga autoritetet kombëtare përgjegjëse për ndjekjen ligjore.  Në këtë kontekst, Eurojust-i ka kompetencë promovimin e koordinimit ndërmjet autoriteteve kompetente të Shteteve të ndryshme Anëtare dhe lehtësimin e implementimit të ndihmës së ndërsjellë juridike dhe të kërkesave të ekstradimit.  Eurojust-i u themelua, si person juridik, në Dhjetor 2000, mbas rekomandimit të bërë nga Këshilli Evropian Tamepere dhe ka nga një përfaqësues nga secili prej 27 Shtetet Anëtare. “Krimi Kompjuterik” është një prej fushave të kompetencës së Eurojust-it. | | |
| Slajdi 18 | | Rrjeti Gjyqësor Evropian në çështjet Penale u themelua në Qershor 1998 me synimin për luftuar kundër krimit të organizuar dhe terrorizmit në Bashkimin Evropian me anë të rritjes dhe thjeshtimit të bashkëpunimit ndërmjet autoriteteve gjyqësore.  Në fakt është një rrjet i pikave të kontaktit nga gjyqësori, bazuar në autoritetet qendrore të secili Shtet Anëtar përgjegjës për bashkëpunimin gjyqësor ndërkombëtar, pikat kombëtare të kontaktit, në secilin Shtet Anëtar, dhe në fund magjistratët ndërlidhës.  Një prej synimeve të Rrjetit Gjyqësor Evropian në çështjet Penale është dhënia e informacionit të detajuar, i disponueshëm për magjistratët, për të lehtësuar bashkëpunimin ndërkombëtar ndërmjet organizatave gjyqësore dhe urdhrave gjyqësorë. Në këtë kontekst, Rrjeti Gjyqësor Evropian për çështjet Penale zhvilloi Atlasin, një mjet kompjuterik, i cili i lejon përdoruesve të tij të identifikojnë lehtësisht autoritetin lokal kompetent në secilin Shtet Anëtar për marrjen dhe ekzekutimin e kërkesave reciproke për ndihmë juridike.  Supozohet që pikat e kontaktit janë të disponueshme për tu kontaktuar nga autoritetet gjyqësore lokale për lehtësimin e bashkëpunimit gjyqësor ndërmjet Shteteve Anëtare dhe gjithashtu për t’i mbështetur këto autoritete për përgatitjen e kërkesave për bashkëpunim gjyqësor.  Një lloj i tillë rrjeti, i cili realizon dërgimin shumë të shpejtë dhe të lehtësuar të kërkesave për bashkëpunim ndërkufitar, mund të jetë shumë i vlefshëm në mbledhjen e provave elektronike. | | |
| Slajdi 19 | | Konventa Evropian për Ndihmën e Ndërsjellë në çështjet Penale e Këshillit të Evropës nga viti 1959, është baza e dukshme e Konventës së Budapestit për Krimin Kibernetik. Në fakt, Konventa e Budapestit nuk mbulon të gjitha çështjet ekzistuese për bashkëpunimin ndërkombëtar; teksti thjesht flet për modalitete dhe kanale bashkëpunimi të shpejta, të reja, që nuk kanë ekzistuar më parë.  Të gjitha Shtetet Anëtare të Këshillit të Evropës (me përjashtim të San Marinos) e kanë ratifikuar këtë Konventë, që do të thotë se nga të gjitha Palët në Konventën e Budapestit, e vetmja Palë jo anëtare në Konventën e 1959 janë Shtetet e Bashkuara të Amerikës.  Ky fakt vërteton vlerën e shtuar të Konventës së Budapestit në krijimin për herë të parë të një kuadri të përbashkët ligjor për bashkëpunimin ndërkombëtar gjyqësor dhe policor ndërmjet shumicës së Shteteve Evropiane dhe Shteteve të Bashkuara. Ky është një aspekt i rëndësishëm sepse Neni 14, 2, thotë se procedurat për bashkëpunimin ndërkombëtar të Konventës do të zbatohen edhe për veprat penale të parashikuara në përputhje me Nenet 2 deri 11 të Konventës, si dhe për veprat e tjera penale të kryera me anë të sistemeve kompjuterike dhe për mbledhjen e provave në formë elektronike për çdo vepër tjetër penale. | | |
| Slajdi 21 | | Pjesa e Tretë – Reagimi ndërkombëtar ndaj krimit kibernetik: Konventa e Budapestit për Krimin Kibernetik | | |
