|  |  |
| --- | --- |
|  | **CyberCrime@IPA**  **Projekti i Përbashkët BE/KiE për Bashkëpunimin Rajonal kundër Krimit Kibernetik**  **Trajnimi Gjyqësor**  **Kurs i Përparuar për Krimin Kibernetik dhe Provat Elektronike për Gjyqtarët dhe Prokurorët**  Manuali i Trajnimit dhe Guida për Trajnerët – Versioni 1.0  Divizioni i Krimit Kibernetik dhe Mbrojtjes së të Dhënave  Drejtoria e Përgjithshme për të Drejtat e Njeriut dhe Shtetin e së Drejtës  Strasburg, Francë  30 Qershor 2013 |
| [**www.coe.int/cybercrime**](http://www.coe.int/cybercrime)  Description: 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 Faks: +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**

Hyrje 4

1 Vështrim i Përgjithshëm 5

1.1 Qëllimi i Kursit 5

1.2 Pse është i domosdoshëm ky trajnim 5

1.3 Programi Mësimor 6

2 Si përdoret guida për trajnerët 6

3 Vështrim i Përgjithshëm i Kursit 7

3.1 Sa i gjatë është kursi dhe për kë është 7

3.2 Kush do ta japë kursin 7

3.3 Si do të jepet kursi 8

3.4 Objektivat e kursit 8

3.5 Grupi i trajnerëve dhe pjesëmarrësit e synuar 8

3.5.1 Pjesëmarrësit 8

3.5.2 Kriteret e përvojës 8

3.5.3 Trajnerët 8

3.5.4 Kriteret e përvojës 8

3.6 Burimet 9

3.6.1 Kriteret për burimet e kursit 9

3.7 Vlerësimi 13

3.8 Axhenda e Kursit 15

3.9 Objektivat e Mësimit dhe të Kursit 16

Puna në grup për bashkëpunimin ndërkombëtar 16

4 Kontaktet Kryesore 19

5 Planet e Mësimit 20

**Hyrje** 20

**Ushtrime Praktike** (nëse nevojitet) 22

**Kontrolli i Njohurive** 22

Mësimi: 1.1.2 – Zhvillimi i një Hetimi 23

Mësimi: 1.1.3 – Puna në Grup – Hetimi 34

Mësimi 1.1.4 - Bashkëpunimi Ndërkombëtar..............................................................................38

Mësimi: 1.1.5 – Puna në Grup – Bashkëpunimi Ndërkombëtar 47

Mësimi: 1.1.6 – Puna në Grup – Identifikimi i të Dyshuarve 48

Mësimi: 1.2.1 – Rishikim Ditor 50

Mësimi: 1.2.2 – Prezantim–Kriminalistika Dixhitale–Pjesa 1 51

Mësimi: 1.2.2 – Prezantim – Kriminalistika Dixhitale – Pjesa 2 60

Mësimi: 1.2.3 – Puna në Grup – Kriminalistika Dixhitale 62

Mësimi: 1.2.4 – Prezantim – Përgatitja e Çështjes për Gjykatë 64

Mësimi: 1.2.5 – Punë në Grup – Finalizimi i çështjes 94

6 Vlerësimi nga pjesëmarrësit 97

7 Vlerësimi i pjesëmarrësve 97

# Hyrje

Me mbështetjen e shoqërive në të gjithë botën tek 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, të 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” si dhe është ngritur një qendër rajonale me bazë në Kroaci.

1. Vështrim i Përgjithshëm

## Qëllimi i Kursit

Ky kurs është hartuar për të vazhduar mbas kursit bazë për gjyqtarët dhe prokurorët që u zhvillua nga projekti i Këshillit të Evropës CyberCrime@IPA. Do t’i pajisë gjyqtarët dhe prokurorët me njohuri të mëtejshme për 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.

* Synimi i kursit është të ofrojë njohuri dhe aftësi për t’ju mundësuar gjyqtarëve dhe prokurorëve të përmbushin rolet e tyre në lidhje me hetimet për krimin kibernetik.
* Ky kurs është hartuar të bazohet mbi rezultatet e kursit bazë për krimin kibernetik për gjyqtarët dhe prokurorët dhe duhet të ndiqet vetëm nga ata që e kanë përfunduar me sukses atë kurs.

Kursi do të mbulojë temat e mëposhtme:

* Kryerja e një hetimi,
* Identifikimi i llojeve të veprave penale të kryera,
* Përcaktimi i vendndodhjes së provave, dëshmitarëve dhe të dyshuarve,
* Sigurimi i provave në mënyrë të pranueshme, pavarësisht se ku mbahen,
* Përgatitja për aktivitetet e kontrollit dhe sekuestrimit që kanë të bëjnë me provat elektronike,
* Trajtimi i pajisjeve dixhitale që janë pjesë e hetimit,
* Udhëzimi i specialistëve të kriminalistikës dhe të tjerëve që nevojiten për të mbështetur fazën e hetimit,
* Përgatitja për intervista me të dyshuarit,
* Paraqitja e provave për krimet kibernetike
* Marrja në konsideratë e aspekteve përkatëse gjatë procesit gjyqësor dhe gjykimit.

## Pse është i domosdoshëm ky trajnim

Gjyqtarët dhe prokurorët luajnë një rol të rëndësishëm në hetimin dhe gjykimin e individëve ose grupeve që kryejnë vepra penale. Me rritjen e numrit të krimeve që kanë brenda tyre elemente të krimit kibernetik, 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, Ndihmën e Ndërsjellë Juridike, 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.

Ky Modul Trajnimi është ndërtuar në një mënyrë të tillë që t’ju mundësojë gjyqtarëve dhe prokurorëve që kanë kaluar modulin bazë të trajnimit që të përmirësojnë njohuritë e tyre për natyrën e krimit kibernetik, termat dhe teknologjinë duke trajtuar skenarë me çështje praktike që nga ankesa fillestare, nëpër hetim dhe deri tek procesi i gjykimit.

Ky modul është hartuar 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.

Ky kurs është hartuar si një përzierje e mësimeve dhe një skenari praktik, që fillon që nga kallëzimi i krimit deri në përgatitjen e çështjes për gjykim. Prezantimet plotësojnë mësimin e krijuar gjatë skenarit praktik. Skenari i është përshtatur kohës dhe do të kërkojë azhurnim për ta lidhur me kohën në të cilën do të zhvillohet. Ai mund të përshtatet në mënyrë që kompania viktimë të jetë në vendin ku do të zhvillohet kursi, me qëllim që legjislacioni penal dhe procedural të jetë i lidhur me materialin.

1. 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.

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. 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. Si e tillë u krijua një skenar i detajuar duke përdorur një kronologji kohe që lidhej me zhvillimin e parë të këtij kursi. Mesazhet e postës elektronike që janë përdorur janë origjinale dhe u krijuan gjatë një periudhe kohe për të krijuar autenticitetin dhe mundësinë që pjesëmarrësit të kryejnë hetime në kohë reale duke përdorur burimet e disponueshme në Internet. Krahas kësaj, u krijua një seri me llogari bankare si material mbështetës. Këto përdorën banka dhe degë bankare të mirëfillta për t’i lejuar pjesëmarrësve të përdorin përsëri burimet online për të caktuar tërheqjen e fondeve për mbështetjen e hetimit. Synimi është krijimi i ndërgjegjësimit për aftësinë e kryerjes së hetimeve duke përdorur burimet online si dhe duke përdorur mekanizmat e bashkëpunimit ndërkombëtar që shpesh marrin shumë kohë për tu përfunduar. Me qëllim që materialet mbështetëse të jenë efektive në të ardhmen, ato duhet të azhurnohen rregullisht dhe të përshtaten me kohën. Materialet aktuale janë të përfshira si model.

Roli kyç i zhvilluesit të trajnimit është të garantojë synimin e përgjithshëm të çdo evenimenti të mësimit dhe arritjen e 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.

1. Vështrim i Përgjithshëm i Kursit
   1. Sa i gjatë është kursi dhe për kë është

Ky kurs është hartuar si një program dy ditor për gjyqtarët dhe prokurorët si pjesë e programit të tyre të formimit fillestar ose programit të trajnimit të vazhduar në rastet kur nuk e kanë përfituar më parë këtë trajnim.

* 1. 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. Për këtë kurs është veçanërisht e rëndësishme të përfshihen trajnerët që kanë njëfarë përvoje më këtë lloj hetimi. Për këtë qëllim mund të jetë e përshtatshme të përdoren njohuritë dhe aftësitë e komunitetit të zbatimit të ligjit që trajtojnë krimin kibernetik.

* 1. 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 dhe ushtrime praktike me letër. Rekomandohet që pjesëmarrësit të ndahen në grupe pune me jo më shumë sesa 6 njerëz për të gjithë kursin. Siç detajohet më lart, në Seksionin 1, trajnerët duhet të marrin në konsideratë përshtatjen e ushtrimeve dhe metodologjitë e tjera të mësimdhënies në programin në nivel kombëtar. Ky kurs është shumë interaktiv dhe do të kërkojë një punë të madhe hetimore nga ana e pjesëmarrësve si dhe ofrimin e një mbështetjeje shumë të madhe nga trajnerët në kurs.

* 1. 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.

* 1. 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 ose gjatë trajnimit të vazhduar për ata që nuk e kanë kryer këtë kurs më parë.

### Kriteret e përvojës

Ky kurs është hartuar të ndiqet vetëm nga ata që e kanë përfunduar kursin e trajnimit bazë për krimin kibernetik dhe provat elektronike, hartuar nga Këshilli i Evropës, ose ekuivalenti i tij kombëtar.

### Trajnerët

Qendrat e Trajnimit Gjyqësor duhet të punësojnë trajnerë për këtë kurs dhe duhet të përfshijnë trajnerët me përvojë në kryerjen e hetimeve për krimin kibernetik si dhe që janë përgjegjës për ndjekjen ligjore dhe gjykimin e çështjeve të tilla.

### Kriteret e përvojës

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

* 1. Burimet

### Kriteret për burimet e kursit

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

* Një sallë me madhësi të përshtatshme sipas numrit të pritshëm të pjesëmarrësve në kurs. Salla duhet të rregullohet duke përdorur një tryezë të rrumbullakët për çdo grup pune, sipas rastit bazuar në guidën me 6 pjesëmarrës për çdo grup.
* 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)
* Kopje të Guidës së Këshillit të Evropës për Provat Elektronike
* Dërrasë të Bardhë për secilin grup pune
* Markera shkrues për Tabelën e Bardhë (të paktën 2 për secilën ngjyrë: blu, të zinj, të kuq dhe jeshilë) për secilin grup pune
* Një Tabelë Flipchart me letër të mjaftueshme, për secilin grup pune
* 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 për secilin grup pune
* Një kompjuter laptop për secilin grup pune me rregullim të ngjashëm me Kompjuterin e Trajnerit dhe akses në Internet për të lejuar që të zhvillohen kërkimet hetimore.
* Makinë Virtuale të përgatitur specifikisht për këtë kurs dhe të përfshirë në paketën e burimeve.
* Të gjitha materialet mbështetëse të ofruara me paketën e trajnimit.

Burimet pasuese janë përgatitur për të mbështetur zhvillimin e kursit. Ato janë dhënë në formë elektronike sepse janë voluminoze. Këshilli i Evropës do të japë të gjitha burimet për vendet.

Informacioni kryesor për skenarin dhe afatet kohore që do të përdoren gjatë kursit janë dhënë në një skedar që përcakton aktivitetet dhe pikat kryesore të skenarit. Ky skedar titullohet “2012-08-20 am - Scenario and evidence for advanced course.docx” dhe duhet të gjendet në seksionin e Profileve të paketës së materialeve.

Më poshtë është një listë e skedarëve që do të përdoren në sesionin e parë praktik 1.1.3. Ato duhet të jepen si materiale mbështetëse që pasojnë shpjegimin e skenarit. Siç mund të shihet, emri i skedarit përmban datën e mesazhit elektronik, radhën e tij në sekuencë dhe një përshkrim. Është e rëndësishme të mbahet mend se në shembullin e parë duhet të jepen vetëm mesazhet elektronike pa koka sepse pjesëmarrësit në trajnim duhet të pranojnë nevojën për kokat e zgjeruara të mesazheve elektronike dhe duhet t’i kërkojnë ato.

2012-08-11 - Email 1 - 00007 to Humor products extortion email - no headers.pdf

2012-08-16 - Email 2 - 00007 to Humor products extortion email - no headers.pdf

2012-08-16 - Email 2 - 00007 to Humor products extortion email- headers.pdf

2012-08-17 - Email 3 - Humor to 00007 - We cannot pay criminals email - no headers.pdf

2012-08-19 - Email 4 - 00007 to Humor Products - instruction email and attachments - headers.pdf

2012-08-19 - Email 4 - 00007 to Humor Products - instruction email and attachments - no headers.pdf

2012-08-19 - Email 4 - attachment 387\_237 pixels.pdf

2012-08-19 - Email 4 - attachment 547\_558 pixels.pdf

2012-08-19 - Email 4 - attachment car-original.jpg

2012-08-21 - Email 5 - Humor Products to 00007 querying instructions for advertising car- no headers.pdf

2012-08-21 - Email 6 - 00007 to Humor Products - Apologies - no headers.pdf

2012-08-21 - Email 7 - Advert Placed - no headers.pdf

2012-08-25 - Email 8 - rgrealestate to HumorProducts - Mercedes Advert has expired.pdf

2102-08-21 - Email 6 - 00007 to Humor Products - Apologies - headers.pdf

Skedari pasues është një përmbledhje e llogarive bankare që Kompanisë Humor iu kërkua të krijonte nga kërcënuesi. Ato janë të gjitha llogari HSBC dhe u përdorën për të tërhequr të ardhurat nga krimi nga ATM-të në vende të ndryshme, nga korrierët e rekrutuar nga Myler. ATM-të e përdorura janë të mirëfillta dhe ekzistojnë në secilin vend. Pjesëmarrësit duhet ta përdorin këtë dokument si pjesë e hetimit të tyre, për shembull për përcaktimin e tërheqjes së parave. Nëse pjesëmarrësit nuk e kanë kërkuar këtë deri në sesionin 1.1.5, ky dokument duhet t’ju shpërndahet.

2012-10-25 - HSBC Bank Statements - Master Copy Transactions to 28th Oct 2012.pdf

Mesazhet elektronike dërguar nga Myler për rekrutimin e korrierëve për të ndihmuar në tërheqjen e pagesave për krimin janë të përfshira në paketën e trajnimit. Ato ndahen në 3 kategori sipas kreut të përgjithshëm të quajtur “Mule Emails”.

Nënkategoritë janë:

* **Ftesat për Korrierët nga Ralf Myler** 
  + Këto janë mesazhet e para elektronike që Myleri u dërgoi bashkëpunëtorëve të tij nga klubi i motoçiklistëve. Ju lutem mos harroni se përfshihen jo vetëm ata që e pranuan ofertën por edhe ata që e refuzuan. Këto duhet të ndihmojnë pjesëmarrësit për të vlerësuar fajin e korrierëve.
* **Përgjigjet nga Korrierët për Ralf Myler**
  + Këto janë përgjigjet që pranojnë ose refuzojnë ftesën nga Myler.
* **Udhëzimet për ATM për Korrierët nga Myler**
  + Këto janë seri mesazhesh të dërguara tek ata që e pranuan ofertën nga Myler, ku jepen udhëzimet për tërheqjet e parave.
* **Mesazhet elektronike me koka nga Korrierët**
  + Këto janë mesazhet elektronike nga korrierët që kanë kokat e zgjeruara dhe mund të përdoren nga trajneri për të ndihmuar shpjegimin sesi u gjurmuan mesazhet elektronike.

Skedarët e dhënë sipas secilës kategori janë:

**Ftesat për Korrierët nga Ralf Myler**

Invite 2 from 00007 to Bertram Klausen - headers.docx

Invite 2 from 00007 to Bertram Klausen - no headers.pdf

Invite 2 from 00007 to Jacob Wright - headers.docx

Invite 2 from 00007 to Jacob Wright - no headers.pdf

Invite 2 from 00007 to Johan Lauritsen - headers.docx

Invite 2 from 00007 to Johan Lauritsen - no headers.pdf

Invite 2 from 00007 to Khalid Abrahamsson - headers.docx

Invite 2 from 00007 to Khalid Abrahamsson - no headers.pdf

Invite 2 from 00007 to PetrHaluza - headers.docx

Invite 2 from 00007 to PetrHaluza - no headers.pdf

Invite from 00007 to Alexander Ponomaryov - headers.docx

Invite from 00007 to Alexander Ponomaryov - no headers.pdf

Invite from 00007 to Bertram Klausen - headers.docx

Invite from 00007 to Bertram Klausen - no headers.pdf

Invite from 00007 to David Boholyubov - headers.docx

Invite from 00007 to David Boholyubov - no headers.pdf

Invite from 00007 to Doreen Kirsch - headers.docx

Invite from 00007 to Doreen Kirsch - no headers.pdf

Invite from 00007 to Gabriyel Kozlowski - headers.docx

Invite from 00007 to Gabriyel Kozlowski - no headers.pdf

Invite from 00007 to IvankaPavlovic - headers.docx

Invite from 00007 to IvankaPavlovic - no headers.pdf

Invite from 00007 to Jacob Wright - headers.docx

Invite from 00007 to Jacob Wright - no headers.pdf

Invite from 00007 to Johan Lauritsen - headers.docx

Invite from 00007 to Johan Lauritsen - no headers.pdf

Invite from 00007 to KarelVachon - headers.docx

Invite from 00007 to KarelVachon - no headers.pdf

Invite from 00007 to Kensel Duarte - headers.docx

Invite from 00007 to Kensel Duarte - no headers.pdf

Invite from 00007 to Khalid Abrahamsson - headers.docx

Invite from 00007 to Khalid Abrahamsson - no headers.pdf

Invite from 00007 to Kuntz Koppany - headers.docx

Invite from 00007 to Kuntz Koppany - no headers.pdf

Invite from 00007 to Layton Murray - headers.docx

Invite from 00007 to Layton Murray - no headers.pdf

Invite from 00007 to Luka Berggram - headers.docx

Invite from 00007 to Luka Berggram - no headers.pdf

Invite from 00007 to Marija Slatic - headers.docx

Invite from 00007 to Marija Slatic - no headers.pdf

Invite from 00007 to NadanSibincic - headers.docx

Invite from 00007 to NadanSibincic - no headers.pdf

Invite from 00007 to PetrHaluza - headers.docx

Invite from 00007 to PetrHaluza - no headers.pdf

Invite from 00007 to RuzenaStepankova - headers.docx

Invite from 00007 to RuzenaStepankova - no headers.pdf

Invite from 00007 to SiiriHurmerinta - headers.docx

Invite from 00007 to SiiriHurmerinta - no headers.pdf

Invite from 00007 to Turner Desilets - headers.docx

Invite from 00007 to Turner Desilets - no headers.pdf

Invite from 00007 to Tyler Metcalfe - headers.docx

Invite from 00007 to Tyler Metcalfe - no headers.pdf

**Përgjigjet nga Korrierët për Ralf Myler**

Reply to 00007 - hushmail - from Layton Murray - no headers.pdf

Reply to 00007 - hushmail bounced message - from Layton Murray - no headers.pdf

Reply to 00007 from Alexander Ponomaryov - no headers.pdf

Reply to 00007 from Doreen Kirsch- no headers.pdf

Reply to 00007 from Gabriyel Kozlowski - no headers.pdf

Reply to 00007 from IvankaPavlovic - no headers.pdf

Reply to 00007 from Johan Lauritsen - no headers.pdf

Reply to 00007 from KarelVachon - no headers.pdf

Reply to 00007 from Kensel Duarte - no headers.pdf

Reply to 00007 from Kuntz Koppany - no headers.pdf

Reply to 00007 from Luka Berggren - no headers.pdf

Reply to 00007 from Marija Slatic - no headers.pdf

Reply to 00007 from RuzenaStepankova - no headers.pdf

Reply to 00007 from SiiriHurmerinta - no headers.pdf

Reply to 00007 from Tyler Metcalfe - no headers.pdf

Reply to Ralph Muller - Yahoo - from Layton Murray - no headers.pdf

**Udhëzimet ATM për Korrierët nga Ralf Myler**

ATM Instructions email - Alexander Ponomaryov - no headers.pdf

ATM Instructions email - Doreen Kirsch - no headers.pdf

ATM Instructions email - GabriyelKoslowski - no headers.pdf

ATM Instructions email - IvankaPavlovic - no headers.pdf

ATM Instructions email - Kensel Duarte - no headers.pdf

ATM Instructions email - Kuntz Koppany - no headers.pdf

ATM Instructions email - Marija Slatic - no headers.pdf

ATM Instructions email - RuzenaStepankova - no headers.pdf

ATM Instructions email - SiiriHurmerinta - no headers.pdf

**Mesazhet elektronike me koka nga Korrierët**

alexander\_ponomaryov.txt

berggrenluka.txt

gabkoz.txt

ivankapav.txt

kenselduarte.txt

kirschdoreen.txt

kuntzkoppany.txt

lauritsenjohan.txt

siirihurmenrinta.txt

slaticmarija.eml

slaticmarija.txt

sruzena.txt

tylermetcalfe12.txt

vachonkarel.txt

U krijua një makinë virtuale që pretendon të jetë imazhi i kompjuterit të keqbërësit Ralf Myler. Kjo u krijua gjatë zhvillimit të kursit të parë dhe u përdor për të dërguar dhe marrë mesazhet elektronike kërcënuese. Ajo përmban gjithashtu të gjithë informacionin që pritet të jetë në posedim të të dyshuarit. Kjo makinë virtuale duhet të përdoret për të demonstruar përfitimet e kriminalistikës dixhitale dhe për të inkurajuar pjesëmarrësit që të kërkojnë informacion specifik nga hetuesit e kriminalistikës dixhitale. Kjo pajisje është e disponueshme në një USB dhe udhëzimet e qarta për përdorimin e saj janë përfshirë në planin mësimor për sesionin 1.2.2, Pjesa 2. Krahas kësaj, janë krijuar dy skedarë shtesë që rezultojnë nga analiza kriminalistike e kompjuterit të Mylerit. Ato duhet të drejtojnë pjesëmarrësit drejt nevojës që provat të përdoren në çështjen penale. Një skedar e ka kokën e zgjeruar ndërsa tjetri nuk e ka.

Këto skedarë janë:

mule-tracking-emails-headers.docx

mule-tracking-emails.docx

Janë siguruar burime materiale shtesë për të ndihmuar trajnerin me përgatitjen e kursit. Këto përfshihen në kategorinë e përgjithshme të profileve dhe përfshijnë informacion bazë për skenarin, duke përfshirë të dhëna për viktimën dhe klubin e motoçiklistëve, të cilit i përkasin të gjithë korrierët dhe Myleri. Janë dhënë gjithashtu lista e korrierëve rezervë për zhvillimin e mëtejshëm të kursit. Këto lista përmbajnë të dhëna për individët që mund të përdoren në mënyrë të sigurt në skenarë të ndryshëm. Listat përmbajnë adresa të mirëfillta të postës elektronike që mund të aksesohen dhe përdoren për krijimin e mesazheve të reja për skenarët. Këto skedarë janë:

2012-08-20 - Spare Mules.docx

Mule Contact List.docx

Profile - EPIMCA.docx

Profile - Humor Products.docx

Skenari ka një element që ka të bëjë me steganografinë dhe me qëllim që të ndihmohet trajneri, skedarët përkatës janë përfshirë në paketën e trajnimit. Këto skedarë janë:

car-original.JPG

car-original.png

car-original2.jpg

car-stego-new.png

car-stego.png

Card data for photo.docx

Card stripe information.docx

creditcards.txt

Setup-OpenStego-0.5.2.exe

stego-instruction.png

Siç detajohet më lart, skenari është pika kryesore e këtij kursi dhe mbështetet nga një numër prezantimesh përkatëse të tematikave. Këtu nuk përfshihen vetëm slajdet, por gjithashtu edhe shënimet për të ndihmuar trajnerin. Prezantimet janë si më poshtë:

FINAL Presentation - Session 1.1.1 - Course Opening.pptx

FINAL Presentation - Session 1.1.2 - Developing an Investigation plan

FINAL Presentation - Session 1.1.4 - International Cooperation

FINAL Presentation - Session 1.2.1 - Daily Review

FINAL Presentation - Session 1.2.2 - Digital Forensics

FINAL Presentation - Session 1.2.2 - Digital Forensics - Evidence

FINAL Presentation - Session 1.2.4 - Preparing the Case for Court

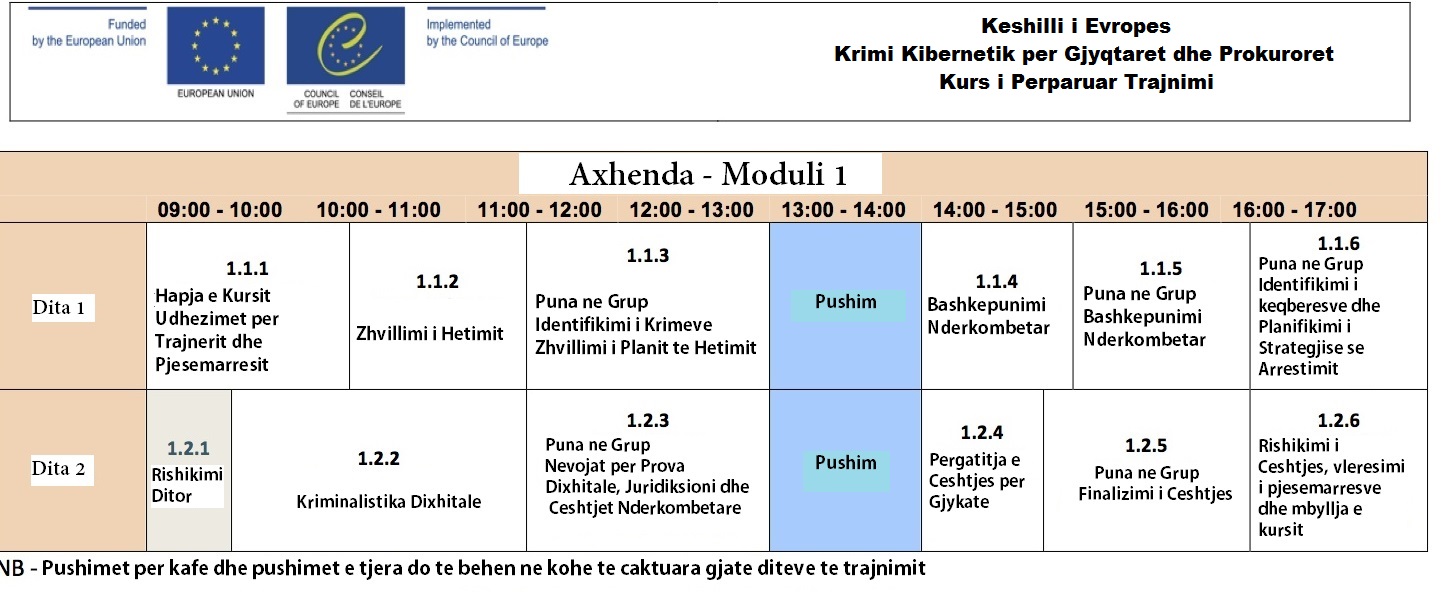
FINAL Presentation - Session 1.2.6 - Course Closure

Për shkak të natyrës së këtij kursi dhe mbështetjes së tij në një skenar, është thelbësore që trajneri të ketë kohë të mjaftueshme për tu ndërgjegjësuar për përmbajtjen e kursit dhe për përgatitjen për dhënien e tij. Siç është përmendur më parë, burimet materiale për skenarët u zhvilluan në vitin 2012 dhe mund të jetë e nevojshme që disa prej mesazheve dhe deklaratave të bankave në veçanti të azhurnohen për tu bërë aktuale me kohën e zhvillimit të kursit. Është përgjegjësia e trajnerit, në lidhje me institucionin trajnues që zhvillon kursin që të garantojë këtë gjë për audiencën.

* 1. Vlerësimi

Nuk është kërkuar asnjë vlerësim i njohurive të pjesëmarrësve dhe as nuk është dhënë si pjesë e këtij kursi pilot. Vendet që do të realizojnë këtë trajnim në nivel kombëtar mund të duan që të përfshijnë një vlerësim të tillë. Megjithatë, trajnerët duhet t’i kontrollojnë njohuritë e studentëve gjatë kursit, me anë të pyetjeve, kuizeve ose metodave të tjera për të garantuar se janë arritur objektivat e mësimdhënies.

* 1. Axhenda e Kursit

****

* 1. Objektivat e Mësimit dhe të Kursit

|  |  |  |
| --- | --- | --- |
| **Numri i Mësimit** | **Titulli i Mësimit** | **Objektivat** |
| **1.1.1** | **Hyrja në Kurs** | * Identifikimi i trajnerëve dhe i pjesëmarrësve * Përcaktimi i strukturës dhe përmbajtjes së kursit * Përfundimi i detyrave përkatëse administrative * Shpërndarja e dokumentacionit për kursin * Njohja e pjesëmarrësve me trajnerët dhe pjesëmarrësit e tjerë * Shpjegimi i ambienteve dhe procedurave në vend duke përfshirë edhe Çështjet e Shëndetit dhe të Sigurisë |
| **1.1.2** | **Prezantim – Zhvillimi i një Hetimi** | * Identifikoni detajet e viktimës * Përgatisni një përshkrim të shkurtër të fakteve të raportuara * Përshkruani humbjen, shpjegimin dhe justifikimin për të * Përcaktoni vendndodhjen e sistemit kompjuterik të viktimës, teknikët përgjegjës për mirëmbajtjen që mund të japin të dhëna rreth tij * Diskutoni verifikimin dhe kontrollin e kryer nga viktima * Vlerësoni informacionin për të dyshuarin dhe komunikimin e mundshëm me të * Identifikoni mjetet e komunikimit dhe burimin * Përcaktoni burimin e aktivitetit kriminal * Identifikoni instrumentet financiarë të përfshirë * Identifikoni dëshmitarët * Merrni në konsideratë provat mbështetëse që mund të nevojiten |
| **1.1.3** | **Puna në grup për hetimin** | * Identifikoni veprat penale të kryera në skenar * Zhvilloni një plan hetimi * Identifikoni të dhënat e mëtejshme që mund të duhen për kryerjen e hetimit * Renditni burimet e nevojshme për zhvillimin e hetimit |
| **1.1.4** | **Prezantim –Bashkëpunimi Ndërkombëtar** | * Identifiko nevojën për bashkëpunim ndërkombëtar për hetimin e shumë prej veprave penale që mund të jenë kryer; * Identifikoni kanalet e bashkëpunimit ndërkombëtar dhe instrumentet e disponueshëm, mënyrat e përdorimit të tyre, axhendat dhe efektivitetin e metodave të disponueshme të bashkëpunimit; * Diskutoni avantazhin e mekanizmave të bashkëpunimit të përshkruara në Konventën e Budapestit për Krimin Kibernetik dhe identifikoni parimet e përgjithshme të saj, masat provizore dhe rrjetin 24/7. |
| **1.1.5** | Puna në grup për bashkëpunimin ndërkombëtar | * Zbatoni në skenar mekanizmat e bashkëpunimit ndërkombëtar * Detajoni kërkimet e nevojshme për ruajtjen dhe marrjen e provave nga jashtë shtetit * Zhvilloni një plan për përftimin e provave nga jashtë shtetit në mënyrën më efektive. * Merrni në konsideratë implikimet për hetimin e vonesave në mekanizmat e bashkëpunimit ndërkombëtar. |
| **1.1.6** | **Puna në grup për identifikimin e të dyshuarit dhe planifikimi i strategjisë së arrestimit** | * Merrni në konsideratë provat e disponueshme * Identifikoni të dyshuarit në çështje * Identifikoni dëshmitarët e çështjes * Zhvilloni strategjinë e arrestimit të të dyshuarve * Identifikoni çështjet e rikuperimit të provave * Përgatituni për arrestimin dhe kontrollin e banesës së të dyshuarit * Përgatitni kërkesat ndërkombëtare për mbështetjen e strategjisë së arrestimit. |
| **1.2.1** | **Dita e Parë - Rishikimi** | * Identifikoni fushat e aktiviteteve të ditëve të mëparshme që janë kuptuar nga pjesëmarrësit * Identifikoni fusha të tilla ku pjesëmarrësit kanë nevojë të rishikojnë materialet për të sjellë njohuritë e tyre në nivelin e kërkuar |
| **1.2.2** | **Prezantim – Kriminalistika Dixhitale** | * Shpjegoni termin “Digital Forensics” * Krahasoni Kriminalistikën Dixhitale me shkencat tradicionale të kriminalistikës * Përkufizoni të paktën tre degë të Kriminalistikës Dixhitale * Identifikoni katër hapat në hetimet e Kriminalistikës Dixhitale * Diferenconi ndërmjet dy kategorive të gjurmëve dixhitale * Përshkruani sesi Kriminalistika Dixhitale mund të mbështesë hetimet * Shpjegoni sesi funksionon Steganografia * Krahasoni tre metoda sesi rikuperohen skedarët e fshirë * Karakterizoni llojet e ndryshme të Hapësirës së Papërdorur në Sistemin e Skedarëve * Zbatoni teorinë e Kriminalistikës Dixhitale në një skenar praktik * Identifikoni përfitimet e hetimit me anë të Kriminalistikës Dixhitale * Përshkruani sesi virtualizimi mund të ndihmojë Kriminalistikën Dixhitale |
| **1.2.3** | **Puna në grup për provat dixhitale, nevojat e provave, çështjet ndërkombëtare dhe juridiksionale** | * Merrni në konsideratë provat dixhitale të paraqitura në skenar * Përgatisni planin e intervistës për të dyshuarin * Përgatisni dokumentacionin përkatës për ruajtjen dhe prodhimin e provave nga jashtë shtetit. * Përcaktoni impaktin e provave dixhitale në skenar |
| **1.2.4** | **Prezantim – Përgatitja e çështjes për gjykatë** | * Menaxhimi i ndjekjes ligjore * Mbledhja e provave nga jashtë shtetit nëpërmjet Ndihmës së Ndërsjellë Juridike * Garantoni se nuk ka asnjë pengesë procedurale dhe ligjore në lidhje me kërkesat për marrjen e provave * Trajtoni çështjet e dëshmitarëve në juridiksione të tjera gjatë procedimeve * Plotësoni me saktësi dhe azhurnoni të gjithë dokumentacionin dhe procedurat përkatëse * Garantoni se janë përgatitur dosjet e përshtatshme dhe dokumentet mbështetës, dhe paraqitini ato në formatin e kërkuar brenda afateve përkatëse kohore * Ia tregoni mbrojtjes provat (nëse është nevoja) * Trajtoni çështjen e pranueshmërisë së provave elektronike dhe provave të tjera * Garantoni përputhshmërinë me KEDNJ-në dhe pajtimin me dispozitat e tjera * Njihni rolin dhe pritshmëritë nga ekspertët/specialistët si dëshmitarë * Dokumentoni plotësisht të gjitha vendimet, veprimet, alternativat dhe arsyetimin në përputhje me politikat dhe legjislacionin aktual * Identifikoni mënyrat e paraqitjes së provave elektronike në procedimin gjyqësor |
| **1.2.5** | **Puna në grup në finalizimin e çështjes gjyqësore** | * Përgatisni dosjen e çështjes për procedimin gjyqësor të të dyshuarit * Merrni në konsideratë provat elektronike që do të paraqiten në gjykatë. * Mbani parasysh nëse provat dixhitale kërkojnë prova të specializuara. * Finalizoni hetimin * Përcaktoni ndonjë boshllëk që mund të ekzistojë tek provat |
| **1.2.6** | **Mbyllja e kursit** | * Jepni vlerësimin e duhur për kursin dhe efektivitetin e tij * Plotësoni formularët e vlerësimit të kursit * Identifikoni nivelin tjetër të mësimit që nevojitet që pjesëmarrësit të përmirësojnë njohuritë dhe aftësitë e tyre në këtë fushë. |

1. Kontaktet Kryesore

Personi i mëposhtëm është pika e kontaktit për çdo pyetje apo kërkim 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 88 41 21 03  Fax +33 3 90 21 56 50  [alexander.seger@coe.int](mailto:alexander.seger@coe.int) |  |

1. Planet e Mësimit

|  |  |  |
| --- | --- | --- |
| **Mësimi: 1.1.1– Hapja e Kursit** | | **Kohëzgjatja: 60 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 që ata të kenë informacion të mjaftueshëm për programin e aktiviteteve dhe axhendën e kursit. Ofrimi i informacionit për detajet administrative, të shëndetit dhe të sigurisë gjatë kursit. Prezantimi i pjesëmarrësve me trajnerët dhe pjesëmarrësit e tjerë. | | |
| **Objektivat:**  Në fund të 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 | | |
|  | **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. | |
| **Slajdi 2**  **Slajdi 4**  **Slajdi 5**  **Slajdi 6**  **Slajdi 8**  **Slajdi 10**  **Slajdi 11**  **Slajdi 13**  **Slajdet 14 deri 15**  **Slajdet 16 deri 19** | **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 duhet të trajtohen kur ky kurs të zhvillohet në nivel kombëtar. Trajneri duhet të sigurohet se informacioni është i lidhur me vendin e zhvillimit të kursit.  Synimet e sesionit janë renditur si më poshtë:   * Pajisja e pjesëmarrësve me informacion për nevojën për kurs trajnimi dhe synimin 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.   Këtu trajtohen çështjet e shëndetit dhe të sigurisë. Këto do të varen nga vendi i zhvillimit të kursit. Është përgjegjësia e trajnerit të sigurohet se disponon informacionin e saktë për t’iu dhënë pjesëmarrësve.  Këtu jepet informacioni bazë i kursit për pjesëmarrësit, titulli i kursit është “Trajnim i Përparuar për Provat Elektronike dhe Krimin Kibernetik për Gjyqtarët dhe Prokurorët”. 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.  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.  Ky slajd është lënë bosh që secili vend të vendosë emrat e trajnerëve që do të japin kursin.  Është e rëndësishme që pjesëmarrësve t’iu shpjegohet synimi i përgjithshëm i kursit që në fillim të tij. Kjo do t’iu mundësojë atyre të vlerësojnë arsyen e përfshirjes së tyre në kurs. Synimi i përgjithshëm i këtij kursi është të pajisë me njohuri dhe aftësi gjyqtarët dhe prokurorët që të përmbushin rolet e tyre në lidhje me hetimet e krimit kibernetik. Ky kurs është hartuar duke u bazuar në rezultatet e kursit bazë të trajnimit për krimin kibernetik për gjyqtarët dhe prokurorët dhe duhet të ndiqet vetëm nga ata që e kanë përfunduar me sukses atë kurs.  Në këtë slajd shpjegohen objektivat e detajuar të kursit. Këto duhet t’ju shpjegohen pjesëmarrësve në këtë fazë. Në shpjegim janë përfshirë edhe pjesët themelore të secilit leksion.  Në këtë slajd janë përfshirë metodologjia dhe aspektet e kursit dhe duhet t’ju shpjegohen pjesëmarrësve.   * Prezantime dhe ushtrime praktike * Skenarë praktik * Dhënie progresive e letrave * Punë në grup për tema të ndryshme * Vlerësim i Grupit * Mbështetje për grupet nga trajnerët kombëtarë * Mbështetje rezervë nga trajnerët në sesionet e punës në grup   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.  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”   “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 20** | **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 ketë një kohë e caktuar për pyetjet. | |