| Slajdet 22 deri 25 | | Siç u përmend në mësimet e tjera, Konventa e Budapestit u hap për nënshkrim në 23 Nëntor 2001 dhe hyri në fuqi në Korrik 2004. Deri në Prill 2013, 57 Shtete janë ose Palë, nënshkrues ose janë ftuar të aderojnë.  Në rastet e hetimit të çështjeve konkrete të krimit kibernetik, Palët në Konventë fitojnë mundësinë e përdorimit, kryesisht kur kërkohet bashkëpunim ndërkombëtar, të mjeteve të reja dhe inovative të hetimit. Këto mundësi të reja mund të përdoren kur krimi në hetim është një nga veprat penale të përcaktuara në Konventë, por gjithashtu edhe në raste të tjera, nëse vepra penale është kryer me anë të një sistemi kompjuterik ose provat e krimit janë ruajtur ose regjistruar me pajisje dixhitale. Kjo thuhet në Nenin 14 të Konventës.  Ishte hera e parë që komuniteti ndërkombëtar bëri përpjekje të përbashkëta për të rënë dakord për një marrëveshje universale për çështje që lidhen me krimin kibernetik dhe provat elektronike, me shpresën që më në fund shumica e Shteteve do të mbështesnin këtë qëllim. Sot, ajo mbetet instrumenti i parë dhe i vetëm detyrues ndërkombëtar për krimin kibernetik.  Secili shtet që ratifikon Konventën dhe bëhet Palë fiton në proces një akses në forumin universal të bashkëpunimin, edhe me forcat e policisë edhe me organet gjyqësore.  Konventa prezanton kanale të reja për bashkëpunimin ndërkombëtar. Disa prej dispozitave të saj janë shumë inovative dhe të jashtëzakonshme, por mund të konsiderohen si përgjigje adekuate dhe të domosdoshme ndaj realiteteve të reja të kriminalitetit kibernetik.  Megjithatë, Konventa për Krimin Kibernetik nuk kërkon të jetë i vetmi instrument i detyrueshëm ndërkombëtar për bashkëpunimin ndërkombëtar. Deklarohet në Konventë në Nenin 23 se vetë Konventa do të jetë e zbatueshme në kuadër të instrumenteve të tjerë ekzistues për bashkëpunimin ndërkombëtar në çështjet penale. Për pasojë, Neni 27 përshkruan parimet e përgjithshme që duhet të respektohen në mungesë të traktateve ose konventave ndërkombëtare të zbatueshme.  Nga ana tjetër, duhet të nënvizohet se rregullat e prezantuara nga nenet e Konventës krijojnë kanale dhe mjete të reja bashkëpunimi ndërmjet Palëve që nuk lejoheshin nga ndonjë instrument tjetër i mëparshëm. | | |
| Slajdi 27 | | Pjesa e Katërt – Konventa e Budapestit – instrumentet e bashkëpunimit ndërkombëtar  Rregullat e Konventës, përsa i takon bashkëpunimit ndërkombëtar, përshkruhen në kapitullin III të konventës. Shumica e rregullave në këtë kapitull janë rregulla procedurale dhe operacionale, gjithashtu të përbashkëta edhe për konventa të tjera ndërkombëtare. Të tjerat janë shumë inovative dhe duhet të eksplorohen më në detaj. | | |
| Slajdet 28 dhe 29 | | Neni 26 përshkruan situatën që ndodh kur autoritetet e një Pale, gjatë një hetimi të brendshëm, zbulojnë se një pjesë e informacionit që mbledhin duhet t’i kalohet autoriteteve të një Pale tjetër – por pa nevojën e pasjes së një kërkese nga ajo Palë. Kjo mund të bëhet nëse informacioni duket i dobishëm ose i nevojshëm për të filluar një hetim për një vepër penale në kuadër të Konventës. Megjithëse në të kaluarën ndihma e ndërsjellë ishte zakonisht pasive, shteti A kërkon ndihmë nga shteti B, Konventa nxit një qasje më proaktive. Megjithatë, kjo dhënie “spontane” informacioni, në përputhje me Nenin 26 pikën 2, mund t’i nënshtrohet disa kushteve, si për shembull kërkesës për konfidencialitet ose për përdorim specifik të të dhënave. | | |
| Slajdet 30 deri 32 | | Neni 29 është një prej dispozitave më të rëndësishme të Konventës së Budapestit. Neni 29 përcakton rregullat në lidhje me ruajtjen e përshpejtuar të të dhënave të mbajtura në një sistem kompjuterik. Ai përcakton një kuadër paralel me dispozitat e brendshme në lidhje me ruajtjen e përshpejtuar të të dhënave. Në përgjithësi, kjo dispozitë i lejon një Pale kontraktore t’i kërkojë një Pale tjetër ruajtjen e përshpejtuar të të dhënave, nëse në të njëjtën kohë ajo shpreh qëllimin e bërjes së një kërkese zyrtare për ndihmë në një kontroll, apo një sekuestrim, apo ndonjë masë tjetër të ngjashme.  Në këtë rast, pala e kërkuar duhet të veprojë si të jetë e nevojshme, me të gjithë kujdesin e duhur, për ruajtjen e të dhënave të kërkuara, në përputhje me ligjin e saj të brendshëm.  Siç u përmend më lart, ky është një instrument i ri i bashkëpunimit ndërkombëtar. Ky është një instrument i ri si rezultat i specifikës së mjedisit dixhital. Ndihma ndërkufitare konsumon shumë kohë. Karakteri përshpejtues i masës është një nevojë e imponuar nga nevoja për të ruajtur diçka që në pak momente mund të fshihet tërësisht.  Është me vend të theksojmë se kjo është një masë mbrojtëse për arsye urgjente dhe nuk nënkupton automatikisht zbulimin e të dhënave të ruajtura. Në fakt, në rastet kur lejohet zbulimi i të dhënave, ka rregulla shumë të ngushta që e lejojnë këtë, mbi të gjitha nëse të dhënat nuk janë thjesht të dhëna trafiku.  Praktikisht, ruajtja e përshpejtuar e të dhënave mund të realizohet dhe pastaj më vonë ka arsye për moszbulimin e këtyre të dhënave për palën kërkuese.  Është e rëndësishme të merret parasysh se kriminaliteti i dyfishtë nuk mund të kërkohet nga pala e kërkuar, si kusht për mbrojtjen e të dhënave. | | |