|  |  |  |
| --- | --- | --- |
| Mësimi: 1.1.2 – Zhvillimi i një Hetimi | | **Kohëzgjatja: 60 Minuta** |
| **Burimet materiale të nevojshme:**   * Kompjuter tavoline apo laptop me Windows 7 dhe me programin Office 2010 * Projektor * Prezantimi në formatin PowerPoint | | |
| **Synimi:**  Synimi i këtij sesioni është të njohë pjesëmarrësit me konceptin e hetimeve të strukturuara dhe trajton elementët përkatës që do të merren në konsideratë nga marrja e ankimeve me anë të hetimit. | | |
| **Objektivat:**   * Identifikoni të dhënat e viktimës * Përgatisni një përshkrim të shkurtër të fakteve të raportuara * Përshkruani humbjen, shpjegimin dhe justifikimin e saj * Përcaktoni vendndodhjen e sistemeve kompjuterike të viktimës, teknikët përgjegjës me mirëmbajtjen që mund të japin informacion në lidhje me to * Diskutoni verifikimin dhe kontrollin e kryer nga viktima * Vlerësoni të dhënat për të dyshuarit dhe komunikimin e mundshëm me ta * Identifikoni mjetet e komunikimit dhe burimin * Përcaktoni burimin e aktivitetit kriminal * Identifikoni instrumentet financiare të përfshira * Identifikoni dëshmitarët * Merrni në konsideratë provat mbështetëse që nevojiten | | |
| **Nr i Slajdit** | **Përmbajtja:** | |
| **Slajdi2**  **Slajdi 3**  **Slajdi 4**  **Slajdi 5**  **Slajdi 6**  **Slajdi 7**  **Slajdi 8**  **Slajdi 9**  **Slajdi 10**  **Slajdi 11**  **Slajdi 12**  **Slajdet 13 & 14**  **Slajdi 15**  **Slajdi 16** | Sa herë që një çështje raportohet tek autoritetet kompetente, një veprimet e para është analiza e kallëzimit, me qëllim kontrollimin nëse përfshihen të dhëna të mjaftueshme dhe të nevojshme për të filluar një hetim.  Edhe hetimi do të fillojë me nga një ankesë ose nga të dhënat publike (të disponueshme në masmedia ose në Internet), ose një analizë krimi/kërkesë nga patrullimi i rrjetit ose një kërkesë për ndihmë që vjen nga një autoritet i huaj. Është shumë e rëndësishme që faktet të jenë të qarta që nga fillimi me qëllim që të përdoret qasja më e mirë për hetimin.  Persona përgjegjës për marrjen e kallëzimeve nga viktimat duhet të jenë të ndërgjegjshëm se çfarë informacioni nevojitet për kallëzimin dhe se çfarë informacioni kërkohet për fillimin e hetimit.  Përpara se të fillojmë të shohim formën dhe përmbajtjen e kallëzimit, është e rëndësishme të kontrollohet nëse veprimet e raportuara përbëjnë vepër penale, sepse mund të kemi disa situata kur veprimet e kryera nuk janë të inkriminueshme në legjislacionin kombëtar (P.sh: liria e shprehjes).  Për çështjet e krimit kibernetik, kallëzimi duhet t’i drejtohet organeve kompetente dhe përfshin të paktën të dhënat dhe informacionin e mëposhtëm:   * Detajet e identifikimit të viktimës (adresa, emri, numri i telefonit, vendi, posta elektronike, numri i identifikimit online, lloji i aktivitetit në rastin e personave juridikë); * Përshkrim i shkurtër i fakteve të raportuara, kohës kur dhe si ndodhën, vendin, rezultatet, etj; * Humbja, shpjegimi dhe justifikimi i saj; * Vendndodhja e sistemeve kompjuterike të viktimës, teknikët përgjegjës për mirëmbajtjen e tyre që mund të japin të dhëna për to; * Rezultatet e hetimit dhe kontrollet e kryera nga viktima, nëse ka, në lidhje me faktet; * Të dhënat për të dyshuarit dhe komunikimi i mundshëm me ta; * Mjetet e komunikimit dhe burimi; * Burimi i veprimeve kriminale, vendndodhja, kompjuteri, serveri, uebsajti. * Instrumentet financiare të përdorura për transferimin e parave dhe mënyrat e transferimit; * Dëshmitarët që mund të mbështesin faktet ose që janë në dijeni të tyre; * Provat mbështetëse për veprimet inkriminuese.   Bazuar në ankimin, përmbajtjen e tij dhe analizën pasuese të dokumenteve ose provave bashkëngjitur, është e rëndësishme të identifikohen veprat e kryera. Në varësi të natyrës së veprave do të identifikohet njësia kompetente për hetimin e çështjes brenda policisë ose prokurorisë, mënyrat e mbledhjes së provave, si dhe nevoja për përdorimin e mjeteve të bashkëpunimit ndërkombëtar, siç mund të jetë rasti.  Mund të ketë situata kur vlera e paragjykimit mund të supozojë ekzistencën e një krimi ose të një forme të rënduar të tij, dhe kjo është arsyeja se pse nevojitet ndërlidhje ndërmjet veprimeve kriminale dhe madhësisë së paragjykimit. Për shkak të këtij fakti dhe nevoje, njësitë kundër krimit kibernetik duhet të zhvillojnë një metodologji ndërlidhjeje ndërmjet njësive policore dhe institucioneve të tjera që përfshihen në këtë proces.  Identifikimi i veprave penale duhet të jetë një proces i vazhdueshëm gjatë gjithë hetimit dhe ndjekjes penale, sepse ka situata ku dalin fakte të reja dhe mund të shqyrtohen vepra të reja penale për çështjen.  Kur identifikojmë më shumë të dyshuar të përfshirë në veprimet kriminale, secili prej tyre duhet të vlerësohet në bazë të fakteve dhe provave të mbledhura. Renditja e të gjithë identifikuesve për secilin të dyshuar dhe diferencimi nga anëtarët e tjerë të grupit kriminal do të jenë të dobishme për vlerësimin.  Në fillim të hetimit përfshirja e disa personave mund të mos jetë shumë e qartë dhe ju do të keni nevojë për më shumë informacion dhe prova për të marrë vendimet.  Mbasi mblidhen të gjitha provat dhe përdoren të gjitha instrumentet e hetimit për çështjen, ju mund të vendosni në lidhje me veprat penale të kryera nga i dyshuari/të dyshuarit dhe situatën e tyre (dëshmitar, keqbërës kryesor, bashkëpunëtor etj.).  Të gjitha të dhënat, informacioni dhe provat që duhen identifikuar dhe mbledhur mund të merren kryesisht nga viktimat, dëshmitarët, bazat e të dhënave të policisë, burimet e hapura dhe palët e treta.  Aktiviteti i mbledhjes dhe vlerësimit të të dhënave dhe provave të tilla duhet të fokusohet tek identifikimi i mjeteve dhe vendi se ku duhet të merren.  Të dhënat dhe provat kanë qëllimin e qartësimit të fakteve të raportuara, identifikimit të të dyshuarve dhe vendeve ku u zhvillua aktiviteti kriminal, si dhe ekzaminimi i natyrës dhe vlerës së humbjeve.  Në të njëjtën kohë me marrjen e ankimit, është e rëndësishme të identifikohen të dhënat dhe informacioni i nevojshëm për procesin e investigimit dhe të përcaktohen kanalet dhe mjetet e marrjes së tyre.  Në procesin e mbledhjes së provave, një aspekt i rëndësishëm nuk është alarmimi i të dyshuarit/të dyshuarve sepse ata mund të shkatërrojnë provat, veçanërisht provat dixhitale, si p.sh. të dhënat në kompjuterët e tyre.  Në të gjitha hapat që po përpiqeni të bëni gjatë hetimit duhet të vlerësoni se cili do të jetë rezultati dhe si do të përdoret ai.  Të gjitha veprimet e kryera nga i dyshuari dhe të gjitha provat ose të dhënat që mund të mblidhni, duhet të vlerësohen me qëllim identifikimin e motivimit dhe sjelljes së të dyshuarit.  Nevojitet një prioritizim i veprimeve për identifikimin e provave me qëllim që të merren në një kohë të shkurtër përgjigjet më të rëndësishme ndaj pyetjeve të ngritura gjatë hetimit ose ndjekjes ligjore.  Në momentin e regjistrimit të kallëzimit, duhet të kryhet një vlerësim së bashku me viktimën i situatës së krijuar dhe risqeve të mundshme që mund të prekin viktimën, sistemeve kompjuterike, interesave ose mallrave të tjerë komercialë.    Është e mundur që gjatë aktivitetit kriminal disa kërcënime të mbeten për viktimën ose interesat e tij financiare, si dhe për sistemet kompjuterike të viktimës ose të një personi tjetër.  Është gjithashtu e nevojshme të identifikohen masat e mbrojtjes të nevojshme për mbrojtjen kundër risqeve të identifikuara.  Kur flitet për sistemet kompjuterike, masat mbrojtëse mund t’i referohen aspekteve teknike – mbrojtjes së serverëve ose bërjes së kopjeve rezervë. Përsa i takon interesave komercialë, reputacioni personal ose i biznesit të një personi ka nevojë për mbrojtje, duke kufizuar paragjykimin e përgjithshëm material, e cila është arsyeja për ruajtjen e konfidencialitetit të disa elementëve.  Në varësi të natyrës së fakteve, mund të duam që viktima të mbajë kontakte me të dyshuarin dhe të mbajë një sjellje të caktuar për të realizuar me sukses hetimin dhe identifikimin e të dyshuarit dhe provave. Megjithëse viktima këshillohet të mbajë kontakt me të dyshuarin për të mbledhur më shumë prova, ne duhet të koordinojmë dhe vendosim për të gjitha hapat dhe të mos e lëmë viktimën të keqkuptojë dhe kryejë veprime të paligjshme.  Gjatë procesit të vlerësimit të riskut dhe identifikimit të masave për largimin e risqeve, mund të nevojitet mbështetje shtesë nga kompanitë ose personat e tretë.  Për rrjedhim, për vlerësimin e sulmeve kibernetike kundër programeve kompjuterike, mund të kërkohet mbështetja e ekspertëve të kriminalistikës dixhitale.  Për identifikimin e disa të dhënave ose për ndalimin e disa aktiviteteve kompjuterike mund të angazhohen kompanitë, edhe nga juridiksione të ndryshme, me qëllim që të mbyllin një uebsajt ose të eliminojnë programin kompjuterik në serverin e kompanisë.  Është e rëndësishme të ketë një vlerësim të përhershëm të riskut për viktimën dhe interesat e tij/saj gjatë të gjithë hetimit dhe gjithashtu të mbahet kontakt i përhershëm me viktimën me qëllim që të bëhen veprimet e përshtatshme kur të jetë nevoja.  Në çështjet e krimit kibernetik, provat nuk kanë vetëm natyrë dixhitale por edhe fizike, të tilla si dokumentet, komunikimet, dëshmitë e dëshmitarëve, etj.  Në rast të provave dixhitale, nga fillimi i skenës duhet të identifikohet se ku janë provat dhe të garantohet siguria e tyre. Është e ditur se provat në mjedisin virtual mbahen për një periudhë dhe nëse nuk identifikohen me shpejtësi mund të ndikojnë negativisht në hetim.  Pas identifikimit të vendeve se ku mund të merren provat dixhitale, duhet të nxirren masa të përshtatshme për mbrojtjen dhe sigurinë e tyre. Do të ishte mirë sikur hetuesit të merrnin informacion në lidhje me vendin e kontrollin dhe sekuestrimin me anë të kompjuterit. Kjo do të ndihmojë njësitë e kriminalistikës dixhitale të vendosin cilën ose sasinë e pjesëve fizike të kompjuterit, programet kompjuterike, vendosjen e ekspertëve.  Në një hetim për krimin kibernetik, provat dixhitale mund të mblidhen nga vende të ndryshme, por burimet më të rëndësishme janë të mëposhtmet:   * Kompjuterik nga i cili janë kryer veprimet, por kjo jo gjithmonë do të thotë identifikimi i kriminelit;   Programet ose serverët e kompromentuar mund të përdoren për fshehjen e identitetit të kriminelit, për rrjedhojë është e rëndësishme të mblidhen që në fazën e parë të dhënat dhe informacioni i nevojshëm për identifikimin e burimit të sulmit.   * Sistemi kompjuterik i sulmuar ose i kompromentuar, sipas rastit, në varësi të natyrës së krimit.   Serverët/kompjuterët duhet të izolohen menjëherë dhe të mbyllen me qëllim që të analizohen nga ekspertët e kriminalistikës, nëse kjo nuk sjell ndonjë risk. Për të garantuar funksionimin e duhur të një aplikacioni, faqeje interneti, etj. që mund të jetë në serverët e kompromentuar, ata duhet të fiken dhe të zëvendësohen me kopje të sigurta. Nuk rekomandohet përdorimi i kompjuterit/serverit të kompromentuar mbas dijenisë për një aktivitet kriminal. Nëse sulmi ishte i suksesshëm për shkak të një virusi të zakonshëm, edhe kopja e sigurtë mund të ketë të njëjtën pikë të dobët. Kjo është arsyeja që kopjet e sigurta duhet të analizohen dhe rregullohen nëse është e mundur përpara rivendosjes në funksionim të sistemeve.  Duhet të realizohet mënyra e kryerjes së vlerësimit të programeve dhe sistemeve kompjuterike të komprometuara për ruajtjen e integritetit të të dhënave.   * Sistemet e tjera kompjuterike të përdorura për kryerjen e sulmeve kompjuterike në një formë apo në një tjetër.   Kur provat dixhitale janë tek kompanitë shërbimofruese të Internetit ose tek Palët e Treta, ato duhet të kontaktohen menjëherë për ruajtjen e të dhënave të nevojshme.  Ne mund të dërgojmë kërkesën e ruajtjes së të dhënave tek kompanitë shërbimofruese të Internetit, duke iu kërkuar atyre ruajnë të dhënat e regjistrimit, veçanërisht kur kompani të tilla janë jashtë juridiksionit kombëtar dhe koha e ruajtjes është e kufizuar. Në disa juridiksione, kërkesa e ruajtjes duhet të dërgohet tek pikat e kontaktit 24/7, e cila do të detajohet tek seksioni i bashkëpunimit ndërkombëtar.  Kur është fjala për provat dixhitale në procesin e vendimeve për mënyrat sesi do të procedojë hetimi, do të jetë me shumë rëndësi të merret parasysh koha e nevojitur për t’i marrë provat nga juridiksionet e tjera, sipas rastit. Në të njëjtën kohë duhet të identifikohen instrumentet dhe kanalet për kërkimin e ndihmës nga vendet e tjera.  Sistemet e komunikimit elektronik të përdorura për aktivitetet kriminale janë të rëndësishme gjatë një hetimi dhe kjo është arsyeja se pse nevojiten për identifikimin dhe paraqitjen e mesazheve ndërmjet viktimës dhe të dyshuarit në një format që është i përshtatshëm për të gjetur burimin e tij.  Për provat fizike, zakonisht nuk ka kritere për ruajtjen kundër shkatërrimit ose eliminimit. Për disa prova mund të ketë kufizime të procesit të marrjes së tyre, si p.sh. sekreti bankar për transaksione specifike, statusi dhe mjetet e përdorura për t’i marrë ato (raporti i policisë, miratimi i prokurorit ose gjyqtarit) ose juridiksioni, kur mund të merren vetëm nëpërmjet instrumenteve të bashkëpunimit ndërkombëtar.  Nganjëherë provat fizike mund të jenë më të lehta për tu marrë krahas provave dixhitale dhe vlerësimi i tyre mund të çojë drejt disa rrugëve të rëndësishme për hetimin.  Në çështjet e krimit kibernetik, shpesh ka viktima që nuk janë të ndërgjegjshëm se sistemi i tyre kompjuterik është sulmuar/kompromentuar ose se janë prekur interesat e tyre të biznesit. Sulmet kompjuterike mund të rezultojnë në komprometimin e disa serverëve/kompjuterëve njëherësh në një aktivitet të vetëm kriminal, kështu që është e rëndësishme identifikimi i viktimave dhe informimi i tyre në lidhje me situatën dhe ofrimi i mundësisë për mbrojtjen e kompjuterëve dhe interesave të tyre, por gjithashtu edhe për mbledhjen e provave mbështetëse për hetimin.  Viktimat duhet të kontaktohen dhe informohen për hetimin dhe më pas duhet t’iu kërkohet të japin të dhënat që kanë dhe t’iu jepet mundësia për të bërë kallëzimet. Të gjitha komunikimet duhet të garantojnë konfidencialitetin edhe për viktimën edhe për hetimin.  Nga dëshmitarët krijohet një kategori e veçantë. Ata duhet të identifikohen sepse mund të jenë në posedim të të dhënave dhe provave të rëndësishme që do të përdoren gjatë hetimit me qëllim vërtetimin e aktiviteteve kriminale.  Ata duhet të identifikohen sa më shpejt që të jetë e mundur dhe vendosja e kontakteve me ta duhet të konsiderohet si prioritet.  Duhet të ndiqen kriteret ligjore dhe procedurat e punës të zbatueshme për metodat e përdorura për kontaktimin e dëshmitarëve dhe mjeteve për të kërkuar të dhënat dhe provat e mbajtura.  Bashkëpunimi me viktimën(at) gjatë hetimit duhet të jetë i vazhdueshëm në bazë të nevojës për të informuar viktimën për progresin, për të shpjeguar procedurat gjyqësore dhe për të dhënë ndihmën sa herë që të jetë e nevojshme.  Mund të ketë raste kur viktimat identifikojnë të dhënat shtesë që nuk u dhanë në fillim të hetimit ose që dalin më vonë dhe që nuk mund të diheshin ose të përdoreshin nga hetuesit.  Kontakti me viktimat dhe dëshmitarët duhet të jenë në linjë me nevojat dhe interesat e tyre, duke respektuar racën, besimin fetar dhe të drejtat e njeriut.  Në rastet kur hetohen veprat penale kompjuterike, është me vend të mos fokusohemi vetëm tek “metodat e reja” të hetimit të lidhura me kompjuterin dhe Internetin, por edhe tek metodat tradicionale dhe të gjitha detajet e fakteve duhet të analizohen me të njëjtën vlerë.  Të gjitha veprimet hetimore për tu kryer duhet të parashikojnë veçanërisht:   * Vërtetimin e aktivitetit kriminal dhe ndalimin e tij, * Identifikimin e të dyshuarve dhe dënimin e tyre, dhe * Rikuperimin e dëmit.   Nuk ka asnjë dyshim se për çdo sulm dhe krim, një nga detyrat e para është ndalimi i krimit dhe gjithashtu humbjet. Ka disa situata ku mund të analizojmë dhe vendosim me shumë kujdes dhe ky veprim mund të shtyhet për një periudhë të caktuar kohe për qëllime të hetimit nëse është më shumë i dëmshëm.  Aktivitetet për tu kryer duhet të prioritizohen, bazuar në dispozitat ligjore dhe procedurat e punës së policisë.  Për përcaktimin e aktiviteteve dhe mënyrës së realizimit të tyre mund të konsultohen prokurori, viktima, dëshmitarët ose njerëzit nga departamentet ose institucionet e tjera dhe vendimet të merren së bashku. Ne duhet të konsiderojmë se viktimat mund të jenë shumë emocionale për shkak të natyrës së situatës.  Duhet të sigurohet vazhdimësia e hetimit, për këtë arsye në rast të një hetimi kompleks, nevojitet një grup për kryerjen e aktiviteteve, me një marrëdhënie të mirë dhe përhapje të rregullt të të dhënave dhe rezultateve ndërmjet anëtarëve.  Aktivitete ose lidhje të tjera kriminale me çështje të tjera mund të gjenden gjatë hetimit dhe në raste të tilla informacioni duhet të dërgohet tek departamentet kompetente.  Përgatitja e dosjes dhe hartimi i dokumentacionit të nevojshëm për paraqitjen e rezultateve duhet jetë një preokupim i vazhdueshëm i hetuesve me qëllim lejimin e ndërlidhjes së të gjitha të dhënave dhe provave të identifikuara.  Një aspekt tjetër i rëndësishëm lidhet me metodën e mbledhjes së të dhënave dhe provave si dhe sesi do të ruhen dhe përdoren ato. Për këtë qëllim duhet të respektohen të gjitha dispozitat dhe procedurat ligjore dhe provat duhet të mbahen të sigurta dhe të sakta.  Në varësi të sistemit ligjor kombëtar, kompetenca e hetimit mbahet nga policia ose prokuroria, dhe bashkëpunimi ndërmjet policisë dhe prokurorisë përcaktohet nga një kornizë specifike ligjore.  Për rrjedhim, përveç aktiviteteve fillestare që do të realizohen nga institucioni që mori ankimin, me qëllim garantimin e integritetit ose ruajtjes së provave, eliminimit të riskut dhe ndalimit të aktiviteteve kriminale, çështja duhet të paraqitet tërësisht nga prokurori, së bashku me masat e marra deri në atë moment.  Megjithëse kapaciteti njerëzor dhe teknik i forcave të policisë zakonisht është më i madh sesa i prokurorisë, prokurorët kanë njohuri të mëdha juridike dhe kompetenca ligjore specifike. Arsyeja e kësaj mase është se disa prej masave të hetimit nuk mund të kryhen pa miratimin e prokurorit. Nga ana tjetër disa aktivitete hetimore mund të vendosen nga prokurori, dhe për këtë arsye prokurori duhet të përfshihet në hetim.  Bashkëpunimi ndërmjet policisë dhe prokurorisë nevojitet gjatë gjithë hetimit dhe kryesisht i referohet:   * Përcaktimit të veprave penale të kryera * Përcaktimit të masave hetimore, dhe * Vlerësimit të rezultateve dhe vendimmarrjes për kontrollet, arrestimet dhe marrjes në pyetje të të dyshuarve.     Një nga prioritetet e një hetimi është identifikimi i të dyshuarit/të dyshuarve. Ata mund të lenë disa gjurmë të drejtpërdrejta të identitetit të tyre ose mund të përdorin ndërmjetës në kryerjen e veprave penale kompjuterike ose tradicionale. Të dhëna të dobishme në Internet për të dyshuarin mund të gjenden jo vetëm nga aktivitetet e tij/saj kriminale.  Vendndodhja e të dyshuarve është e rëndësishme për identifikimin e hapësirës për kryerjen e aktiviteteve kriminale dhe ku ndodhen prova të rëndësishme për çështjen.  Mbasi identifikohet i dyshuari, është shumë e rëndësishme të kryhen veprimet hetimore për sqarimin e aspekteve përkatëse të çështjes, si vijon:   * Vendndodhja e kompjuterit të përdorur për kryerjen e veprave penale; * Vendndodhja e të dyshuarit ose adresat e tjera të përdorura; * Lidhja e përdorur e Internetit (lidhje me kabull, lidhje pa kabull, ISP, etj.) * Dijenia dhe përfshirja në veprimet kriminale; * Bashkëpunimi me të dyshuarit e tjerë dhe përfshirja e tyre; * Llogaritë bankare.   Hetimi i aspekteve financiare mund të ndihmojë në identifikimin dhe gjetjen e të dyshuarit/të dyshuarve dhe gjithashtu në rikuperimin e produktit financiar të krimeve të kryera për të mbuluar dëmin e shkaktuar.  Të gjitha veprimet hetimore të lidhura me të dyshuarin duhet gjithashtu të ndjekin lidhjet me personat e tjerë që janë në dijeni ose të përfshirë në veprimtarinë kriminale, si dhe skenarë të tjerë të mundshme që ai mund të krijojë në favor ose në mbrojtje të tij. Këta njerëz mund të na japin prova të rëndësishme me qëllim identifikimin dhe gjetjen e vendndodhjes së të dyshuarit kryesor.  Nuk duhet të harrojmë se nganjëherë të dhënat nga shërbimet e ndryshme (energji elektrike, ujë, gaz, telefon) mund të na ndihmojnë gjithashtu për identifikimin e kriminelit/kriminelëve.  Baza e të dhënave e policisë si dhe hetimet aktuale ose të mëparshme të kryera nga departamente të tjera të policisë mund të eksplorohen për identifikimin dhe gjetjen e të dyshuarit. Nëse mjedisi i krimit është një shërbim online, ofruesi i shërbimit mund të ketë gjithashtu të dhëna të dobishme për identifikimin e të dyshuarit.  Bashkëpunimi me autoritetet ose njësitë e tjera policore është i lidhur ngushtë me mënyrën e kryerjes së hetimit dhe duhet t’i referohet të gjitha aspekteve të parashikuara në këtë proces.  Pra, bashkëpunimi është i dobishëm për sqarimin e aspekteve të mëposhtme:   * Shkëmbimi i informacionin për faktet, personat, mënyrat e veprimit, lidhjet në hetime; * Mbledhja e të dhënave dhe provave; * Dhënia e mbështetjes logjistike për kryerjen e disa aktiviteteve; * Ndihma e specializuar për çështjet teknike, financiare ose çështjet e tjera;     Aktivitetet e bashkëpunimit duhet të kenë një urdhër specifik me prioritete të caktuara për hetimin dhe në bazë të procedurave dhe protokolleve të bashkëpunimit.  Vlerësimi i aktiviteteve të kryera, rezultatet e arritura dhe provat e identifikuara janë një proces në vazhdimësi gjatë hetimit dhe duhet të përqendrohen tek pikat e mëposhtme:   * Si u zbatuan këto aktivitete; * Nëse u respektuan vendimet ose hapat; * Nëse provat e mbledhura janë të mjaftueshme për marrjen e vendimeve; * Nëse u respektuan procedurat dhe dispozitat ligjore; * Nëse u hetuan të gjitha aspektet; * Urdhrat për masa hetimore shtesë; * Nëse aktiviteti kriminal u ndalua dhe se cili është impakti i tij nëse ai vazhdon.   Ky vlerësim duhet gjithashtu të përcaktojë kohën për kontrollet, arrestimet, dhe marrjet në pyetje.  Data dhe mënyra e kryerjes së këtyre aktiviteteve duhet të vendoset në bazë të provave të mbledhura, natyrës së aktivitetit kriminal dhe kategorisë së të dyshuarve.  Është e mundur që të vendoset që në fillim të kapen të dyshuarit në veprim dhe më pas të kryhen kontrollet ose në fillim të kontrollohen dhe arrestohen të dyshuarit dhe më pas të kontrollohen dhe arrestohen të tjerët në një fazë të mëvonshme.  Të gjitha vendimet duhet të merren në interes të hetimit dhe të viktimave, në respektim të procedurave dhe dispozitave ligjore.  Mënyrat e kryerjes së kontrolleve, identifikimi i të dyshuarve dhe sekuestrimi i provave dhe kryerja e kontrollit të pronës kërkon një përgatitje specifike dhe të veçantë të njerëzve që do ta realizojnë këtë, në përputhje me natyrën e vendit ku do të kryhen aktivitetet, identitetet dhe risqet e lidhura me të dyshuarit, dhe natyrën e provave dhe pronat që do të identifikohen.  Pajisja dhe përgatitja e personelit që do të angazhohet në aktivitetet e sipërpërmendura është një aktivitet shumë i rëndësishëm, në linjë me atë që u prezantua më parë.  Përgatitja e dokumenteve në dosjen gjyqësore dhe udhëzimi i personelit për marrjen në pyetje të të dyshuarve duhet të marrë në konsideratë të gjitha aktivitetet investigative që u kryen, veprat penale dhe provat e administruara.    Rekomandohet që në fund të një hetimi të bëhet vlerësimi i çështjes, me qëllim identifikimin e të gjitha aspekteve negative të çështjes.  Aspektet negative ndihmojnë për përmirësimin e performancës, metodave dhe procedurave për çështje të tilla në mënyrë që të eliminohen në të ardhmen risqet e kryerjes të lidhura me aktivitetet e kryera.  Aspektet pozitive lidhen me përvoja specifike që do të përdoren në trajnimet e ardhshme të personelit, metodat e bashkëpunimit me viktimat ose aktivitetet e tjera.  Përvojat, pikat e mësimit dhe praktikat më të mira mund të përhapen në departament ose nëpërmjet kanaleve të autorizuara tek departamente të tjera.  Disa situata gjatë një hetimi mund të paraqiten dhe diskutohen për vlerësimin e reagimit ndaj tyre dhe alternativave për veprimet e së ardhmes.  Ju jeni të gjithë hetues në këtë trajnim dhe duhet të hetoni një skenar hipotetik sot dhe nesër. Për shkak të punës në grup, ju dhe pjesëtarët e grupit tuaj që janë ulur me ju në tryezën e rrumbullakët duhet të hetoni çështjen dhe të identifikoni keqbërësin/keqbërësit.  Një nga gjërat e para që duhet të kuptojmë është krimi dhe mënyra e veprimit. Nëse sulmi është shumë teknik dhe i paqartë për ju, është gjithmonë mirë të kaloni pak kohë që ta kuptoni sesi funksionon krimi ose modeli i krimit. Në skenarin e dhënë, kemi të bëjmë me një sulm DDOS (Distributed Denial Of System), i cili mund të jetë shumë teknik për ata që nuk e njohin këtë lloj sulmi kibernetik. DDOS është në fakt një sulm që i bëhet sistemit kompjuterik me një kërkesë masive për akses dhe i zë të gjitha burimet e sistemit kompjuterik të viktimës me këto kërkesa. Pra, kërkesat e zakonshme dhe të ligjshme nuk mund të marrin përgjigje nga ky sistem për shkak të kërkesave të mëdha nga sulmi dhe ky sistem do të duket i paarritshëm. Kuptimi teknik i sulmit DDOS ka të bëjë me mbingarkimin e gjerësisë së valës.   * Një nga misionet e para që keni është të përcaktoni përfundimisht nëse ky sulm është vepër penale sipas ligjit tuaj penal. Nëse po shkruajeni se çfarë lloj vepre është. * Misioni juaj kryesor në këtë skenar është identifikimi i keqbërësit që viktimizoi Kompaninë Humor. * Është gjithmonë e dobishme të përgatitet një listë me veprime për tu kryer. Për zhvillimin e çështjes gjyqësore në listë të përfshihet çfarë është e disponueshme, çfarë mund të mblidhet nga burimet e hapura dhe burimet në Internet, çfarë të dhënash të tjera mund të merren nga Kompanitë Shërbimofruese të Internetit (si p.sh. ISP-të, bankat, regjistrimet e kompanive të energjisë elektrike, shoqëritë tregtare, ndihma ndërkombëtare). Ju lutem mbani parasysh se trajnerët në klasë janë ofrues të dhënash offline. Nëse i shkruani kërkesat tuaja (në një letër të vogël) si prokuror ose si gjyqtar, ato mund t’ju ofrojnë të dhëna të vlefshme. Disa prej kërkesave tuaja mund të kenë rezultate pozitive por jo të gjitha, siç ndodh dhe në jetën reale. * Nganjëherë të menduarit me detaje dhe kontrollimi i çdo të dhëne të vetme mund të ndihmojë në vlerësimin e përgjithshëm të situatës. Ju lutem bëni disa përpjekje në të njëjtën kohë. Kur të keni mbledhur të gjithë informacionin, mund të analizoni se çfarë do të thotë ai. * Është mirë gjithmonë që të mendoni edhe si keqbërës. Nëse mundeni ta bëni, mund të kontrolloni të gjitha vendet e duhura dhe të kuptoni se kush është mbrapa krimit. * Ju lutem mos harroni se ky është trajnim dhe trajnerët janë gati t’ju ndihmojnë në rast dyshimi ose pyetjesh. * Pjesëmarrja juaj aktive është për identifikimin e keqbërësit dhe kontributi juaj vlerësohet. | |
|  | **Ushtrime Praktike (nëse ka)**  Nuk ka ushtrime praktike të lidhura me këtë sesion. | |
|  | **Kontrolli i Njohurive**  Për këtë kurs nuk është parashikuar asnjë kontroll njohurish krahas atij të renditur më lart. Nuk është kërkuar asnjë vlerësim zyrtar. | |

|  |  |  |
| --- | --- | --- |
| Mësimi: 1.1.3 – Puna në Grup – Hetimi | | **Kohëzgjatja: 90 Minuta** |
| **Burime materiale të nevojshme:**   * Një sallë të përshtatshme për një numër të parashikuar pjesëmarrësish. Kjo sallë duhet të rregullohet duke vendosur një tryezë të rrumbullakët për çdo grup, ku është e mundur, bazuar në një numër prej 6 pjesëmarrësish në grup. * Kopje të Guidës për Provat Elektronike të Këshillit të Evropës * 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) * Dërrasë të Bardhë për secilin grup * Markera për Dërrasë të Bardhë (të paktën 2 për secilën ngjyrë: blu, të zezë, të kuqe dhe jeshile) për secilin grup * 1 Tabelë Flipchart me letër të mjaftueshme për secilin grup * Stilolapsa dhe blloqe për pjesëmarrësit * Kapëse aktesh, vrimahapëse dhe gërshërë për secilin grup * Ngjitës Blu ose një produkt të ngjashëm me të për ngjitjen e përkohshme të letrës në mure për secilin grup * Një kompjuter laptop për secilin grup të ngjashëm me kompjuterin e trajnerit dhe me akses në Internet që të realizohen kërkimet hetimore. * Të gjitha materialet mbështetëse të dhëna me paketën e trajnimit. | | |
| **Synimi:** Ky sesion është hapja e skenarit praktik. Synimi është që pjesëmarrësit të identifikojnë rolet në grupin hetimor, të caktojnë detyrat dhe të identifikojnë parametrat e hetimit që do të kryhet si dhe veprat penale që mund të jenë kryer. | | |
| **Objektivat:**  Në fund të sesionit, pjesëmarrësit do të jenë në gjendje të:   * Identifikojnë veprat penale të kryera në skenar * Zhvillojnë një plan hetimi * Identifikojnë informacion shtesë që nevojitet për kryerjen e hetimit * Rendisin burimet e nevojshme për kryerjen e hetimit | | |
| **Nr. Slajdit** | **Përmbajtja:** | |
|  | Përdorimi i një prezantimi është fakultativ për këtë sesion. Nëse është e nevojshme një prezantim mund të përdoret për të mbështetur ushtrimin e dhënies së letrave që iu jep studentëve informacion të mjaftueshëm për fillimin e hetimit dhe përmbush objektivat e sesionit. | |
|  | **Ushtrime Praktike (sipas rastit)**  Ky sesion është tërësisht praktik dhe fillon me kallëzimin e viktimës së krimit. Vepra është një kërcënim i kryer nga një shtetas Gjerman Ralf Myler.  Skenari bazohet në konceptin e mëposhtëm:  Humor Products (Humor) është një kompani Hungareze që shet pjesë rezervë për makina të shtrenjta në të gjithë botën nëpërmjet Internetit. Të ardhurat e saj janë 10 milion Euro në vit dhe është një biznes me rritje shumë të shpejtë me të ardhura që i rriten në vit me 250%. Kompania Humor mbështetet tek Interneti për më shumë se 85% të shitjeve të saj. Çdo ndërprerje e aftësisë për shitjet online do të kishte një efekt të rëndë në vazhdueshmërinë e biznesit. Kompania Humor sapo ka investuar 5 milion Euro në një depo të re shpërndarjeje dhe ka punësuar 20 punonjës të tjerë për të përballuar kërkesat. Fatkeqësisht, si të gjitha bizneset me rritje të shpejtë, procedurat e rikuperimit nga fatkeqësitë nuk janë në të njëjtin ritëm me rritjet e shitjeve dhe kompania nuk ka asnjë plan për rikuperimin nga fatkeqësitë apo vazhdimësinë e biznesit. Nuk ka asnjë pajisje rezervë që do t’i lejojë biznesit të vazhdojë normalisht punën në rast të mosfunksionimit të lidhjes së Internetit.  Ralf Myler është një shtetas Gjerman, i cili është një specialist informatik i vetëpunësuar. Atij nuk po i ecën shumë në biznes dhe po lufton që të paguajë hipotekën dhe është në borxhe me bankën e tij. Ai ka disa kreditorë të tjerë që po e ndjekin për paratë që iu detyrohet. Në Maj 2012, ai ndërmori një Udhëzim në Lumin Rin të rregulluar nga një klub ndërkombëtar motoçiklistësh në të cilin ai bën pjesë. Gjatë udhëtimit ai miqësohet me një numër njerëzish nga Evropa, të cilët ishin anëtarë të grupit të motoçiklistëve (8 prej të cilëve do të bëhen më vonë korrierë në aktivitetet e tij kriminale kundër kompanisë Humor). Një tjetër person në këtë udhëtim ishte dhe Veselko Ivanković, i cili është drejtori i Sistemeve Informatike të Kompanisë Humor. Veselko dhe Ralfi u bënë shumë miq gjatë udhëtimit. Veselko ishte i zhgënjyer me punën që bënte dhe nuk ishte shumë i rezervuar në diskutimet e tij me Ralfin, duke i thënë se punëdhënësit e tij nuk kuptonin asgjë nga siguria informatike dhe se biznesi i tyre nuk do t’i mbijetonte një sulmi mbi sistemet kompjuterike. Nuk ka asnjë sugjerim se Veselko ishte i përfshirë në ndonjë mënyrë në ngjarjet që pasuan më pas.  Ralf Myler u kthye në shtëpi mbas pushimeve për tu përballur me një grumbull të madh letrash që i kërkonin menjëherë pagesën e detyrimeve të tij. Ai vendos që të përfitonte nga situata dhe nga informacioni që kishte marrë nga Veselko gjatë pushimeve dhe më pas hartoi një plan për të zhvatur para nga Kompania Humor.  Myler harton një plan për zhvatjen e parave nga Kompania Humor dhe realizohet një shkëmbim mesazhesh elektronike në të cilat ai së fundmi arrin objektivin e tij dhe e bind Kompaninë Humor të ndjekë një rrugë rrethore që t’ia transferojë paratë atij. Nga ana e tij ai përdor një numër korrierësh, në vende të ndryshme për grumbullimin e parave nga bankomatet, duke i pajisur ata më parë me karta. E gjithë historia është në mesazhet elektronike dhe ato janë në mbështetje të kursit. Krahas kësaj, ka deklarata bankare që tregojnë tërheqjet e shumave të parave, si dhe listat e korrierëve. Të gjithë aktorët në këtë skenar kanë adresa të mirëfillta të postës elektronike. Emrat e përdoruesve dhe fjalëkalimet janë në listat e dhëna me paketën e trajnimit dhe mund të përdoren nëse çmohet e nevojshme për të rikrijuar skenarin për tu siguruar se datat në mesazhet elektronike dhe në deklaratat bankare janë në një kohë të lidhur me zhvillimin e kursit. Deklaratat bankare tregojnë tërheqjet e parave gjatë një periudhe të caktuar. Bankomatet e përdorura janë të vërteta dhe mund të tregohen në një hartë, nëse pjesëmarrësit e dëshirojnë këtë, për të treguar zonën në të cilën u bënë tërheqjet e ndryshme. Edhe njëherë, mund të jetë e nevojshme të azhurnohen deklaratat bankare për ti bërë sa më të afërta në kohë. Nuk ka një zgjidhje të vetme për këtë skenar dhe synimi është të bëhet e mundur që pjesëmarrësit të marrin në shqyrtim alternativa të ndryshme dhe të identifikojnë se çfarë provash nevojiten dhe sesi t’i marrin ato, edhe për hetimin edhe për procedimin gjyqësor. Trajnerët do të duhet të jenë shumë interaktiv dhe të ofrojnë mbështetje për pjesëmarrësit; në disa rrethana, mund të jetë e nevojshme të jepet ndihmë shtesë për tu siguruar që të respektohet axhenda dhe të arrihen rezultatet.  Më poshtë është profili i kompanisë viktimë, Kompanisë Humor Products.  Humor Products (Humor) është një kompani Hungareze, e krijuar në 1 Janar 1960 që shet pjesë rezervë për makina të shtrenjta në të gjithë botën nëpërmjet Internetit. Të ardhurat e saj janë 20 milion Euro në vit. Është një biznes me rritje shumë të shpejtë me të ardhura që i rriten në vit me 250%. Kompania Humor mbështetet tek Interneti për më shumë se 85% të shitjeve të saj. Çdo ndërprerje e aftësisë për shitjet online do të kishte një efekt të rëndë në vazhdueshmërinë e biznesit. Kompania Humor sapo ka investuar 5 milion Euro në një depo të re shpërndarjeje dhe ka punësuar 20 punonjës të tjerë për të përballuar kërkesat. Fatkeqësisht, si të gjitha bizneset me rritje të shpejtë, procedurat e rikuperimit nga fatkeqësitë nuk janë në të njëjtin ritëm me rritjet e shitjeve dhe kompania nuk ka asnjë plan për rikuperimin nga fatkeqësitë apo vazhdimësinë e biznesit. Nuk ka asnjë pajisje rezervë që do t’i lejojë biznesit të vazhdojë normalisht punën në rast të mosfunksionimit të lidhjes së Internetit.  CEO dhe drejtor i Kompanisë Humor është Ratimir Novosel, që e mori kompaninë nga babai i tij në vitin 2004. Ai ka qenë përgjegjës për zhvillimin e shpejtë që nga ajo datë. Struktura e drejtimit të kompanisë nuk është zhvilluar në të njëjtin ritëm si aktiviteti i biznesit. Kompania Humor është mbytur në një farë mënyre nga suksesi i biznesit të tyre online.  Vaselko Ivankovic, që ka qenë me këtë kompani për 5 vjet, drejton sistemet e teknologjisë së informacionit dhe prezencën online të kompanisë. Ai është përgjegjës për menaxhimin e sistemeve si dhe sigurinë e biznesit online. Ai ia ka paraqitur vërejtjet e tij Drejtorit për 2 vjet se siguria e serverëve të kompanisë kërkon një ekzaminim dhe rinovim të sigurisë. Drejtori ka qenë shumë i zënë me zhvillimin e biznesit të tij dhe nuk i ka marrë seriozisht këto paralajmërime.  **Detajet e Kontaktit:**  Humor Products  7782 Sárok  Piroska u. 23. Hungary  **Tel:**(69) 912-707  **Email:**[humorproducts@gmail.com](mailto:humorproducts@gmail.com)  **Data e themelimit:** 1 Janar 1960  Skedarët e mëposhtëm përmbajnë mesazhet elektronike fillestare të dërguara viktimës nga keqbërësi dhe përgjigjet. Këto duhet t’ju jepen studentëve për ekzaminim:  2012-08-11 - Email 1 - 00007 to Humor products extortion email - no headers.pdf  2012-08-16 - Email 2 - 00007 to Humor products extortion email - no headers.pdf  2012-08-17 - Email 3 - Humor to 00007 - We cannot pay criminals email - no headers.pdf  2012-08-19 - Email 4 - 00007 to Humor Products - instruction email and attachments - no headers.pdf  2012-08-19 - Email 4 - attachment 387\_237 pixels.pdf  2012-08-19 - Email 4 - attachment 547\_558 pixels.pdf  2012-08-19 - Email 4 - attachment car-original.jpg  2012-08-21 - Email 5 - Humor Products to 00007 querying instructions for advertising car- no headers.pdf  2012-08-21 - Email 6 - 00007 to Humor Products - Apologies - no headers.pdf  2012-08-21 - Email 7 - Advert Placed - no headers.pdf  2012-08-25 - Email 8 - rgrealestate to Humor Products - Mercedes Advert has expired.pdf  Skedarët e mëposhtëm përmbajnë të njëjtin mesazh elektronik dhe me koka të zgjeruara. Ato duhet t’ju jepen pjesëmarrësve kur ata të kërkojnë kokat e zgjeruara:  2012-08-11 - Email 1 - 00007 to Humor products extortion email - headers.pdf  2012-08-16 - Email 2 - 00007 to Humor products extortion email- headers.pdf  2012-08-19 - Email 4 - 00007 to Humor Products - instruction email and attachments – headers.pdf  2102-08-21 - Email 6 - 00007 to Humor Products - Apologies - headers.pdf  Nëse pjesëmarrësit arrijnë në konkluzionin se kanë nevojë për deklaratat bankare të produkteve të Kompanisë Humor për të zhvilluar hetimin, duhet të jepet skedari i mëposhtëm. Ju lutem vini re se datat duhet të ndryshohen për të reflektuar periudhën kur do të zhvillohet kursi.  File name - 2012-10-25 - HSBC Bank Statements - Master Copy Transactions to 28th Oct 2012.pdf  Zhvilluesi i kursit dhe trajnerët duhet të sigurohen se i kanë lexuar dhe janë familjarë me mesazhet elektronike dhe dokumentet e tjerë me qëllim që zhvillimi i kursit të jetë efektiv.  Skenari është i drejtpërdrejtë; megjithatë, ai është hartuar në një mënyrë të tillë që pjesëmarrësit të duhet të identifikojnë pjesët që duhet të realizojnë hetimin. Është e rëndësishme të ndihmohet mësimi me dhënien e një informacioni minimal në fillim dhe më pas me prova të tjera si dhe kur ata identifikojnë ekzistencën e tyre. Për shembull, mesazhet elektronike pa koka duhet të jepen të parët dhe pjesëmarrësit më pas mund të kërkojnë informacion shtesë, si p.sh. kokat e zgjeruara. | |
|  | **Kontrolli i Njohurive**  Për këtë kurs nuk është parashikuar asnjë kontroll specifik për njohuritë përveç atij të renditur më lart. Nuk është kërkuar asnjë vlerësim zyrtar. | |