| Slajdet 33 dhe 34 | | Zbulimi i të dhënave të trafikut përshkruhet në Nenin 30 të Konventës së Budapestit. Në lidhje me të dhënat e trafikut, teksti i Konventës parashikon një model më të lehtë për lehtësimin e bashkëpunimit ndërkombëtar. Nuk ka rregulla specifike për zbulimin e përshpejtuar të të dhënave, sepse nuk ka rregulla specifike për zbulimin e përshpejtuar në nivelin kombëtar, në kapitullin e rregullave procedurale. Në fakt, pa e thënë shprehimisht Konventa harmonizon rregullat kombëtare të zbulimit dhe mbrojtjes së përshpejtuar të provave dhe ato që rregullojnë bashkëpunimin ndërkombëtar. | | |
| Slajdet 35 dhe 36 | | Neni 31 i Konventës përcakton një rregull të përgjithshëm për ndihmën e ndërsjellë në lidhje me aksesimin e të dhënave kompjuterike të ruajtura. Megjithëse ky nen, dhe Neni 23 të cilit i referohet, shprehin aspiratën e përgjithshme që palët të bashkëpunojnë në ndjekjen ligjore të krimit kibernetik në “shkallën më të gjerë të mundshme”, nuk krijon detyrime të reja për bashkëpunim. I gjithë bashkëpunimi i nënshtrohet traktateve dhe instrumenteve ndërkombëtare ekzistues që rregullojnë bashkëpunimin ndërkufitar në hetimet tradicionale.  Praktikisht, Neni 31 sjell rregulla të përgjithshme në mjedisin kibernetik që zbatohen në jetën reale për vite me radhë. | | |
| Slajdet 37 dhe 38 | | Neni 32 përcakton mundësinë që i është dhënë agjencive të zbatimit të ligjit nga një Shtet Palë në Konventë, të marrin provat e ruajtura në një kompjuter fizikisht të ndodhur në territorin e një Pale tjetër, pa ndonjë kërkesë për bashkëpunim ndërkombëtar. Kjo mund të bëhet nëse, gjatë një hetimi konkret, oficerët përgjegjës kanë nevojë të marrin informacion nga një burim i hapur nga një kompjuter i ndodhur në një shtet të huaj ose nga një kompjuter, aksesi në të cilin u autorizua nga një person i autorizuar në mënyrë të ligjshme.  Përsa i takon informacionit me burim të hapur, duhet të vërehet se ky hetim “me burim të hapur” është diçka që mund ta bëjë çdo qytetar, me iniciativë, në shumicën e vendeve. Kjo dispozitë synon thjesht të autorizojë agjentët e zbatimit të ligjit ta bëjnë dhe ata gjithashtu këtë gjë, në të njëjtën kohë, të kualifikojnë si vlefshme provat e marra në këtë mënyrë.  Por nga ana tjetër dispozita ka një qasje shumë të re. Nuk ka ekuivalent në botën fizike për këtë mundësi të re: në të kaluarën, një oficer duhet të udhëtonte fizikisht në shtetin tjetër dhe të kërkonte ndihmën e autoriteteve lokale. Ai nuk mund të bënte gjithçka vetë dhe çdo veprim i hetimit do të bëhej në emër të autoriteteve të atij vendi.  Neni 32 thotë të kundërtën. Sipas këtij neni, çdo punonjës i zbatimit të ligjit nga çdo vend i botës mund të marrë informacion nga një vend tjetër, edhe sikur të mos jetë informacion “me burim të hapur”, nëse personi që ka autoritetin e ligjshëm për të zbuluar të dhënat jep pëlqimin e tij/saj të ligjshëm dhe të vullnetshëm. Ai aktivitet hetimor nuk ka nevojë për ndonjë autorizim të Shtetit me juridiksionin e vendit ku ruhet informacioni. Disa Shtete nuk e pranojnë Konventën për shkak të këtij hartimi. Ata pretendojnë se është kundër parimit të sovranitetit. Megjithatë, nuk ka as një propozim ose ndonjë zgjidhje tjetër për problemet komplekse të hetimeve ndërkufitare ose hetimeve në “re”. Jeta reale zbulon se në shumicën e rasteve është e pamundur të hetohet krimi kibernetik ose të mblidhen provat elektronike në nivel ndërkombëtar, duke përdorur kanalet tradicionale. Është e pamundur sepse koha që nevojitet nuk përputhet me paqëndrueshmërinë dhe brishtësinë e provave elektronike. Kjo është arsyeja se pse një hetim ndërkufitar i kryer nga autoritetet e zbatimit të ligjit do të ishte me efiçent.  Por nga ana tjetër, nganjëherë është vërtet e pamundur të përdoren kanale të rregullta të bashkëpunimit – në lidhje me shërbimet në “re”, përdoruesit (dhe hetuesi) nuk e dinë ekzaktësisht se ku janë ruajtur fizikisht të dhënat e kërkuara nga policia. | | |