|  |  |  |
| --- | --- | --- |
| **Mësimi 1.1.4 - Prezantim – Bashkëpunimi Ndërkombëtar** | | **Kohëzgjatja: 30 Minuta** |
| **Objektivat:**  Në këtë sesion, pjesëmarrësit do të identifikojnë nevojën për bashkëpunim ndërkombëtar për hetimin e shumë veprave penale që mund të jenë kryer.   * Ata do të identifikojnë kanalet e bashkëpunimit ndërkombëtar dhe instrumentet e disponueshme, mënyrat e përdorimit të tyre, afatet kohore dhe efektivitetin e mënyrave të bashkëpunimit që janë të disponueshme. * Do të diskutohen avantazhet e mekanizmave të bashkëpunimit të përshkruara në Konventën e Budapestit për Krimin Kibernetik – të identifikojnë parimet e tij të përgjithshme, masat provizore dhe rrjetin 24/7 për ndihmën e ndërsjellë juridike. | | |
| **Nr. i Slajdit** | **Përmbajtja:** | |
| **Hyrja**  **Slajdi 1**  **Slajdi 2**  **Slajdi 3** | Ky sesion do të nënvizojë rëndësinë e bashkëpunimit ndërkombëtar për hetimin e çështjeve konkrete të krimit kibernetik. Do të përshkruhen instrumentet e disponueshëm për krimin kibernetik, kryesisht Konventa e Budapestit për Krimin Kibernetik.  **Objektivat e Sesionit**  Në këtë sesion pjesëmarrësit:   * Do të identifikojnë nevojën për bashkëpunim ndërkombëtar për hetimin e shumë prej veprave penale që mund të jenë kryer; * Do të identifikojnë kanalet e bashkëpunimit ndërkombëtar dhe instrumentet e disponueshëm, mënyrat e përdorimit, afatet kohore dhe efektivitetin e metodave të bashkëpunimit që janë të disponueshme; * Do të diskutojnë avantazhin e mekanizmave të bashkëpunimit të përshkruara në Konventën e Budapestit për Krimin Kibernetik dhe do të identifikojnë parimet e tij të përgjithshme, masat provizore dhe rrjetin 24/7.   **Axhenda**  Pjesa e Parë e prezantimit do të fokusohet tek nevojat për bashkëpunim ndërkombëtar në çështjet konkrete.  Pjesa e Dytë do të trajtojë disa instrumente dhe mekanizma të përgjithshëm të bashkëpunimit ndërkombëtar, përveç instrumenteve specifikë të përdorur në çështjet e krimit kibernetik.  Në Pjesën e Tretë do të trajtohen rregullat e bashkëpunimit ndërkombëtar të Konventës së Budapestit, si kujtesë nga trajnimi fillestar.  Pjesa e Katërt do të trajtojë në thellësi çështjen konkrete në shqyrtim, duke përforcuar nevojën konkrete dhe praktike për bashkëpunim ndërkombëtar.  Së fundi, Pjesa e Pestë do të trajtojë temat kryesore të të gjithë prezantimit. | |
| **Slajdi 4**  **Slajdi 5**  **Slajdi 6**  **Slajdi 7**  **Slajdi 8**  **Slajdi 9**  **Slajdi 10**  **Slajdi 11**  **Slajdi 12**  **Slajdi 13**  **Slajdi 14**  **Slajdi 15**  **Slajdi 16**  **Slajdi 17**  **Slajdi 18**  **Slajdi 19**  **Slajdi 20** | **Pjesa e Parë**  **Nevoja për bashkëpunim ndërkombëtar në çështje konkrete**  Është fakt i dukshëm se Interneti është i përhapur në të gjithë botën dhe mund të aksesohet dhe përdoret nga të gjithë në planet. Krimi Kibernetik duhet të trajtohet si fenomen global. Krimi kibernetik është më transnacionali ndër të gjithë krimet. Ata që duan të hetojnë krimin kibernetik duhet të jenë të ndërgjegjshëm se detyra e tyre kërkon një bashkëpunim ndërkombëtar efiçent. Në fakt, duke qenë global në natyrë, pa bashkëpunim ndërkombëtar, hetimet për krimin kibernetik nuk ka shumë të ngjarë të kenë sukses.  Avokatët hasin pyetje paraprake të vështira kur kryhet një krim në hapësirën kibernetike.  Interneti është kudo dhe nuk është e lehtë të përcaktohet vendndodhja përkatëse ligjore e krimit. Nëse, për shembull, keqbërësi vepron në Vendin A dhe kompjuteri i synuar i viktimës është në Vendin B, por komunikimi i paligjshëm i përdorur nga krimineli u realizua nga një kompani shërbimofruese e Internetit me bazë në Vendin C, dhe nëse të gjitha këto vende i përkasin juridiksioneve të ndryshme, pyetja e parë që një punonjës i zbatimit të ligjit duhet të zgjidhë është vendi i saktë ligjërisht i krimit, përsa i takon juridiksionit. Duhet të qartësohet vendi ku u krye krimi, në mënyrë që të mund të përcaktohet se cili është ligji material i zbatueshëm dhe se cili është juridiksioni kompetent (policia, prokuroria, gjykata).  Hetuesi duhet të respektojë juridiksionin e tij – kompetencën e tij territoriale. Sipas këtij këndvështrimi, juridiksioni do të jetë një kufi detyrues për hetimet penale. Ky realitet ngre dy pyetje të pazgjidhura.  E para ka të bëjë me hetimet ndërkufitare: si mundet një punonjës i zbatimit të ligjit të hetojë në mënyrë të ligjshme jashtë shtetit të tij, nëse i duhet të veprojë me urgjencë? Si mundet ai të marrë dhe të mbledhë prova të ruajtura “në derën ngjitur”, në një shtet tjetër nëse ai ndjen se provat mund të zhduken me shpejtësi?  Pyetja e dytë ka të bëjë me hetimin në “re”. Askush nuk e di se ku (fizikisht) mund të ruhen të dhënat, të ruajtura në “re”. Ndoshta, askush nuk e di cili është juridiksioni kombëtar për disa të dhëna në “re”. Si mundet një punonjës i zbatimit të ligjit të marrë dhe mbledhë të dhëna të ruajtura në “re”, kudo që të jenë të ruajtura fizikisht.  **Disa çështje praktike në lidhje me hetimet ndërkombëtare për krimin kibernetik**  Niveli i njohurive dhe përvojës së oficerëve të policisë dhe prokurorëve në raportimin dhe depozitimin e akuzave mund të jetë me rëndësi të madhe për të kuptuar sa më mirë çështjen dhe për ndërmarrjen e veprimeve adekuate dhe në kohë me qëllim ruajtjen dhe përftimin e provave.  Oficerët e policisë dhe prokurorët duhet të kërkojnë ndihmë shtesë kur ekziston nevoja, edhe nga brenda “shtëpisë” por edhe nga jashtë, duke përfshirë bashkëpunimin dhe kontributin nga viktima, që sigurisht ka interes në zgjidhjen e çështjes.  Specifikimi i instrumentit ligjor të përdorur për kërkimin e ndihmës – traktati, konventa ose instrument tjetër bashkëpunimi.  Identifikimi qartësisht se kush e bën hetimin/ndjekjen ligjore. Jepni të gjitha detajet e nevojshme të kontaktit dhe mjetet e preferuara të komunikimit.  Përmbledhja e çështjes – jepni një strukturë të detajuar të çështjes në hetim ose ndjekje ligjore, duke përfshirë një përmbledhje të provave që mbështesin hetimin/ndjekjen ligjore. Shpjegoni arsyetimin logjik për provat dhe veprimet që kërkohen në lidhje me hetimin në progres.  Referencë ndaj dispozitave ligjore kombëtare në fuqi – tekst i plotë i të gjitha dispozitave ligjore përkatëse në hetim/ndjekje ligjore, duke përfshirë dispozitat në fuqi për dënimet.  Saktësoni identifikimin e ndihmës që kërkohet – çfarë kërkoni me saktësi.  Jepni informacionin e mëposhtëm:  Për deklaratat/dëshminë e dëshmitarit:   * Vendndodhjen e personit * Rregullat procedurale kombëtare që lidhen me dëshmitarin * Të dhënat specifike dhe listën e pyetjeve të kërkuara nga dëshmitari   Për provat dokumentare:   * Një indikacion të qartë të dokumenteve që do të merren * Një indikacion të qartë në lidhje me vendin ku mund të gjenden asetet ose personin ose entitetin që i mban ato   Për provat elektronike:   * Specifikoni në sa më shumë detaje që të mundeni provat e mundshme elektronike që do të merren, jepni informacionin e nevojshëm teknik për provat që kërkohen nëse është i disponueshëm (ora e serverit/sistemit, korniza kohore, detajet identifikuese të tilla si adresat IP dhe MAC, adresat e postës elektronike, detajet e llogarisë së përdoruesit, etj. * Tregoni vendin dhe detajet ku gjenden asetet ose personin ose entitetin që i mban ato.   Për ekzekutimin e një urdhri kontrolli:   * Merrni një urdhër të vlefshëm kontrolli nga autoriteti gjyqësor vendas * Jepni tregues të saktë për vendin dhe objektet që do të kontrollohen * Specifikoni rregullat e detajuara që duhet të ndiqen në ekzekutimin e kontrollit * Jepni indikacione të sakta për provat të cilat do të kërkohen;   Për sekuestrim/konfiskim:   * Jepni një kopje të urdhrit të vlefshëm të sekuestrimit ose konfiskimit të lëshuar nga autoriteti gjyqësor vendas * Saktësoni indikacionet e objekteve të sekuestruar/konfiskuar * Tregoni rregulla specifike nëse nevojitet për ekzekutimin e kontrollit   Për masa hetimore të posaçme:   * Jepni një kopje të një urdhri të vlefshëm për SIMs, lëshuar nga autoriteti gjyqësor vendas * Specifikoni fushën e veprimit dhe natyrën e veprimeve që do të ndërmerren * Specifikoni kushtet e posaçme që duhet të respektohen – identitetin/anonimitetin e agjentëve të infiltruar, kriteret logjistike dhe teknike, mbulimin e kostove dhe shpenzimeve, specifikimi i kanaleve të komunikimit, etj. * Nëse është e nevojshme, pasja e një marrëveshjeje GPH të nënshkruar.   Nxirrni në pah çdo kriter specifik për konfidencialitetin.  Përcaktoni dhe specifikoni nivelin e urgjencës në ekzekutimin e kërkesës si dhe afatet kohore.  Identifikimin e duhur dhe sa me të saktë që të jetë e mundur të të dyshuarit/të dyshuarve – mbani mend se në këtë botë virtuale – identiteti mund të fshihet, modifikohet ose vidhet lehtësisht.  Identifikim i duhur i provave që do të kërkohen nëpërmjet Ndihmës së Ndërsjellë Juridike – prioritizimi i provave (përcaktimi i prioriteteve) – përzgjedhja vetëm e provave më të rëndësishme për hetimin – racionalizimi i burimeve dhe rritja e efiçencës.  Identifikimi i pikave të përshtatshme të kontaktit në vendet e tjera – pikat 24/7 në dritën e Konventës së Budapestit, kanalet e Interpolit, etj. – veçanërisht për çështjet “e nxehta” ku duhet të ndërmerren veprime imediate për të siguruar dhe ruajtur të dhënat dixhitale (provat elektronike).  Përcaktimi i kontakteve informale me homologë të përshtatshëm përpara depozitimit të kërkesave zyrtare për Ndihmë të Ndërsjellë Juridike me qëllim informimin e tyre për kërkesa të ardhshme, duke kryer kontrolle operacionale me qëllim specifikimin e kërkesës në mënyrë sa më të detajuar.  Të siguroheni se juridiksioni është identifikuar siç duhet përsa i takon faktit se ku ndodhen provat/keqbërësit/viktimat duke mbajtur parasysh thjesht çështje teknologjike të tilla si pronësia e të dhënave elektronike, vendndodhja fizike e serverit/ISP-s dhe rezidenca ligjore e pronarit/pronarëve të serverit/ISP-s – d.m.th rasti kur serverët mund të ndodhen në një shtet të caktuar ose në rastin e shërbimeve informatike të ofruara në “Re” me pronar të regjistruar dhe që veprojnë në një juridiksion të ndryshëm.  Zona të ndryshme kohore – vështirësi në vendosjen e kontakteve edhe në përdorimin e mjeteve moderne të komunikimit (d.m.th telekonferencat) – mund të vonojë kërkesa për hetim/NNJ dhe të rrisë kostot – ka akoma zyra policie dhe prokurorie që nuk kanë akses në telefonatat ndërkombëtare!  Përkthimi i dokumenteve – shumë shtete mund të kërkojnë që Ndihma e Ndërsjellë Juridike të përkthehet në gjuhën(t) e tyre zyrtare.  Pengesat e gjuhës gjatë kontakteve të drejtpërdrejta ose informale ndërmjet prokurorëve dhe punonjësve të zbatimit të ligjit.  Nivele të ndryshme rëndësie për hetimet e krimeve kibernetike në vende të ndryshme. Krimet kibernetike të lidhura me ekonominë do të ishin në fund të listës së prioriteteve në vendet ku mbizotëron krimi i dhunshëm; krimi i organizuar dhe terrorizmi i lidhur me krimin kibernetik do të kishin një rëndësi krejt të ndryshme, etj. Si rezultat mund të jetë që kërkesave për ndihmë në çështjet e krimit kibernetik thjesht iu jepet një prioritet i ulët, veçanërisht atyre që vijnë nga vendet me aspak ose pak histori bashkëpunimi në situata të ndërsjella.  Merrni në konsideratë dhënien e mbështetjes teknike ose me ekspert nëse pala kërkuese nuk ka kapacitete për të ekzekutuar kërkesën tuaj.  Merrni në konsideratë dhe përdorimin e masave dhe mjeteve hetimore tradicionale sa herë që është e mundur – oficerët e policisë/prokurorët janë më të mësuar me të, nganjëherë mund t’i shërbejë qëllimit dhe të japë prova të mjaftueshme për hetimin e suksesshëm dhe procedimin penal. | |
| **Slajdi 22**  **Slajdi 23**  **Slajdi 24**  **Slajdi 25**  **Slajdi 26** | **Pjesa e Dytë**  **Mekanizmat e Përgjithshëm të Bashkëpunimit Ndërkombëtar**  Interneti është i shtrirë tashmë në të gjithë botën dhe përdoret nga të gjithë në planet. Krimi kibernetik duhet të trajtohet si një fenomen global.  Konventa Evropiane për Ndihmën e Ndërsjellë në Çështjet Penale e Këshillit të Evropës, e vitit 1959, është baza e të gjithë bashkëpunimit gjyqësor ndërkombëtar në Evropë, madje edhe në çështjet e krimit kibernetik.  Në fakt, Konventa e Budapestit nuk i mbulon të gjitha çështjet ekzistuese të bashkëpunimit ndërkombëtar dhe thjesht pretendon të mbulojë kanale dhe modalitete bashkëpunimit të reja dhe që nuk kanë ekzistuar më parë.  Të gjitha Shtetet Anëtare e Këshillit të Evropës (me përjashtim të San Marinos) e kanë ratifikuar Konventën e vitit 1959, gjë e cila do të thotë se nga të gjitha Palët e Konventës së Budapestit, e vetmja Palë jo anëtare e Konventës janë Shtetet e Bashkuara të Amerikës.  Ky fakt vërteton vlerën e shtuar të Konventës së Budapestit, e cila krijoi për herë të parë një kornizë të përbashkët ligjore për bashkëpunimin ndërkombëtar policor dhe gjyqësor ndërmjet shumicës së Shteteve Evropiane dhe Shteteve të Bashkuara. Ky është një aspekt veçanërisht i rëndësishëm sepse Neni 14/2 thotë se procedurat e bashkëpunimit ndërkombëtar të Konventës do të zbatohen krahas veprave penale të përcaktuara në përputhje me Nenet 2 deri 11 të Konventës, si dhe veprat e tjera penale të kryera me anë të një sistemi kompjuterik dhe për mbledhjen e provave në formë elektronike të ndonjë vepre tjetër penale.  Bashkimi Evropian është një mbështetës i madh i Konventës së Budapestit – dhe ka marrë pjesë madje, si vëzhgues, në punimet e hartimit të Konventës. Që nga ajo kohë, Bashkimi Evropian i inkurajon Shtetet Anëtare të ratifikojnë Konventën.  Por sigurisht, brenda Bashkimit Evropian, një gamë e gjerë mjetesh të bashkëpunimit ndërkombëtar, madje edhe jashtë qasjeve më të fundit, bazuar në parimin e njohjes reciproke.  Shumica e avantazheve të sistemeve Evropiane bazohen në mundësinë e kontakteve të drejtpërdrejta ndërmjet autoriteteve gjyqësore nga secili Shtet Anëtar. Në përputhje me këtë mundësi, secili gjyqtar dhe prokuror mund të bëjë direkt një kërkesë tek një gjyqtar ose një prokuror tjetër. Ky është një mjet shumë i fortë në lidhje me hetimit, gjithashtu i përshtatshëm në çështjet e krimit kibernetik.  Këto kontakte të drejtpërdrejta operacionale mbështeten nga një strukturë e organizuar e pikave gjyqësore të kontaktit - Atlasi – që i lejon praktikantëve të identifikojnë menjëherë autoritetin lokal kompetent në secilin Shtet Anëtar për marrjen dhe ekzekutimin e kërkesës për ndihmë ligjore të ndërsjellë. Atlasi është një mjet kompjuterik që i lejon praktikantëve të identifikojnë autoritetin lokal.  Pikat e kontaktit, të përfshira në Atlas, janë ndërmjetës aktivë me detyrën e lehtësimit të bashkëpunimit gjyqësor ndërmjet Shteteve Anëtare. Supozohet se pikat e kontaktit janë të disponueshme për kontaktim nga autoritetet gjyqësore lokale, në lidhje me ndërmjetësimin dhe lehtësimin e bashkëpunimit gjyqësor ndërmjet Shteteve Anëtare dhe gjithashtu për mbështetjen e atyre autoriteteve për përgatitjen e kërkesave për bashkëpunim gjyqësor.  Një lloj i tillë rrjeti, për realizimin e shpejtë dhe të lehtë të kërkesave për bashkëpunim ndërkufitar, mund të jetë i vlefshëm në mbledhjen e provave elektronike.  Interpoli është një organizatë ndërkombëtare e policisë me 190 anëtarë nga të gjitha kontinentet. Për arritjen e objektivit të tij, përmirësimin dhe lehtësimin e bashkëpunimit, Interpoli krijoi një sistem global për komunikimin e policive dhe zhvilloi databaza specifike dhe analiza të informacionit të policisë: një rrjet pikash kontakti (Interpol National Central Reference Points - NCRP[[3]](#footnote-4)), i cili përpiqet të japë ndihmë të vazhdueshme për anëtarët e tij.  Deri në Shtator 2011, NCRP-ja kishte rreth 120 pika reference në të gjithë botën. Këto pika reference miratuan strukturën e pikave të kontaktit 24/7 të krijuar nga Neni 35 i Konventës Evropiane për Krimin Kibernetik.  Objektivi i kësaj strukture është mundësimi që policia të identifikojë menjëherë ekspertët në vendet e tjera dhe të marrë menjëherë ndihmë në hetimet kompjuterike dhe mbledhjen e provave. Ky rrjet është i disponueshëm 24 orë në ditë, shtatë ditë në javë.  Fusha e zbatimit të NCRP-s është të realizojë shkëmbimin e të dhënave dhe informacionit ndërmjet anëtarëve të saj dhe të ofrojë mbështetje teknike dhe operacionale. Në fakt, synimi kryesor i NCRPs është garantimi se informacioni i zakonshëm policor të mund të shkëmbehet sa më shpejt që të jetë e mundur, nëpërmjet kanaleve të përshtatshme dhe të posaçme të Interpolit; kjo përfshin informacionin për terroristët e dyshuar, personat në kërkim, gjurmët e gishtërinjve, profilet e ADN-s, dokumentet e udhëtimit të vjedhura ose të humbura, automjetet e vjedhura, veprat e artit të vjedhura, etj. Ky lloj i informacionit potencialisht të rëndësishëm të dhënë nga Interpoli është sigurisht shumë i dobishëm në hetimet konkrete. Megjithatë, saktësisht për shkak të fushës së veprimit të rrjetit, ai nuk mund të përdoret për të kërkuar me urgjencë, për shembull, ruajtjen e të dhënave kompjuterike, ose ruajtjen e të dhënave të trafikut, ose ndonjë lloj tjetër masë për marrjen ose ruajtjen e provave. Me fjalë të tjera, lloji i bashkëpunimit që mund të ofrohet nga ky rrjet specifik i Interpolit bazohet në të njëjtat parime që zbatohen për bashkëpunimin e përgjithshëm të Interpolit. | |
| **Slajdi 28**  **Slajdi 29**  **Slajdi 30**  **Slajdi 31**  **Slajdi 32**  **Slajdi 33**  **Slajdi 34**  **Slajdi 35**  **Slajdet 36 dhe 37** | **Pjesa e Tretë**  **Mekanizmat e Bashkëpunimit Ndërkombëtar të Konventës së Budapestit për Krimin Kibernetik**  Rregullat e Konventës në lidhje me bashkëpunimin ndërkombëtar përshkruhen në kapitullin III të Konventës. Shumica e rregullave në këtë kapitull janë rregulla operacionale dhe procedurale, të përfshira gjithashtu edhe në konventa të tjera ndërkombëtare. Të tjerët janë më inovative dhe duhet të ekzaminohen në detaje.  Neni 26 përshkruan situatën që ndodh ku autoritetet e një Pale, gjatë një hetimi ndërkombëtar penal, zbulojnë se një pjesë e informacionit që kanë marrë duhet t’i përcillet autoriteteve të një Shteti tjetër – por pa marrë kërkesë nga ai Shtet. Kjo mund të bëhet nëse informacioni duket të jetë i dobishëm ose i nevojshëm për të filluar një hetim në lidhje me një vepër penale në kuadër të Konventës.  Ndonëse ndihma reciproke në të kaluarën ka qenë zakonisht pasive, ku shteti A i kërkonte ndihmë shtetit B, Konventa inkurajon një qasje më proaktive. Megjithatë, kjo dhënie “spontane” informacioni, në përputhje me pikën 2 të Nenit 26, mund t’i nënshtrohet disa kushteve, si për shembull kërkimin e konfidencialitetit ose një përdorim specifik të të dhënave.  Neni 29 është një nga dispozitat më të rëndësishme të Konventës së Budapestit. Neni 29 përcakton rregulla në lidhje me ruajtjen e përshpejtuar të të dhënave të memorizuara në një sistem kompjuterik. Ky nen siguron një kuadër paralel ndaj dispozitës së brendshme në lidhje me ruajtjen e përshpejtuar të të dhënave. Në përgjithësi, kjo dispozitë i lejon një Pale Kontraktore të kërkojë nga një Palë tjetër ruajtjen e përshpejtuar të të dhënave, nëse në të njëjtën kohë ajo shpreh synimin e saj për të bërë një kërkesë zyrtare për ndihmë për një kontroll, ose një sekuestrim ose një masë të ngjashme.  Në këtë rast, pala e kërkuar duhet të veprojë si të jetë e nevojshme, me të gjithë zellin e duhur, për të ruajtur të dhënat e kërkuara, në përputhje me ligjin e saj të brendshëm.  Siç u përmend më parë, ky është një mjet i ri i bashkëpunimit ndërkombëtar.  Është e rëndësishme të merret në konsideratë, se kriminaliteti i dyfishtë nuk mund të kërkohet nga pala e kërkuar, si një kusht i mbrojtjes së të dhënave.  Ky instrument i ri është rezultati i specifikës së mjedisit dixhital. Dihet se ndihma ndërkufitare është shumë konsumuese përsa i takon kohës. Karakteri i përshpejtuar i masës është një nevojë e imponuar nga domosdoshmëria për të ruajtur diçka që në pak momente mund të zhduket plotësisht.  Është me vend të themi se kjo është vetëm një masë ruajtjeje, për arsye urgjente dhe nuk nënkupton automatikisht zbulim të të dhënave të ruajtura. Në fakt, në rastet ku lejohet një zbulim i të dhënave, ka rregulla shumë të ngushta të cilat e lejojnë atë, sidomos nëse të dhënat nuk janë thjesht të dhëna trafiku.  Në terma praktikë, një ruajtje e përshpejtuar e të dhënave mund të realizohet dhe pastaj më vonë, mund të rezultojë se ka arsye për të mos i zbuluar të dhënat palës që i kërkon ato.  Zbulimi i të dhënave të trafikut përshkruhet në zbatim të Nenit 30 të Konventës së Budapestit. Në lidhje me të dhënat e trafikut, teksti i Konventës përcakton një model më të lehtë për lehtësimin e bashkëpunimit ndërkombëtar. Nuk ka rregulla specifike për një zbulim të përshpejtuar të të dhënave, sepse nuk ka rregulla specifike për zbulimin e përshpejtuar në nivel kombëtar, në kapitullin e rregullave procedurale. Në fakt, duke e nënkuptuar, Konventa harmonizon rregullat e brendshme për ruajtjen e përshpejtuar të provave dhe rregullat që rregullojnë bashkëpunimin ndërkombëtar.  Neni 31 i Konventës përcakton një rregull të përgjithshëm për ndihmën reciproke në lidhje me hyrjen tek të dhënat e ruajtura kompjuterike. Megjithëse ky nen dhe Neni 23 të cilit i referohet, shprehin një aspiratë të përgjithshme që palët të bashkëpunojnë në ndjekjen e krimit kibernetik në “shtrirjen më të gjerë të mundshme”, ai nuk krijon detyrime të reja për bashkëpunim. I gjithë bashkëpunimi i nënshtrohet traktateve ekzistuese dhe instrumenteve ndërkombëtarë që rregullojnë bashkëpunimin ndërkufitar në hetimet tradicionale.  Neni 32 përcakton mundësinë që i jepet institucioneve të zbatimit të ligjit nga një Shtet Palë në Konventë për marrjen e provave të ruajtura në një kompjuter që fizikisht ndodhet në territorin e një Pale tjetër, pa ndonjë kërkesë për bashkëpunim ndërkombëtar.  Përsa i takon të dhënave nga burime të hapura, duhet të vërehet se ky hetim “me burim të hapur” është diçka që çdo shtetas mund ta bëjë me iniciativën e tij në shumicën e vendeve.  Ana tjetër e dispozitës është një mjet hetimi shumë inovativ, pa ekuivalent në botën fizike. Në fakt, metodologjia tradicionale e hetimit jashtë kufijve supozon që një oficer duhet të udhëtojë fizikisht në shtetin tjetër dhe të kërkojë ndihmë nga autoritetet lokale. Ai nuk mund të bëjë gjë vetë dhe çdo veprim hetimor duhet të praktikohet në emër të autoriteteve kombëtare të vendit.  Neni 32 thotë të kundërtën: çdo punonjës i zbatimit të ligjit mund të marrë informacion nga një shtet tjetër, edhe sikur të mos jetë “me burim të hapur”, nëse personi që ka autoritetin ligjor për zbulimin e të dhënave jep pëlqimin e tij – edhe pa ndonjë autorizim nga Shteti me juridiksionin e vendit ku ruhen të dhënat.  Neni 33 ka të bëjë me bashkëpunimin ndërkombëtar për interceptimin e komunikimeve. Në fakt ky nuk është një instrument i ri: atij i referohen instrumente të tjerë detyrues ndërkombëtarë. Megjithatë Neni 33 ka një fushëveprimi specifike: mbledhjen në kohë reale të të dhënave të trafikut.  Nga ana tjetër, rregulli më i rëndësishëm i deklaruar në Nenin 33 i referohet limiteve të zbatimit të kësaj mase hetimore. Dhe limitet janë kushtet dhe procedurat e parashikuara në zbatim të ligjit të brendshëm. Pra, ky modalitet i bashkëpunimit do të përcaktohet nga secili Shtet në të njëjtat 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.  Një nga dispozitat më të rëndësishme operacionale të Konventës është Neni 35, që vendos për të gjitha Palët Kontraktore detyrimin për të krijuar një pikë kontakti të disponueshme në mënyrë të vazhdueshme (një të ashtuquajtur rrjet pikash kontakti 24/7).  Objektivi i përgjithshëm i këtyre pikave të kontaktit është lehtësimi i bashkëpunimit ndërkombëtar, me anë të dhënies së konsulencës teknike për pikat e tjera të kontaktit, duke aktivizuar mekanizimin e duhur të ruajtjes së përshpejtuar të të dhënave, mbledhje urgjente të provave, ose identifikim dhe zbulim të personave të dyshuar.  **Vlera e shtuar e këtij rrjeti: mund të ofrojë ndihmë dhe bashkëpunim shumë shpejt edhe sikur një kërkesë zyrtare për bashkëpunim mund të bëhet në rrugë informale.** | |
| **Slajdi 39**  **Slajdi 40**  **Slajdi 41**  **Slajdi 42**  **Slajdi 43**  **Slajdi 44** | **Pjesa e Katërt**  Nevoja për bashkëpunim ndërkombëtar në çështje konkrete – çështja në diskutim  **Hapat dhe masat e Ndihmës së Ndërsjellë Juridike:**   1. Kërkesë shtetit në juridiksionin e të cilit është uebsajti [www.hushmail.com](http://www.hushmail.com), me qëllim që të merren të dhëna të disponueshme për llogarinë "0007". 2. Nëse analiza kriminalistike e sulmit/sulmeve DDoS mbi produktet e kompanisë humour jep të dhëna shtesë për Kompaninë Shërbimofruese të Internetit të sulmuesve, NNJ duhet të lëshohet për marrjen e të dhënave nga ISP lokale në shtetet ku e ka origjinën adresa IP. 3. Mbas kryerjes së analizës kriminalistike të uebsajtit <http://hungary.carssale.eu> dhe përcaktimit të IP-ve për ata që kanë aksesuar dhe shkarkuar foto të postuara nga Kompania Humor dhe të kërkuara nga i dyshuari, NNJ duhet të lëshohet në vendin e origjinës për ato adresa IP me qëllim që të merren të dhënat dhe provat për pronarin/përdoruesin e adresës IP. 4. Sapo identifikohen korrierët, dërgoni kërkesat për NNJ në shtetet e tyre të banimit me qëllim që t’i merrni ata në pyetje si të dyshuar/dëshmitarë, kontrolloni kompjuterët e tyre për prova në lidhje me Ralf Mylerin dhe sekuestroni kartat e kreditit dhe prova të tjera të disponueshme (letrat nga bankomatet, regjistrimet e kamerave të vëzhgimit të bankomateve, etj.). 5. Kur vërtetohet fajësia për (disa) korrierët, merrni parasysh lëshimin e NNJ-ve për ekstradimin e tyre (urdhra arresti) ose, kur nuk është i mundur ekstradimi, transferimi i çështjes dhe procedimit penal në shtetin e origjinës/banimit të korrierit. | |
| **Slajdet 46 dhe 47** | **Pjesa e Pestë**  **Përmbledhja**  Në mbyllje të sesionit, pjesëmarrësit duhet   * Të njohin dimensionin global të Internetit dhe rëndësinë e bashkëpunimit ndërkombëtar në fushën e krimit kibernetik * Të identifikojnë nevojën e bashkëpunimit ndërkombëtar për hetimin e shumë prej veprave penale që mund të jenë kryer; * Të identifikojnë kanalet e bashkëpunimit ndërkombëtar dhe instrumentet e disponueshëm, mënyrat e përdorimit të tyre, afatet kohore dhe efektivitetin e metodave të bashkëpunimit që janë të disponueshme; * Njohin avantazhin e mekanizmave të bashkëpunimit të përshkruara në Konventën e Budapestit për Krimin Kibernetik dhe identifikoni parimet e tij të përgjithshme, masat provizore dhe rrjetin 24/7. | |

|  |  |  |
| --- | --- | --- |
| Mësimi: 1.1.5 – Puna në Grup – Bashkëpunimi Ndërkombëtar | | **Kohëzgjatja: 60 Minuta** |
| **Burimet materiale të kërkuara:**   * Një sallë e përshtatshme për një numër të parashikuar pjesëmarrësish. Kjo sallë duhet të rregullohet duke vendosur një tryezë të rrumbullakët për çdo grup, ku është e mundur, bazuar në një numër prej 6 pjesëmarrësish në grup. * 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) * Kopje të Guidës për Provat Elektronike të Këshillit të Evropës * Dërrasë të Bardhë për secilin grup * Markera për Dërrasë të Bardhë (të paktën 2 për secilën ngjyrë: blu, të zezë, të kuqe dhe jeshile) për secilin grup * 1 Tabelë Flipchart me letër të mjaftueshme për secilin grup * Stilolapsa dhe blloqe për pjesëmarrësit * Kapëse aktesh, vrimahapëse dhe gërshërë për secilin grup * Ngjitës Blu ose një produkt të ngjashëm me të për ngjitjen e përkohshme të letrës në mure për secilin grup * Një kompjuter laptop për secilin grup të ngjashëm me kompjuterin e trajnerit dhe me akses në Internet që të realizohen kërkimet hetimore. * Të gjitha materialet mbështetëse të dhëna me paketën e trajnimit. | | |
| **Synimi:** Ky sesion është hartuar t’i lejojë pjesëmarrëse të ekzaminojnë natyrën e hetimeve ndërkombëtare që ata duhet të kryejnë me qëllim marrjen e provave të veprave penale që kanë identifikuar në fazën e planifikimit të hetimit. Ata duhet të marrin në konsideratë nivelet e ndryshme të bashkëpunimit që janë të disponueshme. | | |
| **Objektivat:**  Në përfundim të sesionit pjesëmarrësit do të jenë në gjendje të:   * Zbatojnë mekanizmat e bashkëpunimit ndërkombëtar në skenar * Detajojnë kërkimet e nevojshme për ruajtjen dhe marrjen e provave nga jashtë shtetit * Zhvillojnë një plan për marrjen e provave nga jashtë shtetit në mënyrën më efektive. * Marrin parasysh implikimet e hetimit të vonesave në mekanizmat e bashkëpunimit ndërkombëtar | | |
| **Nr. i Slajdit** | **Përmbajtja:** | |
|  | Nuk ka prezantim për këtë sesion. | |
|  | **Ushtrime Praktike (nëse ka)**  Edhe njëherë, ky është një sesion praktik, ku pjesëmarrësit do të shqyrtojnë planin e tyre të hetimit nga perspektiva e sigurimit dhe marrjen e provave që lidhen me skenarin. Informacioni i dhënë duhet tashmë t’i ketë pajisur pjesëmarrësit me mjaft konsiderata përsa i takon ruajtjes së të dhënave që ka të ngjarë të eliminohen përpara lëshimit të NNJ-ve dhe marrjes së mëpasshme të të dhënave të ruajtura në formë evidenciare. Prezantimi në sesionin e kaluar duhet të përdoret nga pjesëmarrësit për të identifikuar dhe prioritizuar metodat më të mira. | |
|  | **Kontrolli i Njohurive**  Nuk është parashikuar asnjë kontroll specifik për njohuritë krahas atyre që janë renditur më lart për këtë kurs. Nuk është kërkuar asnjë vlerësim zyrtar. | |

|  |  |  |
| --- | --- | --- |
| Mësimi: 1.1.6–Puna në Grup – Identifikimi i të Dyshuarve | | **Kohëzgjatja: 60 Minuta** |
| **Burimet materiale të kërkuara:**   * Një sallë e përshtatshme për një numër të parashikuar pjesëmarrësish. Kjo sallë duhet të rregullohet duke vendosur një tryezë të rrumbullakët për çdo grup, ku është e mundur, bazuar në një numër prej 6 pjesëmarrësish në grup. * 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) * Kopje të Guidës për Provat Elektronike të Këshillit të Evropës * Dërrasë të Bardhë për secilin grup * Markera për Dërrasë të Bardhë (të paktën 2 për secilën ngjyrë: blu, të zezë, të kuqe dhe jeshile) për secilin grup * 1 Tabelë Flipchart me letër të mjaftueshme për secilin grup * Stilolapsa dhe blloqe për pjesëmarrësit * Kapëse aktesh, vrimahapëse dhe gërshërë për secilin grup * Ngjitës Blu ose një produkt të ngjashëm me të për ngjitjen e përkohshme të letrës në mure për secilin grup * Një kompjuter laptop për secilin grup të ngjashëm me kompjuterin e trajnerit dhe me akses në Internet që të realizohen kërkimet hetimore. * Të gjitha materialet mbështetëse të dhëna me paketën e trajnimit | | |
| **Synimi:** ky sesion ofron mundësinë që pjesëmarrësit të mbledhin të gjitha provat që u janë dhënë në ditën e parë dhe të shqyrtojnë identitetin e çdo të dyshuari me qëllim që të zhvillojnë një strategji për rikuperimin e provave dhe arrestimin. | | |
| **Objektivat:**  Në fund të këtij sesioni, pjesëmarrësit do të jenë në gjendje të:   * Shqyrtojnë provat e marra * Identifikojnë të dyshuarit e çështjes * Identifikojnë dëshmitarët e çështjes * Zhvillojnë një strategji për arrestimin e të dyshuarve * Identifikojnë çështjet rikuperimit të provave * Përgatiten për arrestimin dhe kontrollin e ambienteve të të dyshuarit * Përgatisin kërkesat ndërkombëtare të mbështetjes për strategjinë e arrestimit. | | |
| **Nr. i Slaidit** | **Përmbajtja:** | |
|  | Nuk ka asnjë prezantim për këtë sesion. | |
|  | **Ushtrime Praktike (nëse ka)**  Ky sesion është sesioni i fundit praktik në ditën e parë të kursit. Pjesëmarrësit do të kenë mbledhur të gjitha provat e disponueshme dhe do të shqyrtojnë identitetin e të gjithë të dyshuarve. Më pas ata do të zhvillojnë një strategji për arrestimin, kontrollin dhe sekuestrimin si dhe të identifikojnë aspektet e bashkëpunimit ndërkombëtar që janë të domosdoshme. Në fund të sesionit pjesëmarrësit duhet të kenë arritur në konkluzion se keqbërësi kryesor është Ralf Myler. Nëse ata nuk e kanë arritur këtë konkluzion, duhet të kërkojnë ndihmë nga trajneri, i cili duhet të shpjegojë sesi duhet të arrihet konkluzioni në një hetim.  Sesioni i ditës pasuese mbështetet tek identifikimi i Mylerit sipas skenarit, ai duhet të jetë arrestuar në fillim të ditës së dytë, kompjuteri i tij të jetë sekuestruar dhe të jetë kryer një ekzaminim kriminalistik. Ky ekzaminim do të jetë pjesa e dytë e prezantimit të kriminalistikës dixhitale në ditën e dytë. | |
|  | **Kontrolli i Njohurive**  Për këtë kurs nuk është parashikuar asnjë kontroll specifik i njohurive krahas atyre të renditura më lart. Nuk është kërkuar asnjë vlerësim zyrtar. | |

|  |  |  |
| --- | --- | --- |
| Mësimi: 1.2.1 – Rishikim Ditor | | **Kohëzgjatja: 15 Minuta** |
| **Burimet materiale të kërkuara:**   * Kompjuter Laptop ose Kompjuter tavoline me Sistemin Windows 7 dhe me Programin Office 2010 * Projektor * Prezantim me PowerPoint | | |
| **Synimi:**  Synimi i këtij kursi është rishikimi i aktiviteteve të ditëve të mëparshme, marrja e vlerësimit nga pjesëmarrësit dhe kontrolli që objektivat janë arritur. | | |
| **Objektivat:**  Në përfundim të sesionit pjesëmarrësit do të jenë në gjendje të:   * Identifikojnë fushat e aktiviteteve të ditëve të mëparshme që kanë kuptuar * Identifikojnë fusha të tillë ku ata kanë nevojë të rishikojnë materialet për të sjellë njohuritë e tyre në nivelin e kërkuar | | |
| **Hyrje**  Ky sesion është përgatitur që t’i lejojë pjesëmarrësve të kontrollojnë se i kanë kuptuar mësimet e ditëve të mëparshme dhe se janë në gjendje të përmbushin objektivat e sesioneve individuale. Ky është sesion është gjithashtu për t’i dhënë mundësinë trajnerit të kontrollojë nivelin e njohurive të pjesëmarrësve dhe të identifikojë fushat ku mund të përmirësohen materialet e mësimdhënies. | | |
| **Slajdet**  **1 deri 4** | **Prezantimi me PowerPoint** (ose prezantim i ndonjë lloji tjetër)  Slajdet në këtë prezantim jepen për të ndihmuar trajnerin dhe pjesëmarrësit me aktivitetet e ditëve të mëparshme. Trajneri duhet të bëjë përmbledhjen e këtyre aktiviteteve duke përdorur programin dhe objektivat si standarde. | |
|  | **Ushtrime Praktike** (nëse ka)  Për këtë sesion nuk është përgatitur asnjë ushtrim praktik, megjithatë trajneri duhet të informojë pjesëmarrësit se Myleri është arrestuar në përfundim të ditës së dytë, kompjuteri i tij është sekuestruar dhe është kryer një ekzaminim kriminalistik. Kjo çon drejt ditës së dytë. | |
|  | **Kontrolli i Njohurive**  Trajneri duhet të kontrollojë njohuritë duke bërë pyetjet përkatëse për secilin nga aspektet e trajnimit. | |
|  | **Përmbledhje**  I gjithë ky sesion është hartuar si një përmbledhje e aktiviteteve të ditëve të mëparshme dhe nuk kërkohet asnjë përmbledhje specifike. | |