| Slajdet 39 dhe 40 | | Neni 33 ka të bëjë me bashkëpunimin ndërkombëtar në lidhje me interceptimin e komunikimeve. Ky nuk është një instrument i ri ndërkombëtar për bashkëpunimin: instrumentet e tjerë detyrues ndërkombëtar i referohen atij. Megjithatë, neni 33 ka një fushëzbatimi specifike: mbledhjen në kohë reale të të dhënave të trafikut.  Nga ana tjetër, rregulli më i rëndësishëm i përcaktuar në nenin 33 tregon kufijtë e zbatimit të kësaj mase hetimi. Dhe kufijtë janë kushtet dhe procedurat e parashikuara në ligjin e brendshëm. Pra, ky modalitet i bashkëpunimit do të ofrohet nga çdo Shtet në disa raste për të cilat do të jetë e disponueshme mbledhja në kohë reale e të dhënave të trafikut në një çështje të ngjashme të brendshme. | | |
| Slajdet 41 deri 43 | | Neni 35 është një nga dispozitat më të rëndësishme operacionale të Konventës. Neni 35 i imponon të gjithë palëve kontraktore detyrimin për të krijuar një pikë kontakti të përhershme (një të ashtuquajtur rrjet 24/7 pikash kontakti).  Objektivi i përgjithshëm i këtyre pikave të kontaktit është lehtësimi i bashkëpunimit ndërkombëtar. Këto mund ta realizojnë këtë duke dhënë konsulencë teknike për pikat e tjera të kontaktit, duke aktivizuar mekanizmin e mbrojtjes së përshpejtuar të të dhënave, mbledhja me urgjencë e provave, ose identifikimi dhe zbulimi i të dyshuarve.  Ky rrjet operacional i ekspertëve për kriminalitetin e teknologjisë së lartë u ngrit për të ndihmuar ekspertët e tjerë, nga vendet ose juridiksionet e tjera, në hetimet penale me lidhjet ndërkombëtare. Ai dëshiron të përballet me sfidat e reja që vijnë nga kriminaliteti i shpejtë i teknologjisë së lartë. Nganjëherë, hetimet për krimet kompjuterike duhet të mbrojnë me shpejtësi të dhënat elektronike, në mënyrë që të jetë e mund të gjendet dhe ndiqen ligjërisht të dyshuarit. Kjo nevojë e re nuk mund të përmbushet nga ndonjë kanal tradicional i bashkëpunimit ndërkombëtar. Kjo është vlera e shtuar e këtij rrjeti: ai mund të ofrojë ndihmë dhe bashkëpunim shumë shpejt edhe sikur kërkesa zyrtare për bashkëpunim të ndjekë një rrugë informale. | | |
|  | | **Ushtrime Praktike (sipas rastit)**  Për këtë sesion nuk është përgatitur ndonjë ushtrim praktik | | |
|  | | Kontrolli i Njohurive  Trajneri duhet të kontrollojë njohuritë duke bërë pyetje për secilin nga aspektet e sesionit. | | |
| **Slajdet 45 dhe 46** | | Përmbledhje  Trajneri duhet të përmbledhë/testojë njohuritë për pikat e mëposhtme:   * Njohja e dimensionit global të Internetit dhe dimensioni ndërkombëtar i krimit kibernetik * Të shpjegojë rëndësinë e bashkëpunimit ndërkombëtar dhe të njohë instrumentet e disponueshme për bashkëpunimin ndërkombëtar në fushën e krimit kibernetik * Të identifikojë nevojën e kanaleve efiçente dhe shumë të shpejta për bashkëpunimin ndërkombëtar dhe instrumentet e disponueshme, mënyrat e tyre të përdorimit, afatet kohore dhe efektivitetin * Të përshkruajë përpjekjet nga organizatat ndërkombëtare në lidhje me implementimin e modaliteteve të reja të bashkëpunimit ndërkombëtar * Të diskutojë Konventën e Budapestit për Krimin Kibernetik – të identifikojë parimet e saj të përgjithshme, masat provizore dhe rrjetin 24/7 për ndihmën e ndërsjellë juridike | | |

|  |  |  |
| --- | --- | --- |
| Mësimi 1.3.5 Mbyllja e Kursit | | **Kohëzgjatja 90 Minuta** |
| **Burimet materiale të nevojshme:**   * Kompjuter Laptop ose Kompjuter tavoline me Windows 7 dhe me Programin Office 2010 * Projektor * Prezantimi me PowerPoint * Formularët e vlerësimit për pjesëmarrësit | | |
| **Synimi:**  Ky sesion është hartuar të lejojë pjesëmarrësit të japin vlerësimin e tyre për kursin dhe të ndihmojnë trajnerin në identifikimin e përmirësimeve që duhet të bëhen. I takon gjithashtu trajnerit të bëjë përmbledhjen e përmbajtjes së kursit duke iu referuar synimit dhe objektivave. | | |
| **Objektivat:**  Në përfundim të sesionit pjesëmarrësit do të jenë në gjendje të:   * Japin vlerësimin e duhur për kursin dhe efektivitetin e tij * Të plotësojnë formularët e vlerësimit të Këshillit të Evropës * Të identifikojnë nivelin tjetër të trajnimit që ata duhet të bëjnë për të përmirësuar njohuritë dhe aftësitë e tyre në këtë fushë. | | |
| **Hyrje**  Ky është një sesion i rëndësishëm i kursit dhe duhet të përdoret për të marrë vlerësimin nga pjesëmarrësit në lidhje me përmbajtjen e kursit dhe metodologjinë e përdorur për ta realizuar këtë kurs. Formularët e vlerësimit duhet të plotësohen dhe përfundohen gjatë këtij sesioni. Trajneri duhet të bëjë përmbledhjen gjatë gjithë sesionit dhe të kontrollojë nëse janë përmbushur objektivat. Sapo sesioni të përfundojë trajneri është përgjegjës për të garantuar se është marrë i gjithë vlerësimi dhe se të gjitha ndryshimet që mund të dalin të nevojshme të jenë të përfshira në kurs ose si modifikim i vogël në vazhdim ose gjatë një azhurnimi të madh modifikues të materialit. | | |
| **Slajdet nr.** | **Përmbajtja:** | |
| **Slajdi 1** | **Prezantim me PowerPoint** (ose ndonjë lloj tjetër prezantimi)  Prezantimi me PowerPoint jepet për të ndihmuar trajnerin në inkurajimin e diskutimit për të gjitha sesionet e kursit. Trajneri duhet të dorëzojë formularët e vlerësimit përpara fillimit të sesionit. Në disa rrethana, mund të jetë e përshtatshme të jepen formularët e vlerësimit në fillim të kursit me qëllim që pjesëmarrësit mund t’i plotësojnë gjatë zhvillimit të kursit dhe ndërsa e kanë informacionin të freskët në mendje. Ka gjithashtu një tendencë në fund të kursit që njerëzit të mos i plotësojnë ato tërësisht. | |
| **Slajdet 2 dhe 3** | Si me të gjitha mësimet e tjera të mëparshme, kjo duhet të ndjekë një formë të ngjashme me axhendë dhe objektiva për sesionin të përcaktuara në fillim të mësimit. | |
| Slajdet 4 deri 21 | Axhenda është një mënyrë e dobishme për të kujtuar pjesëmarrësit për përmbajtjen e kursit dhe është përfshirë për të ndihmuar trajnerin  Trajneri duhet të bëjë përmbledhjen e axhendës dhe objektivave të sesionit për secilin nga sesionet. Vlerësimi dhe sugjerimet nga pjesëmarrësit duhet të mbahen shënim për përdorim të ardhshëm. | |
| Slajdi 22 | Është përgjegjësia e trajnerit për të garantuar se pjesëmarrësit i kanë plotësuar formularët e vlerësimit. Trajneri duhet të mbledhë formularët e plotësuar dhe t’ia dorëzojë ato trajnerit në kurs ose t’ia kthejë ato këtij të fundit në rastin më të parë. | |
|  | **Ushtrime Praktike** (sipas rastit)  Përveç plotësimit të formularëve të vlerësimit, nuk ka asnjë ushtrim praktik të shoqëruar me këtë sesion. | |
|  | **Kontrolli i Njohurive**  Sesioni vazhdon me trajnerin që kontrollon njohuritë e fituara nga pjesëmarrësit duke bërë pyetje gjatë fazës së vlerësimit. | |
|  | **Përmbledhje**  Trajnerët duhet të sigurohen se pjesëmarrësve iu janë dhënë mundësi të mjaftueshme për të dhënë vërejtjet/komentet e tyre dhe këto të fundit duhet të mbahen shënim. | |

# Vlerësimi

Vlerësimi është pjesë e rëndësishme e një kursi trajnues dhe duhet të kushtohet koha që duhet që pjesëmarrësit të japin vlerësimin e tyre për mësimin në kurs.

Ky kurs është zhvilluar si një kurs i përgjithshëm dhe si i tillë shumica e materialeve të trajnimit janë me Power Point dhe pa nivelin e ushtrimeve praktike që zakonisht mund të shoqërojnë këtë lloj kursi.

Është përgatitur një formular vlerësimi dhe është vendosur në këtë seksion. Trajnerët janë përgjegjës për të garantuar që formularët të plotësohen dhe t’i kthehen Këshillit të Evropës me qëllim që të bëhen përmirësime për zhvillime të mëtejshme të kursit.

# Vlerësimi

Nuk është kërkuar asnjë vlerësim për këtë kurs; megjithatë ata që do të shpërndajnë materialet në të ardhmen, veçanërisht ato në vendet ku kursi mund të jetë pjesë e një programi mund ta rivlerësojnë këtë. Nëse do të ketë një vlerësim, duhet të përdoren metodologjitë e atij vende që vendos të bëjë vlerësimin në fund të kursit.