|  |  |  |
| --- | --- | --- |
| Mësimi: 1.2.2–Prezantim–Kriminalistika Dixhitale–Pjesa 1 | | **Kohëzgjatja: 60 Minuta** |
| **Burimet materiale të kërkuara:**   * Kompjuter Laptop ose Kompjuter tavoline me sistem Windows 7 dhe me Office 2010 * Projektor * Prezantim me PowerPoint | | |
| **Synimi:** synimi i këtij sesioni është rritja e ndërgjegjësimit të pjesëmarrësve në lidhje me shkencën e kriminalistikës dixhitale dhe vlerën e saj për hetimet penale. Ajo gjithashtu jep informacion në lidhje me provat e gjetura në lidhje me skenarin. | | |
| **Objektivat:**  Në përfundim të sesionit pjesëmarrësit do të jenë në gjendje të:   * Shpjegojnë termin Kriminalistika Dixhitale * Krahasojnë Kriminalistikën Dixhitale me shkencat tradicionale të kriminalistikës * Përkufizojnë të paktën tre nën-degë të Kriminalistikës Dixhitale * Identifikojnë katër hapa në ekzaminimet e kriminalistikës dixhitale * Diferencojnë dy kategoritë e gjurmëve dixhitale * Përshkruajnë se si Kriminalistika Dixhitale mund të mbështesë hetimet * Paraqesin sesi funksionon Steganografia * Krahasojnë tre metodat sesi të rikuperohen skedarët e fshirë * Karakterizojnë llojet e ndryshme të Hapësirës së Papërdorur në Sistemin e Skedarëve * Zbatojnë teorinë e kriminalistikës dixhitale në një skenar praktik * Identifikojnë përfitimet e ekzaminimit të Kriminalistikës Dixhitale * Përshkruajnë sesi Virtualizimi mund të ndihmojë Kriminalistikën Dixhitale | | |
| **Nr. i Slajdit** | **Përmbajtja:** | |
| **Slajdi 4**  **Slajdi 5**  **Slajdi 6**  **Slajdi 7**  **Slajdi 8**  **Slajdi 9**  **Slajdi 10**  **Slajdi 11**  **Slajdi 12**  **Slajdi 13**  **Slajdi 14**  **Slajdi 15**  **Slajdi 16**  **Slajdi 17**  **Slajdi 18**  **Slajdi 19**  **Slajdi 20**  **Slajdi 21**  **Slajdi 22**  **Slajdi 23**  **Slajdi 24**  **Slajdi 25**  **Slajdi 26**  **Slajdi 27** | Shënim: ky slajd është i animuar  Nga vjen termi Digital Forensics[[4]](#footnote-5)?  Për të shpjeguar termin “Digital Forensics” duhet të kuptojmë kuptimin e dy fjalëve. Le të fillojmë më fjalën e fundit: Forensics  Termi “Forensics” vjen nga termi romak “Forum Romanum”, i cili ishte vendi që përbënte qendrën e jetës në Romën Perandorake. Fjala “Forum” në Latinisht nënkupton ekzaktësisht këtë vend publik. Në njërën anë të “Forum Romanum” disa ndërtesa përdoreshin si vende për gjykatat e juridiksionit civil. Pra fjala “Forensics” e ka origjinën e saj në gjykatat e lashta. Njësoj si gjykatat e lashtë në Romën perandorake, ne kemi një gamë të gjerë gjykatash në çdo juridiksion [klik] [klik].  Edhe në gjykatat e lashta, ju mund të gjeni ekspertë të fushave të ndryshme që mund të shpjegonin temat shkencore për avokatët dhe jurinë. [klik] Ky miku ynë në këtë foto përpiqet të shpjegojë formulat matematikore një jurie – një detyrë shumë e komplikuar në ato kohëra – me shumë mundësi edhe sot ;) Funksioni i ekspertit si dëshmitar nuk është i ndryshëm në seancat gjyqësore të ditëve të sotme, për shembull merrni një ekspert të kriminalistikës dixhitale [klik] [klik]. Njësoj siç kanë nevojë gjykatat e lashta për ekspert dëshmitar për shpjegimin e formulave matematikore, po kështu edhe për provat dixhitale nevojitet ekspert dëshmitar në gjykatat e sotme.  Për të kuptuar lidhjen e Kriminalistikës Dixhitale me shkencat e tjera kriminalistike, le të shikojmë disa shembuj.  Kush nga pjesëmarrësit në sallë ka pasur përvoja në seancat gjyqësore që kanë të bëjmë me shkencat kriminalistike të përmendura në këtë slajd?  Ok, në fillim pamë se X pjesëmarrës kanë përvoja me Kriminalistikën Dixhitale, ndërsa pothuaj të gjithë juve keni pasur seanca gjyqësore që përfshinin disa nga shkencat kriminalistike më tradicionale. Kjo nënvizon se Kriminalistika Dixhitale është shkencë mjaft e re ndërsa shkencat e tjera kriminalistike kanë një histori më të gjatë. Por le të jemi të sinqertë – sasia e çështjeve që përfshijnë provat elektronike po rritet me shpejtësi. Pra ka një boshllëk të madh ndërmjet përvojës dhe njohurive në lidhje me Kriminalistikën Dixhitale nga njëra anë, dhe rritjes së çështjeve që përfshijnë provat elektronike nga ana tjetër. Për shkak të këtij fakti, shumica e avokatëve, prokurorëve dhe gjyqtarëve duhet të familjarizohen me këtë shkencë të re. Ata duhet të dinë se çfarë janë provat elektronike dhe se si Kriminalistika Dixhitale mund të ndihmojë në zgjidhjen e çështjeve të tyre. Dhe kjo është ekzaktësisht se përse jemi këtu sot!  Le të shohim nëse mund të gjejmë ngjashmëri ndërmjet hetimit tradicional të gjurmëve dhe Kriminalistikës Dixhitale.  Shënim: Ky slajd është i animuar.  [klik] Në botën reale keni skenën e krimit që duhet të sigurohet – megjithëse nuk jam i sigurtë se ç’bëri kolegu në këtë foto ;)  Në botën e Kriminalistikës Dixhitale ju mund të keni gjithashtu të njëjtën skenë krimi. Pra, hetuesit duhet të sigurojnë skenën në të njëjtën mënyrë që do ta siguronin në kriminalistikën tradicionale. Por në botën e Kriminalistikës Dixhitale kemi gjithashtu edhe një skenë të dytë krimi [klik]. Për kryerjen e një vepre penale mund të jetë përdorur një sistem kompjuterik. Kjo e bën atë një provë të vlefshme për çështjen tonë. Por edhe sikur vetë kompjuteri të mos ishte përdorur për kryerjen e veprës, ai prapëseprapë mund të përmbajë të dhëna të rëndësishme në lidhje me të, fazën përgatitore të veprës, faqet e llogarisë së dokumentuar, lidhjet në Chat ndërmjet viktimës dhe të dyshuarit ose rrethana të tjera që kanë të bëjnë me veprën penale.  Shënim: Ky slajd është i animuar.  [klik] gjithmonë mbani të veshura dorezat kur të siguroni skenën e krimit – ky parim i vjetër i kriminalistikës tradicionale është i vërtetë edhe për Kriminalistikën Dixhitale. Ashtu siç nuk do të donit të linit shenjat e gishtërinjve tuaj ose ADN-në në armën e përdorur për kryerjen e krimit, po kështu nuk do të donit të linit gjurmët tuaja në një pjesë dixhitale të provave si p.sh në një disk të ngurtë. [klik]  Ky është momenti kur hyjnë në lojë write-blockers[[5]](#footnote-6). Ka lloje të ndryshme të write-blockers[[6]](#footnote-7). Disa prej tyre janë pjesë të vogla të programeve kompjuterike që përpiqen të ç’aktivizojnë funksionin e të shkruarit në një disk (programi kompjuterik “write-blockers”). Dhe disa prej tyre janë pjesë fizike që fizikisht bllokojnë sinjalin që është përgjegjës për dërgimin e komandave të shkrimit mbi një disk të ngurtë (pjesët write-blocker të pajisjeve). Në këtë figurë mund të shihni një bllokues shkrimi nga Kompania Tableau. Ka të tjerë nga kompanitë si Wiebetech ose MyKey Technologies. Të gjitha kanë të përbashkët këtë që janë disa porta që lidhin një disk të ngurtë fillestar (provë materiale) dhe disa porta të tjera që lidhin bllokuesin e shkrimit me pajisjen kriminalistike të hetuesit.  Shënim: ky slajd është i animuar.  [klik] Në kriminalistikën tradicionale, hetuesit në skenën e krimit mund të gjejnë dhe sigurojnë gjurmët e këmbëve, ADN dhe gjurmë të tjera si provat që mund të çojnë tek i dyshuari. Gjurmë shumë të ngjashme mund të gjenden edhe në burimet dixhitale: uebsajtet e vizituara nga i dyshuari, dokumentet e krijuara nga ai, fotot e hapura ose madje edhe gjurmët e një sulmuesi që ka hyrë në mënyrë të paautorizuar në një sistem. Si ADN-ja në kriminalistikën tradicionale, disa gjurmë dixhitale nuk janë të dukshme për tu parë dhe nevojiten teknika speciale për nxjerrjen e përmbajtjes provuese nga to. [klik] Shembuj të kësaj janë zona të papërdorura të disqeve. Nganjëherë ekzaminuesit kriminalistikë duhet të futen thellë në strukturën e diskut, sistemet e skedarëve, hapësirat e papërdorura në sistemet e skedarëve dhe strukturat e të dhënave pronësore për të gjetur provat që nevojiten për në procesin gjyqësor.  Shënim: ky slajd është i animuar  [klik] Këtu kemi një shembull tjetër të ngjashmërive ndërmjet shkencave kriminalistike tradicionale dhe Kriminalistikës Dixhitale. Kur hetuesit gjejnë gjurmë gishtërinjsh në mjetin që është përdorur për kryerjen e një krimi, ata kërkojnë në bazën e tyre të të dhënave për të gjetur të njëjtën gjurmë gishtërinjsh. Nëse kanë sukses, mund të thonë se gjurmët e gishtërinjve në mjet i përkasin një personi të caktuar në bazën e tyre të të dhënave. Në kriminalistikën dixhitale, ekziston një mënyrë e ngjashme për të krahasuar dhe gjetur një skedar të caktuar dhe për të provuar se skedari i kërkuar dhe skedari i gjetur përputhen ekzaktësisht. Ndoshta disa prej jush kanë dëgjuar për këto metoda. A ka ndonjë ide dikush këtu?...  [klik] Ndoshta tani? Hashing[[7]](#footnote-8) është termi që po kërkoja. Në një analizë hash, ekzaminuesi kriminalistik llogarit shumat hash të një skedari ose të një disku. MD5, SHA-1, SHA-256, etj., janë disa prej shembujve të zakonshëm për algoritmet kriptografike hash. Sapo të llogaritet vlera hash, e cila në fakt është një zinxhir i gjatë numrash dhe germash, ajo është unike për përmbajtjen e këtij skedari. Asnjë skedar tjetër nuk ka të njëjtën vlerë hash përveç saj dhe me ekzaktësisht të njëjtën përmbajtje. Kjo është arsyeja që ekzaminuesit mund të përdorin vlerat hash për kërkimin e skedarëve dhe për të verifikuar nëse përmbajtja e një kopjeje nga kriminalistika e një disku të ngurtë është e njëjta me përmbajtjen e skedarit të diskut të ngurtë origjinal.  Përsa i takon probabilitetit: Sa gjasa ka, mendoni ju, që dy njerëz të kenë të njëjtat gjurmë gishtash? … **1 në 64 Miliard**! [klik] Dhe sa gjasa ka, do të thoni ju, të fitosh klasën më të lartë në Lotarinë Euromilionëshe? … **1 në 116 milion!** Tani që i dini këto numra të lartë, sa mendoni se është probabiliteti për dy skedarë që të kenë të njëjtën vlerë hash? … Duke përdorur algoritmin MD5, probabiliteti që dy skedarë të kenë të njëjtën vlerë është [klik] **1 në më shumë se 340 Miliard Miliard Miliard Miliard** (2 në fuqi të 128), ndërsa probabiliteti me SHA-1 është mbi **një mijë Miliard Miliard Miliard Miliard** (2 në fuqi të 160). Megjithatë – sa për ta ditur – kërkuesit kanë arritur të prodhojnë përplasje të vlerave hash në kushtet e laboratorit.    Tani, që e pamë sesi është e ngjashme Kriminalistika Dixhitale me shkencat e tjera të kriminalistikës, do të shohim sesi përkufizohet dhe sesi funksionon.  Përkufizimi:  Shkencat kriminalistike është studimi i çdo fushe që lidhet me çështjet ligjore. Shkencat kriminalistike i referohen më specifikisht provave që përmbushin standardet e rrepta të besueshmërisë dhe integritetit shkencor për pranueshmërinë në gjykatë.  Kriminalistika Dixhitale është dega e shkencës kriminalistike që lidhet me marrjen, përpunimin, analizimin dhe raportimin e provave që ruhen në sistemet kompjuterike, pajisjet dixhitale dhe pajisjet e tjera me synimin e pranueshmërisë në gjykatë.    Ka tre kategori kryesore të Kriminalistikës Dixhitale.  Kriminalistika Kompjuterike është më e vjetra nga kategoritë. Ajo prek kompjuterët personalë, serverët dhe pajisjet e ruajtjes së të dhënave. Ka katër nënkategori të Kriminalistikës Kompjuterike. Ato janë:   * Kriminalistika Post Mortem, që ka të bëjë me marrjen, përpunimin, analizimin dhe raportimin e të dhënave të ruajtura në sistemet kompjuterike që nuk janë të ndezura/në funksionim. Kjo është kategoria më tradicionale e kriminalistikës. * Kriminalistika me kompjuter në funksionim/të ndezur, e cila ka të bëjë me marrjen, përpunimin, analizimin dhe raportimin e të dhënave të ruajtura në sistemet kompjuterike që janë në funksionim ose të ndezura. Krahasuar me Kriminalistikën Post Mortem, kjo është një nënkategori mjaft më e re por është duke u bërë gjithnjë e më shumë e rëndësishme sepse shumë të dhëna sot ruhen përkohësisht, larg prej kompjuterit ose kodohen. * Kriminalistika e aplikacioneve është nënkategoria që fokusohet tek analizimi i gjurmëve dhe produkteve të lëna nga mijëra aplikacione të ndryshme. * Kategoria e fundit është kriminalistika që lidhet me pajisjet fizike, të tilla si regjistruesit video, ruterat, pajiset e lojërave, pajisjet skimming të bankave dhe shumë të tjera. Shumë prej këtyre pajisjeve kanë sistemet e tyre vetjake dhe sistemet e operimit.   Tre kategoritë e para janë nënkategoritë për sistemet e ndryshme të operimit, si Windows, Linux, Mac OS X.  Kriminalistika e pajisjeve celulare është një kategori mjaft e re por po bëhet mjaft popullore, përderisa shumë të dhëna që mund të jenë interesante për një hetim mund të ruhen në pajisjet celulare si telefonat smart ose kompjuterët tablet. Nënkategoritë reflektojnë sistemet e ndryshme të operimit. Më popullorët për momentin janë sistemet Google Android dhe iOS nga Mac.  Kategoria e kriminalistikës së rrjeteve kompjuterike trajton provat elektronike që transmetohen nëpërmjet një rrjeti, ose pa kabull ose më kabull, ose në Internet ose në një rrjet lokal. Në kriminalistikën e rrjeteve në funksionim, hetuesit po përballen me situatën kur ata interceptojnë një lidhje në rrjet dhe iu nevojitet të analizojnë rrjedhën e të dhënave menjëherë sapo i interceptojnë. Ndërsa kriminalistika e paketave të kapura të të dhënave trajton analizimin e skedarëve që përmbajnë të regjistruar trafikun e rrjetit.  Shënim: ky slajd është i animuar.  Në një çështje që ka të bëjë me Kriminalistikën Dixhitale, procedura standarde zakonisht konsiston në katër hapa:  [klik] Mbledhja: Provat dixhitale duhet të mblidhen. Kjo mund të realizohet duke grumbulluar të dhëna të paqëndrueshme në një skenar kontrolli & sekuestrimi, duke marrë diskun e të dyshuarit nga një kompjuter i sekuestruar ose në ndonjë proces tjetër gjatë një rasti ku hetuesi duhet të marrë të dhënat nga burime të tjerat me instrumentet kriminalistike. Faza e mbledhjes është shumë e rëndësishme sepse mund të bëhen shumë gabime të pakthyeshme. Është e rëndësishme të mbahet zinxhiri i mbrojtjes së provave i paprekur, të dokumentohen hapat dhe të verifikohen gjithçka që u grumbullua.  [klik] Përpunimi: Hapi i përpunimit është i rëndësishëm sa herë që koha, efektiviteti dhe volume të mëdha të dhënash janë në lojë. Në këtë hap ekzaminuesit kriminalistikë mund të vendosin prioritete për disa lloj pajisjesh ose të dhënash, ata mund të përdorin filtra inteligjent, specifik për çështjen (Data Mining[[8]](#footnote-9)) ose ata thjesht mund të përpunojnë imazhin në një mënyrë që një hetues i zakonshëm të mund ta analizojë atë (p.sh. duke rikuperuar skedarë të fshirë, duke i bërë aksesueshëm mbajtësit e skedarëve, deshifrimin e kodimit, analizimin e të dhënave të programeve si historia e navigimit në Internet, regjistrimet e bisedave në Chat, etj).  [klik] Analiza: Gjatë analizës ekzaminuesi në fakt kërkon për prova dixhitale tek imazhet. Ky hap mund të konsumojë shumë kohë dhe mund të kërkojë shumë ekspertizë për interpretimin e gjurmëve dhe produkteve.  [klik] Prezantimi: Mbas gjetjes së të gjitha provave në hapin e analizës, ekzaminuesi duhet të hartojë një raport për procesin gjyqësor. Puna e tij është të ilustrojë dhe të përkthejë kontekste të vështira teknike për ju si gjyqtarë dhe prokurorë në një mënyrë që ju lehtësisht të kuptoni çfarë provash janë gjetur, ku u gjetën, si u gjetën dhe si mund të kenë përfunduar aty ku u gjetën.    Tani le të shohim disa prej gjurmëve dhe sesi kriminalistika dixhitale mund t’ju ndihmojë – e cila është dhe arsyeja se pse jeni ulur këtu në këtë sesion ;)  Ekzistojnë dy lloj gjurmësh dixhitale:  Gjurmë të evitueshme: këto janë gjurmë që memorizohen nga sistemi i operimit automatikisht por sistemi mund të konfigurohet që të mos t’i memorizojë ato. Për shembull le të marrim programin e navigimit në Internet. Ju shtypni adresën e uebsajtit tuaj të preferuar. Pastaj një ditë më pas dëshironi ta vizitoni përsëri këtë uebsajt dhe filloni ta shtypni përsëri adresën kur papritur programi juaj navigues e përfundon vetë shkrimin e adresës së uebsajtit. Pra duhet të ketë një vend në diskun e ngurtë ku ruhet ekzaktësisht ky informacion. Një shembull tjetër janë programet e menysë Start dhe programet Office; ato mbajnë mend se cilat skedarë janë hapur së fundmi. Ka shumë informacion si ky i memorizuar në diskun e ngurtë. Disa prej këtij informacioni përmendet në këtë slajd. Megjithatë, ju mund të kërkoni në sistemin tuaj dhe konfigurimet e programit dhe ta ndryshoni këtë sjellje. Në mënyrë që t’i evitoni këto gjurmë.  Gjurmë të paevitueshme: në kontrast me gjurmët e evitueshme, gjurmët e paevitueshme nuk mund të konfigurohen që të ndalojnë së funksionuari. Pra, mundësia për të gjetur prova të ruajtura në mënyrë të paqëllimtë në këto zona është mjaft e lartë edhe sikur i dyshuari të përpiqet të pastrojë gjurmët. Do t’ju shpjegoj për pak minuta termat “Slack dhe Unallocated Space[[9]](#footnote-10)” por fatkeqësisht nuk mund t’i trajtojmë në detaje në këtë fazë.  Le të shohim sesi Kriminalistika Dixhitale mund t’ju ndihmojë me këto gjurmë.  Mund t’ju bëj një pyetje? Kush nga ju po navigon në Internet? … Ok, dhe kush nga ju përdor programet shfletues të treguar në këtë slajd? … Wow, ok, pra besoj se të gjithë e dini se programet e navigimit në Internet ruajnë historinë e navigimit, një memorizim të përkohshëm të uebsajteve që keni vizituar dhe informacion regjistrues si dhe vlerat që keni shkruar në fusha formati si p.sh. kërkimi në google dhe informacioni për uebsajtet dhe shkarkimet e juaja të preferuara?  Nëse po, ky slajd do t’ju tregojë diçka të re: tek të gjitha uebsajtet që viziton një i dyshuar, ai plotëson të dhëna dhe ndërvepron dhe kështu që le gjurmë. Disa prej programeve shfletuese mund të konfigurohen që të mos e ruajnë këtë informacion por jo të gjithë programet e mbajnë fjalën në fakt. Nganjëherë historia që nuk duhet të regjistrohet, në fakt regjistrohet por vetëm që programi nuk e tregon se po regjistrohet.  Kështu, Historia e Internetit shpesh është një vend i mirë për të gjetur informacion – aq më shumë në kohëra kur gati të gjithë navigojnë rrjetin dhe shumë krime kryhen në Internet. Nëse shohim disa adresa këtu, mund të shikojmë disa shembuj të URL-ve që duhet ta bëjnë një ekzaminues të paktën kureshtar. Me sa e njoh unë juridiksionin tonë në Gjermani, mund të ketë një ndikim shumë të madh në procesin gjyqësor nëse mund të provohet se i dyshuari qëllimisht kërkoi dhe planifikoi krimin e tij përpara se ta kryente atë. Po në juridiksionin tuaj?...  Më poshtë janë disa shembuj të llojeve të të dhënave që dalin nga ekzaminimi i Kriminalistikës Dixhitale:  **Të dhëna specifike për përdoruesin**  Programet e përdorura, Uebsajtet e vizituara, Kontrollet e kryera, Skedarët e hapur/të ruajtur  **Të dhënat Exif**  Kur dhe ku është bërë një foto me një model të caktuar aparati fotografik, numri serial  **Të dhënat e aplikacioneve të ndryshme**  Programet e Postës Elektronike, historia e chat-it, bazat e të dhënave, konfigurimet, analiza e programeve të dëmshme  **Fragmentet**  Fragmente të fotove si prova, dokumentet, historitë, skedarët e regjistrimit të të dhënave, …  **Dokumentet provues**  Deklaratat e llogarive, letrat kërcënuese, fotot e paligjshme, kontaktet, skedarët e regjistrimit të të dhënave, planimetritë e vjedhura,…  **Të dhënat e paaksesueshme**  Skedarët e fshehur, skedarët e koduar, të dhënat e fshira, skedarë të steganizuar, ruajtja e të dhënave në rrjet/në re  Keni parë disa shembuj të të dhënave që rezultojnë nga Kriminalistika Dixhitale. Përpara se të mbarojmë sesionin tonë, dëshiroj t’ju njoh me tre tema të vogla që tingëllojnë shumë të komplikuara por në fakt nuk janë shumë të vështira për tu kuptuar. Synimi ynë është që herën tjetër që do të dëgjoni ose lexoni për „Steganografinë“, „Rikuperimin e të dhënave të fshira“ ose „Fragmente të gjetura në Hapësirën e Papërdorur të Sistemit të Skedarëve“, ju të thoni: „Oh po, e kuptoj, nuk është shumë e komplikuar.“  Shënim: Ky slajd është i animuar.  A ka përdorur ndonjë prej jush bojë magjike kur keni qenë fëmijë? Koncepti është se ju mund ta fshihni tekstin duke e shkruar me lëngun e limonit. Megjithëse i gjithë teksti juaj është i shkruar në letër të pakoduar, ai nuk mund të shihet nga dikush që nuk e di se ka një mesazh në letër të shkruar me këtë bojë magjike. Personi, të cilit i dërgoni këtë letër e di si ta bëjë të dukshme mesazhin e fshehur. Ata nga ju që e dinë këtë teknikë: a e dini si ta bëni të dukshme bojën? [klik] duke e nxehur me kujdes letrën me një qiri ose një çakmak.  Shënim: Ky slajd është i animuar  Ok, siç thashë tema e parë është në lidhje me fshirjen e të dhënave dhe rikuperimin e tyre.  Fshirja e një skedari është e lehtë, thjesht shtypni tastin „Del“ në tastierë ose zgjidhni komandën „delete“ në menunë e kontekstit. A e di ndonjë se çfarë ndodh në këtë rast?...  [klik] Skedari „fshihet“ duke u dërguar në Kosh. Nuk do ju tregoj histori të gjata, por fakti është se: ky skedar zhvendoset në një direktori tjetër që quhet „Recycle Bin“[[10]](#footnote-11). Nuk kemi të bëjmë me fshirje të mirëfilltë por thjesht me zhvendosje; e njëjta gjë sikur të zhvendosnit skedarin A nga Folderi B tek Folderi C.  A dini ndonjë alternativë tjetër të fshirjes së skedarit në koshin e plehrave?  [klik] Duke mbajtur të shtypur tastin “shift”, ndërkohë duke shtypur tastin “delete”, ju mund ta “fshini përgjithmonë“ një skedar. Më vjen keq t’jua them por edhe kjo nuk e fshin skedarin. Në fakt diçka tjetër ndodh. Ta shohim.  Shënim: Ky slajd është i animuar.  Imagjinoni sistemin e skedarëve sikur të jetë një libër. Ai ndjek aktivitetin e të gjithë skedarëve të tij si në Tabelën e Përmbajtjes, njësoj si renditja e të gjithë kapitujve në fillim të një libri. Këtu shihni sesi duket një tabelë e përmbajtjes, pak e thjeshtëzuar por pak a shumë ajo është. Keni të gjithë emrat e skedarëve (kapitujt), më pas keni faqen në libër ku mund të gjeni një kapitull; një faqe në libër do të ishte një cluster[[11]](#footnote-12) në diskun tuaj të ngurtë; kështu në shembullin tonë ju mund të gjeni skedarin Picture.jpg në Cluster [klik]. Ju mund të gjeni gjithashtu një vlerë sesa faqe është i gjatë ky kapitull, kështu skedari ynë picture.jpg do të ishte 32 clusters në madhësi. Pastaj kemi një vlerë shumë të rëndësishme që pothuaj e kaluam pa e parë, vlerën e caktuar. Një vlerë 01 do të thotë për sistemin e skedarëve: Ky skedar është ok, mos prek. Një vlerë 00 [klik] do të thotë: Ky skedar është i shënuar si i fshirë, herën tjetër që një skedar i ri do të krijohet sistemi i skedarëve mund ta përdorë këtë hyrje në tabelën e përmbajtjes. Kjo është ajo që ndodh sikur ju të bëni komandën Shift-delete për një skedar.  Çfarë bën ekzaminuesi kriminalistik tani? Ai thjesht injoron Statusin e Alokimit dhe thotë: Çdo skedar që shoh në tabelën e përmbajtjes ekziston vërtet për mua. Ne tashmë dimë dy mënyra sesi të rikuperojmë skedarët e fshirë [klik] -> Copy out of Recycle Bin[[12]](#footnote-13) dhe -> Ignore Allocation Status  Mënyra e tretë quhet „Carving“[[13]](#footnote-14). Jo shumë e vështirë. Mënyra “Carving” mund të realizohet kur ripërdoret vendi i një skedari në tabelën e përmbajtjes. Në këtë rast vetëm informacioni në tabelën e përmbajtjes u mbishkrua por të gjitha të dhënat janë akoma në diskun e ngurtë. E njëjta gjë si me një libër. Nëse hiqni vetëm kapitullin A nga tabela e përmbajtjes atëherë të gjitha faqet me tekstin e kapitullit janë akoma në të njëjtin vend në libër. Pra e vetmja gjë për të bërë është merrni librin dhe shikoni në çdo faqe nëse mund të gjeni kokën e kapitullit. Mjetet e mënyrës “Carving” bëjnë të njëjtën gjë; ato kontrollojnë çdo cluster të papërdorur nëse ka një Kokë (të quajtur gjithashtu nënshkrim) p.sh. të një fotoje në formatin .jpeg. Në këtë mënyrë mjetet e “carving” mund të rikuperojnë skedarët edhe sikur të jetë fshirë referenca në Tabelën e Përmbajtjes.  Më e komplikuar se leximi i një libri? Ok, atëherë kalojmë në temën e fundit.  Slacks[[14]](#footnote-15). Hapësirat e papërdorura/të lira janë interesante për ekzaminuesit kriminalistikë sepse përdoruesi nuk ka asnjë influencë se çfarë ruhet në to. Shpesh, janë të dhëna të vjetra që memorizohen në disk përkohësisht ose që u morën nga memoria RAM. Pra, të shohim se çfarë është në fakt hapësira “Slack”.  Mendoni një skedar që është ruajtur në sistemin e skedarëve. Ndoshta një dokument teksti si ky. Ky skedar zë një vend në diskun e ngurtë, le të themi 8 sektorë si ky që shikoni në slajd. Tani imagjinoni që ky dokument teksti fshihet. Siç kemi mësuar nga slajdi i mëparshëm, fshihet vetëm regjistrimi tek Tabela e Përmbajtjes – jo vetë përmbajtja. POR – herët ose vonë sektorët me atë përmbajtje nevojiten përsëri për ruajtjen e të dhënave të tjera. Në rastin tonë një skedar i një fotoje do të ruhet në këto sektorë.  Kur kjo foto e re ruhet, sistemi i skedarëve mund ta memorizojë atë në njësi ruajtjeje që quajtura “clusters”. Një cluster konsiston në disa sektorë. Në shumicën e rasteve, një skedar nuk e mbush të gjithë grupin e sektorëve deri në fund, si në foto [klik]. Fotoja zë 4 sektorë dhe një pjesë të vogël të sektorit të pestë. Por sistemi i skedarëve DUHET t’i caktojë të gjithë grupin e sektorëve kësaj fotoje. Këtu futet në lojë Hapësira e Papërdorur[[15]](#footnote-16) ose e lirë.  Pjesa tjetër e grupit të sektorëve është akoma e alokuar për skedarin por nuk ka ndonjë përmbajtje që i takon skedarit: Kjo quhet File Slack[[16]](#footnote-17).  Hapësira e papërdorur nga skedari përbëhet nga dy hapësira të tjera të papërdorura. E para quhet sektor- ose hapësira e papërdorur RAM. [klik] Kjo hapësirë e papërdorur zë vetëm zonën nga fundi i përmbajtjes së një skedari deri në fund të sektorit. Në kohë të mëparshme kjo hapësirë e lirë përbëhej nga të dhëna kuturu të marra nga memoria RAM, ja përse është emri hapësira e papërdorur RAM. Në ditët e sotme vetëm zerot janë të shkruara – interesante për kriminalistikën? Në fakt jo.  Pjesa tjetër, the Cluster- ose Hapësira e Papërdorur [klik] është shumë më interesante – siç mund ta shihni në foto. Kjo hapësirë fillon direkt mbas hapësirës së sektorit dhe shkon deri në fund të grupit të sektorëve. Përbëhet nga të dhëna të vjetra nga skedarët e fshirë që ruheshin më parë në këtë sektor, ndoshta një pjesë e një letre për provë, ndoshta një pjesë provuese e një skedari të vjetër nga historia e navigimit në Internet?  Mos lejoni që kjo foto t’ju ngatërrojë: mund të ketë shumë më tepër informacion në Hapësirën e Papërdorur sesa në këto dy fjalë. Një sektor është 512 Bytes në madhësi, që do të thotë se ai mund të mbajë deri në 512 karaktere, pra në shembullin tonë në Hapësirën e Papërdorur të Grupit të Sektorëve mund të ruhet një letër me 1536 karaktere, që janë 10 mesazhe SMS.  Ok, le të shohim se çfarë mësuam në këtë sesion | |
|  | **Ushtrime Praktike (nëse ka)** Nuk ka asnjë ushtrim praktik në këtë sesion; megjithatë ka demonstrime nga trajneri. | |
|  | **Kontrolli i Njohurive**  Për këtë kurs nuk është parashikuar asnjë kontroll specifik i njohurive krahas atyre të renditur më lart. Nuk është kërkuar asnjë vlerësim zyrtar. | |