**Shtojcë**

**Materialet e trajnimit dhe materialet për pjesëmarrësit**

1. Projekti i Përbashkët për Krimin Kibernetik @IPA ndërmjet Bashkimit Evropian dhe Këshillit të Evropës (Bashkëpunimi Rajonal në Drejtësinë Penale: Forcimi i kapaciteteve në luftën kundër krimit kibernetik) ka për synim forcimin e kapaciteteve të autoriteteve të drejtësisë penale në Ballkanin Perëndimor dhe Turqi për të bashkëpunuar me efektivitet kundër krimit kibernetik. [↑](#footnote-ref-2)
2. \* Të gjitha referencat për Kosovën, nëse janë territoriale, institucionale ose për popullsinë, në këtë tekst do të kuptohen në përputhje të plotë me Rezolutën 1244 të Këshillit të Sigurimit të Kombeve të Bashkuara dhe pa paragjykim për statusin e Kosovës. [↑](#footnote-ref-3)
3. Hyrje e paautorizuar në një sistem kompjuterik. Shën. i përkthyesit [↑](#footnote-ref-4)
4. Programe të vogla të dëmshme për sistemet kompjuterike. Shën. i përkthyesit [↑](#footnote-ref-5)
5. Programe të vogla të dëmshme që nëse hyjnë në sistemet kompjuterike riprodhojnë veten dhe përhapen nëpërmjet rrjeteve kompjuterike. Shën. i përkthyesit [↑](#footnote-ref-6)
6. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l\_069/l\_06920050316en00670071.pdf [↑](#footnote-ref-7)
7. Mesazhe elektronike të pakërkuara nga marrësi në sasi të mëdha për qëllime tregtare ose qëllime të tjera. Shën. i Përkthyesit [↑](#footnote-ref-8)
8. Lidhje e drejtpërdrejtë ndërmjet dy njerëzve në rrjet pa patur nevojë që komunikimi i tyre të kalojë nëpërmjet ndonjë kontrollori rrjeti, për të mundësuar ndarjen e skedarëve dhe materialeve të tjera. Shën i Përkthyesit [↑](#footnote-ref-9)
9. Mashtrimi Nigerian: mashtrim me pagesën e paradhënieve, të kërkuara me anë të mesazheve elektronike. Shën i Përkthyesit [↑](#footnote-ref-10)
10. Tentativë për të marrë të dhënat personale të dikujt me mashtrim, duke i dërguar një email me njoftim të rremë. Shën i Përkthyesit [↑](#footnote-ref-11)
11. Rrjet sistemesh kompiuterike me programe të dëmshme që kryejnë detyra të automatizuara sipas udhëzimeve të personit që i çon programet e dëmshme në këto rrjete, si p.sh. dërgimi i automatizuar i emailave të padëshiruar, nga kompjutera të ndryshëm pa dijeninë e pronarit të tyre. [↑](#footnote-ref-12)
12. I dëmshëm [↑](#footnote-ref-13)
13. Program kompjuterik [↑](#footnote-ref-14)
14. Program kompjuterik i dëmshëm [↑](#footnote-ref-15)
15. Rrjete Robot [↑](#footnote-ref-16)
16. Gjysëmpërçues plotësues prej oksidi metalik [↑](#footnote-ref-17)
17. Sistemi bazë input/output [↑](#footnote-ref-18)
18. Njësia Qëndrore e Përpunimit të të Dhënave [↑](#footnote-ref-19)
19. Marrja e të dhënave me kompjuter të ndezur” [↑](#footnote-ref-20)
20. Njësitë e Diskut të Ngurtë [↑](#footnote-ref-21)
21. Njësia e të dhënave [↑](#footnote-ref-22)
22. Mbajtja e të Dhënave në Gjendje të Ngurtë [↑](#footnote-ref-23)
23. Rrjet i Ndërlidhur [↑](#footnote-ref-24)
24. Gjerësia e valës. Shën i Përkthyesit [↑](#footnote-ref-25)
25. Pajisje për drejtimin e të dhënave në rrjet. Shën i përkthyesit [↑](#footnote-ref-26)
26. Rrjetet personale. Shën i përkthyesit [↑](#footnote-ref-27)
27. Rrjetet e universiteteve. Shën i përkthyesit [↑](#footnote-ref-28)
28. Rrjetet e qyteteve të mëdha. Shën i përkthyesit [↑](#footnote-ref-29)
29. Gjerësia e valës. Shën i përkthyesit [↑](#footnote-ref-30)
30. Karta e rrjetit. Shën i përkthyesit [↑](#footnote-ref-31)
31. Numër identifikim unik për çdo pajisje. Shën i Përkthyesit [↑](#footnote-ref-32)
32. Pajisje për lidhjen e segmenteve të ndryshme të rrjetit kompjuterik. Shën i Përkthyesit [↑](#footnote-ref-33)
33. Është një lloj memorjeje kompjuterike që përdoret në disa lloj programesh për kërkime shumë të shpejta. Shën i Përkthyesit. [↑](#footnote-ref-34)
34. Pajisje për drejtimin e të dhënave në rrjet. Shën i përkthyesit [↑](#footnote-ref-35)
35. Pa lidhje. Shën i përkthyesit [↑](#footnote-ref-36)
36. Me shkëmbim paketash informacioni. Shën i përkthyesit [↑](#footnote-ref-37)
37. Protokolli i Internetit. Protokoll i përdorur për komunikimin e të dhënave nëpërmjet rrjetit. Shën i përkthyesit [↑](#footnote-ref-38)
38. Protokolli i transferimit të komunikimeve. Shën i përkthyesit [↑](#footnote-ref-39)
39. Protokolli i Transferimit të Postës Elektronike. Shën i përkthyesit [↑](#footnote-ref-40)
40. Protokolli i Transferimit të Skedarëve. Shën i përkthyesit [↑](#footnote-ref-41)
41. Protokolli i Transferimit të Lajmeve dhe Diskutimeve nga një server tek një tjetër. Shën i përkthyesit [↑](#footnote-ref-42)
42. Funksionojnë “nëpërmjet” IP-së. Shën i përkthyesit [↑](#footnote-ref-43)
43. Kompani ofruese e shërbimit të Internetit. Shën i përkthyesit [↑](#footnote-ref-44)
44. Nëpërmjet një linje telefonike tokësore. Shën i përkthyesit [↑](#footnote-ref-45)
45. Nëpërmjet një linje telefonike ADSL (Asymmetric Digital Subscriber Line). Shën i përkthyesit [↑](#footnote-ref-46)
46. Nëpërmjet një linje telefonike tokësore. Shën i përkthyesit [↑](#footnote-ref-47)
47. Pa kabëll. Shën i përkthyesit [↑](#footnote-ref-48)
48. Procesi i modifikimit të informacionit të një adrese rrjeti kur kalon nëpër pajisjet e drejtimit të trafikut në rrjet. Shën i përkthyesit [↑](#footnote-ref-49)
49. Program kompjuterik ose sistem sigurie në rrjet, që kontrollon trafikun hyrës dhe dalës të rrjetit. Shën i Përkthyesit [↑](#footnote-ref-50)
50. Pajisje për drejtimin e të dhënave në rrjet. Shën i përkthyesit [↑](#footnote-ref-51)
51. Komunikimet me zë nëpërmjet Internetit. Shën i Përkthyesit [↑](#footnote-ref-52)
52. Luftëtarët e Rrjetit. Shën i Përkthyesit [↑](#footnote-ref-53)
53. Versioni 4 i IP-së. Shën i Përkthyesit [↑](#footnote-ref-54)
54. Versioni 6 i IP-së. Shën i Përkthyesit [↑](#footnote-ref-55)
55. Gjuha e përdorur për krijimin e skedarëve elektronikë në krijimin e faqeve të Internetit. Shën i Përkthyesit [↑](#footnote-ref-56)
56. Lexohet ‘brauzer. Shën i Përkthyesit [↑](#footnote-ref-57)
57. Protokolli i kontrollit të transmetimit: është një protokoll i krijuar për realizimin e komunikimit nga një pajisje rrjeti tek një tjetër në Internet. Shën i Përkthyesit [↑](#footnote-ref-58)
58. Është një adresë ose vend që identifikon se ku mund të gjenden dokumentet në Internet. Shën i Përkthyesit [↑](#footnote-ref-59)
59. Formë e paraqitjes së një adrese IP 32-bit, që përbëhet nga 4 numra nga 0 në 255, secili i ndarë nga të tjerët me një pikë. p.sh. 172.16.154.1 [↑](#footnote-ref-60)
60. (Simple Mail Transfer Protocol ose SMTP) – Protokolli i Dërgimit të Postës së Thjeshtë [↑](#footnote-ref-61)
61. Serveri i Postës Elektronike [↑](#footnote-ref-62)
62. IMAP (Internet Service Access Protocol) – është një protokoll që i lejon një përdoruesi të tërheqë mesazhet e postës elektronike në kompjuterin e tij nga serveri i Kompanisë që ofron shërbimin e email-it. Shën i Përkthyesit [↑](#footnote-ref-63)
63. Ofrimi i shërbimeve në distancë, të cilat janë të hostuara në Internet. Shën i Përkthyesit [↑](#footnote-ref-64)
64. Shërbime në distancë në Internet. Shën i Përkthyesit [↑](#footnote-ref-65)
65. Është një term që tregon një vend ku mund të lihen mesazhet dhe mund të merren pa pasur nevojën që marrësi dhe dërguesi të takohen. Ky sistem komunikimi ka të bëjë me hapjen e një llogarie në një shërbim të postës elektronike të ofruar në Internet si për shembull nga Hotmail. Një person shkruan një mesazh elektronik por në vend që ta dërgojë e ruan atë në folderin “drafts” në llogarinë e Hotmail-it. Meqë mesazhi elektronik nuk u dërgua, ai nuk mund të kapet nga sistemet përgjuese të shërbimeve të sigurimit. Të dhënat e hyrjes në këtë llogari në Hotmail, më pas, i komunikohen personit me të cilin keqbërësi apo terroristi kërkon të komunikojë, me anë të telefonit duke përdorur një kod të paracaktuar, me sms apo verbalisht, në mënyrë që personi marrës të mund të hyjë në atë llogari dhe ta lexojë mesazhin. Mesazhi më vonë fshihet, kështu që duket sikur nuk ka ekzistuar kurrë. Mbasi mesazhi elektronik kalon, i cili mund të përfshijë edhe detajet e një llogarie tjetër që mund të përdoret për komunikimin e radhës – keqbërësit e braktisin llogarinë e email-it, e cila automatikisht fshihet nga kompania që ofron shërbimin e Internetit mbas një kohe të caktuar – në rastin e uebsajtit Hotmail nëse një llogari e hapur aty nuk përdoret për 30 ditë ajo fshihet. Shën i Përkthyesit. [↑](#footnote-ref-66)
66. Lidhje e drejtpërdrejtë ndërmjet dy njerëzve në rrjet pa patur nevojë që komunikimi i tyre të kalojë nëpërmjet ndonjë kontrollori rrjeti, për të mundësuar shkëmbimin e skedarëve dhe materialeve të tjera. Shën i Përkthyesit. [↑](#footnote-ref-67)
67. Një komunitet personash në Internet i dedikuar për diskutimin e një çështjeje të caktuar me interes për ata persona. Shën i Përkthyesit [↑](#footnote-ref-68)
68. Protokolli i Transferimit të Skedarëve. Shën i Përkthyesit [↑](#footnote-ref-69)
69. TCP (Transmission Control Protocol) është një grup rregullash (ose një Protokoll), të përdorur së bashku me Protokollin e Internetit (Internet Protocol (IP)) për dërgimin e të dhënave në formën e mesazheve ndërmjet kompjuterëve në Internet. IP-ja realizon mbërritjen e të dhënave në destinacion, TCP-ja kujdeset që të ndjekë paketat e të dhënave për një itinerar të efektshëm nëpër autostradat e Internetit. Shën i Përkthyesit [↑](#footnote-ref-70)
70. Shkëmbim mesazhesh në kohë reale – Chat. Shën i Përkthyesit [↑](#footnote-ref-71)
71. Hyrje e paautorizuar. Shën i Përkthyesit [↑](#footnote-ref-72)
72. Dërgimi i një numri shumë të madh të mesazheve elektronike një personi apo adrese specifike e-mail-i, që mund të mbushë të gjithë hapësirën e sistemit dhe mund të shkaktojë ndërprerjen e funksionimit të tij. Shën i Përkthyesit [↑](#footnote-ref-73)
73. Teknika e „Shoulder surfing“ është një teknikë e vëzhgimit të drejtpërdrejtë, si p.sh. të shohësh mbi supet e dikujt për të marrë informacion. Kjo teknikë përdoret për të marrë informacion në vendet ku ka turma njerëzish sepse është më e lehtë të rrish afër dikujt dhe t’i marrësh informacionin ndërkohë që ai/ajo është p.sh. duke plotësuar një formular, po shtyp një numër PIN në një bankomat, ose është duke përdorur një kartë telefonike në një telefon publik. Teknika e „Shoulder surfing“ mund të bëhet edhe nga distanca me ndihmën e dylbive ose pajisjeve të tjera të zmadhimit të pamjes. Për të parandaluar „shoulder surfing“, ekspertët rekomandojnë që tastierën ose fletën e punës ta mbuloni me trup ose me dorë. [↑](#footnote-ref-74)
74. Pajisje ose program kompjuterik që regjistron aktivitetin në kohë reale të një kompjuteri duke përfshirë edhe shtypjen e tastierës (fjalët, numrat etj.) [↑](#footnote-ref-75)
75. Rrjet sistemesh kompjuterike me programe të dëmshme që kryejnë detyra të automatizuara sipas udhëzimeve të personit që i çon programet e dëmshme në këto rrjete, si p.sh. dërgimi i automatizuar i emailave të padëshiruar, nga kompjutera të ndryshëm pa dijeninë e pronarit të tyre. Shën i Përkthyesit [↑](#footnote-ref-76)
76. Skedar identifikues në formë teksti që uebsajtet e dërgojnë në kompjuterët e përdoruesve që i vizitojnë këto uebsajte. [↑](#footnote-ref-77)
77. Reklama ose material promocional i marrë nëpërmjet mesazheve elektronike të pakërkuara. Shën i Përkthyesit [↑](#footnote-ref-78)
78. Ky është emri i falsifikimit të kokave të mesazheve elektronike në mënyrë që mesazhi të duket sikur të ketë ardhur nga dikush apo nga diku tjetër dhe jo nga burimi i vërtetë. Shën i Përkthyesit [↑](#footnote-ref-79)
79. Haktivizmi është akti i hyrjes së paautorizuar në një sistem kompjuterik për qëllime politike ose qëllime të motivuara nga ana sociale. Individi që kryen këtë akt nuk e bën për të bllokuar shërbimet e atij sistemi por për të sjellë në vëmendje një kauzë politike ose sociale. Individi quhet “hacktivist”. Shën i Përkthyesit [↑](#footnote-ref-80)
80. Program/mjet që e bën aktivitetin në Internet të pagjurmueshëm. [↑](#footnote-ref-81)
81. Me kompjuter të fikur. Shën i Përkthyesit [↑](#footnote-ref-82)
82. Me kompjuter të ndezur. Shën i Përkthyesit [↑](#footnote-ref-83)
83. Sekuestrimi i provave elektronike [↑](#footnote-ref-84)
84. http://register.consilium.europa.eu/pdf/en/03/st14/st14583.en03.pdf [↑](#footnote-ref-85)
85. Kopjim i imazheve. Shën i Përkthyesit [↑](#footnote-ref-86)
86. Kopjim i të dhënave. Shën i Përkthyesit [↑](#footnote-ref-87)
87. Internet Service Provider [↑](#footnote-ref-88)
88. Local area network (rrjet lokal) [↑](#footnote-ref-89)
89. [↑](#footnote-ref-90)
90. Pajisje/platformë me të cilën lidhet një kompjuter laptop, që i mundëson atij të përdoret si një kompjuter tavoline. Shën i Përkthyesit [↑](#footnote-ref-91)
91. Verifikues i Adresave të Protokollit të Internetit dhe të Kompjuterit. Shën i Përkthyesit [↑](#footnote-ref-92)
92. Vrasje me dashje. Shën i Përkthimit [↑](#footnote-ref-93)
93. Mohimi i shërbimit. Shën i Përkthimit [↑](#footnote-ref-94)