|  |  |  |
| --- | --- | --- |
| Mësimi: 1.2.2–Prezantim – Kriminalistika Dixhitale – Pjesa 2 | | **Kohëzgjatja: 60 Minuta** |
| **Burimet materiale të kërkuara:**   * Kompjuter Laptop ose Kompjuter Tavoline me sistem Windows 7 dhe me Office 2010 * Projektor * Makinë Virtuale e përgatitur specifikisht për këtë kurs dhe e përfshirë në paketën e burimeve materiale | | |
| **Synimi:** Synimi i këtij sesioni është rritja e ndërgjegjësimit të pjesëmarrësve në lidhje me shkencën e kriminalistikës dixhitale dhe vlerën e saj në hetimet penale. Kursi gjithashtu jep informacion në lidhje me provat e gjetura në lidhje me skenarin. | | |
| **Objektivat:**  Në përfundim të këtij sesioni pjesëmarrësit do të jenë në gjendje të:   * Shpjegojnë termin Kriminalistika Dixhitale * Krahasojnë Kriminalistikën Dixhitale me shkencat e kriminalistikës tradicionale * Përcaktojnë të paktën tre nën-degë të Kriminalistikës Dixhitale * Identifikojnë katër hapa në ekzaminimet e Kriminalistikës Dixhitale * Diferencojnë dy kategoritë e gjurmëve dixhitale * Përshkruajnë se si Kriminalistika Dixhitale mund të mbështesë hetimet * Përshkruajnë sesi funksionon Steganografia * Krahasojnë tre metoda sesi të rikuperojnë skedarët e fshirë * Karakterizojnë llojet e ndryshme të Hapësirës së Papërdorur * Zbatojnë teorinë e Kriminalistikës Dixhitale në një skenar praktik * Identifikojnë përfitimet e ekzaminimit të Kriminalistikës Dixhitale * Përshkruajnë sesi Virtualizimi mund të ndihmojë Kriminalistikën Dixhitale | | |
| **Nr. i Slajdit** | **Përmbajtja:** | |
| **Slajd 1** | Hyrje për trajnerët:  Mbas kontrollit të ambienteve të të dyshuarit, kompjuteri i tij u sekuestrua dhe është gati për analizën kriminalistike. Në këtë sesion ju si trajner mund të demonstroni se u gjetën provat dixhitale gjatë hetimit. Keni zgjedhjen ose të demonstroni “direkt” se çfarë provash u gjetën në kompjuterin e të dyshuarit ose mund të përdorni slajdet ku jepen pamje të provave të gjetura. Pjesa e parë e këtij prezantimi tregon provat nga këndvështrimi i analizës kriminalistike me kompjuter të fikur, ndërsa pjesa e dytë tregon provat nga “këndvështrimi i të dyshuarit” brenda një makine virtuale.  Nëse vendosni të paraqitni provat me ndihmën e slajdeve, të gjitha ato që do ju nevojiten janë përfshin në prezantim. Nëse jeni me përvojë në ekzaminimet e kriminalistikës dixhitale dhe preferoni të bëni një demonstrim direkt, keni nevojë për të mëposhtmet:   * Një vend pune me instrumentet e kriminalistikës të instaluara (preferueshmërisht instrumentet të cilat i përdor me lehtësi). * Programi VirtualBox si program virtualizimi.   Provat në ekzaminimin me kompjuter të fikur:  Për të treguar provat me programin tuaj kriminalistik, vendoseni imazhin e kompjuterit të të dyshuarit në programin tuaj. Mund të përdorni skedarin .vdi, nëse programi juaj e lejon hedhjen në të të imazheve Virtual Box. Mbas hapjes së imazhit, mund ta prezantoni instrumentin kriminalistik tek audienca, duke shpjeguar se çfarë mund të shohin pjesëmarrësit në ekran (p.sh. struktura e direktorisë së diskut të të dyshuarit, imazhi i programit editor hex, imazhi i galerisë, etj).  Nëse instrumenti juaj kriminalistik iu ofron mundësinë për të treguar në mënyrë rekursive të gjitha imazhet në një galeri, ju mund të tregoni të gjitha fotot e direktorisë së përdoruesit „Ralf“ (C:\Users\Ralph\) dhe nëndirektoritë. Do të shihni foton e një makine Mercedes Benz në folderin „C:\Users\Ralph\Documents\humor\“ si dhe në folderin „C:\Users\Ralph\Downloads\“  Në historinë e Internetit të programit shfletues Firefox, ju mund të dalloni gjurmë nga historia e përdoruesit të vizitave në uebsajte të ndryshme. Skedarët ruhen në formën e databazave sqlite dhe mund të shihen ose me programin tuaj kriminalistik ose me një program sqlite (p.sh. Programi SQLite Manager për Programin Shfletues Firefox). Në skedarin „C:\Users\Ralph\AppData\Roaming\Mozilla\Firefox\Profiles\fgu58ymm.default\formhistory.sqlite“, do të gjeni gjurmë për llogarinë e përdoruesit në uebsajtin hushmail me emër „00007@hushmail.com“, si dhe frazat e shkruara për kërkim „how to ddos“[[17]](#footnote-18), „steganography“[[18]](#footnote-19) dhe „tor browser“[[19]](#footnote-20). Në skedarin „C:\Users\Ralph\AppData\Roaming\Mozilla\Firefox\Profiles\fgu58ymm.default\places.sqlite“, ju mund të gjeni uebsajtet e vizituara nga hushmail.com.  Një program tjetër shfletues i Internetit, Programi TOR, është përdorur për të aksesuar llogarinë safe-mail.net. Është shumë e nevojshme të tregohen mesazhet elektronike nga llogaria safe-mail.net duke hyrë konkretisht në llogari me anë të makinës virtuale, sepse programi shfletues nuk regjistron të dhëna provuese.  Makina Virtuale:  Për të filluar makinën virtuale thjesht klikoni dy herë skedarin „CoE-IPA-Advanced.vbox“. Sigurohuni që programi VirtualBox është i instaluar në sistemin tuaj. Fjalëkalimi për llogarinë e përdoruesit Ralf është „secret“. Ky fjalëkalim mund të merret duke përdorur skedarët SAM dhe SYSTEM të nxjerrë nga imazhi në „C:\Windows\system\“ me programin kompjuterik Ophcrack „http://ophcrack.sourceforge.net/“.  Në makinën virtuale, desktop-i i përdoruesit duke përfshirë ikonat për programet OpenStego dhe shfletuesin TOR mund të mbyllen. Programi shfletues TOR mund të përdoret për të aksesuar llogarinë safe-mail.net. Emri i përdoruesit për këtë llogari është 00007security@hushmail.com, fjalëkalimi është „secret“. Mund të përmendni se shpesh përdoruesit priren të përdorin të njëjtin fjalëkalim për qëllime të ndryshme. Mund të tregohen mesazhet elektronike që ruhen në serverë (gjithashtu të disponueshëm në paketën e trajnimit).  Në makinën virtuale, mund të demonstrohet përdorimi nga të dyshuarit i programit OpenStego për të treguar sesi i dyshuari e ç’kodoi foton që viktima kishte vendosur në uebsajtin me reklama. Filloni programin nga ikona në Desktop dhe zgjidhni tabin „Extract“. Fotoja e steganizuar/fshehur mund të gjendet në „C:\Users\Ralph\Downloads\192790683.png“. Ju mund ta përcaktoni folderin e produktit skedarin e mesazhit si të dëshironi. Fjalëkalimi për nxjerrjen e skedarit me tekstin e kartës së kreditit është ai që përmendet në mesazhin elektronik për viktimën. | |
|  | **Ushtrime Praktike (nëse ka)**  Nuk ka asnjë ushtrim praktik në këtë sesion. | |
|  | **Kontrolli i Njohurive**  Për këtë kurs nuk është parashikuar asnjë kontroll specifik njohurish krahas atij të renditur më lart. Nuk është kërkuar asnjë vlerësim zyrtar. | |

|  |  |  |
| --- | --- | --- |
| Mësimi: 1.2.3–Puna në Grup – Kriminalistika Dixhitale | | **Kohëzgjatja: 90 Minuta** |
| **Burimet materiale të kërkuara:**   * Një sallë e përshtatshme për një numër të parashikuar pjesëmarrësish. Kjo sallë duhet të rregullohet duke vendosur një tryezë të rrumbullakët për çdo grup, ku është e mundur, bazuar në një numër prej 6 pjesëmarrësish në grup. * Kompjuter tavoline/laptop me Windows 7 ose 8 dhe me Programin MS Office Professional të instaluar * Projektor dhe ekran për shfaqje imazhesh * Akses në Internet (nëse është i disponueshëm) * Kopje të Guidës për Provat Elektronike të Këshillit të Evropës * Dërrasë të Bardhë për secilin grup * Markera për Dërrasë të Bardhë (të paktën 2 për secilën ngjyrë: blu, të zezë, të kuqe dhe jeshile) për secilin grup * 1 Tabelë Flipchart me letër të mjaftueshme për secilin grup * Stilolapsa dhe blloqe për pjesëmarrësit * Kapëse aktesh, vrimahapëse dhe gërshërë për secilin grup * Ngjitës Blu ose një produkt të ngjashëm me të për ngjitjen e përkohshme të letrës në mure për secilin grup * Një kompjuter laptop për secilin grup të ngjashëm me kompjuterin e trajnerit dhe me akses në Internet që të realizohen kërkimet hetimore. * Të gjitha materialet mbështetëse të dhëna me paketën e trajnimit. | | |
| **Synim:** Ky sesion është për t’i lejuar pjesëmarrësve të konsiderojnë implikimet e provave dixhitale në kontekst të asaj çfarë është gjetur në kompjuterin e të dyshuarit. Ata do të konsiderojnë gjithashtu se çfarë provash të tjera nevojiten. | | |
| **Objektivat:**  **Në përfundim të këtij sesioni, pjesëmarrësit do të jenë në gjendje të:**   * Identifikojnë provat që kërkohen të nxirren nga kompjuteri i të dyshuarit * Përcaktojnë se çfarë ekzaminimesh të tjera kërkohen për mbështetjen e këtyre provave * Marrin në konsideratë fajësinë kriminale të të tjerëve të përfshirë në këtë skenar | | |
| **Nr. i Slajdit** | **Përmbajtja:** | |
|  | Ky sesion është tërësisht praktik dhe nuk përmban ndonjë prezantim. | |
|  | **Ushtrime Praktike (nëse ka)**  Skedarët e mëposhtëm janë shkëmbimet e mesazheve elektronike ndërmjet keqbërësit dhe korrierëve. Këto janë gjetur në kompjuterin e të dyshuarit mbas arrestimit. Ato duhet t’ju jepen pjesëmarrësve për t’i lejuar të vazhdojnë hetimin dhe për të marrë në konsideratë fajësinë e korrierëve si dhe sasinë e provave që do t’ju duhen nga jashtë shtetit.  Ky skedar ka mesazhet elektronike nga kompjuteri i të dyshuarit pa koka dhe duhet të jepet që në fillim:  File name - mule-tracking-emails.docx  Ky skedar ka kokat e mesazheve elektronike në skedarin e mëparshëm dhe duhet të jepen kur të kërkohet nga pjesëmarrësit:  File name - mule-tracking-emails-headers.docx  Skedari i mëposhtëm përmban detajet e emrave të korrierëve të tjerë të cilëve i dyshuari iu dërgoi kërkesë për ndihmë. Këta korrierë nuk u angazhuan në aktivitet kriminal por megjithatë mund të jenë dëshmitarë. Detajet personale në skedar mund të përdoren për krijimin e llogarive të postës elektronike dhe për të përdorur ato që u krijuan për skenarin.  File name - 2012-08-20 - Spare Mules.pdf | |
|  | **Kontrolli i Njohurive**  Për këtë kurs nuk është parashikuar asnjë kontroll specifik njohurish krahas atij të renditur më lart. Nuk është kërkuar asnjë vlerësim zyrtar. | |

|  |  |  |
| --- | --- | --- |
| Mësimi: 1.2.4–Prezantim – Përgatitja e Çështjes për Gjykatë | | **Kohëzgjatja: 45 Minuta** |
| **Burimet materiale të kërkuara:**   * Kompjuter Laptop ose Kompjuter Tavoline me sistemin Windows 7 dhe me Office 2010 * Projektor * Prezantim me PowerPoint | | |
| **Synimi:** Ky sesion synon të pajisë pjesëmarrësit me informacion të mjaftueshëm për t’i lejuar atyre të marrin vendime në lidhje me sesi do të përgatitet çështja dhe do të paraqitet në Gjykatë, duke shqyrtuar të gjitha alternativat dhe çështjet që mund lidhen me vetë gjykatën. | | |
| **Objektivat:**  Në përfundim të këtij sesioni pjesëmarrësit do të jenë në gjendje të:   * Menaxhojnë ndjekjen ligjore * Mbledhin prova nga jashtë shtetit nëpërmjet Ndihmë së Ndërsjellë Juridike * Sigurohen se nuk ka asnjë pengesë procedurale ose ligjore për kërkesat për prova * Kontaktojnë dëshmitarët në juridiksionet e tjera gjatë procedimit gjyqësor * Plotësojnë me saktësi dhe azhurnojnë të gjithë dokumentacionin dhe procedurat përkatëse * Garantojnë se janë përgatitur dosjet e përshtatshme dhe dokumentet mbështetës në formën e kërkuar brenda afateve përkatëse * Informojnë mbrojtjen për provat (nëse nevojitet) * Trajtojnë pranueshmërinë e provave elektronike dhe provave të tjera * Garantojnë pajtueshmërinë me KEDNJ dhe dispozitat e tjera * Njohin rolin dhe pritshmëritë e ekspertëve dëshmitarë * Dokumentojnë plotësisht vendimet, veprimet, alternativat dhe arsyetimin në përputhje me legjislacionin dhe politikat aktuale * Identifikojnë metodat e paraqitjes së provave elektronike në procedimin gjyqësor | | |
| **Nr. i Slajdit** | **Përmbajtja:** | |
| **Slajdi 4**  **Slajdi 6**  **Slajdi 8**  **Slajdi 9**  **Slajdi 11**  **Slajdi 12**  **Slajdi 13**  **Slajdi 14**  **Slajdi 15**  **Slajdi 16**  **Slajdi 17**  **Slajdi 18**  **Slajdi 19**  **Slajdi 20**  **Slajdi 21** | **Qasja inkuizitore dhe adversare**  Shumica e vendeve kontinentale Evropiane kanë një procedurë penale inkuizitore, që do të thotë se në qendër të kërkimit për të vërtetën është faza hetimore.  Provat dixhitale, si dhe provat e tjera, duhet të mblidhen dhe analizohen përpara se të shkojnë në gjykatë. Të gjithë dëshmitarët përkatës duhet të dëgjohen gjatë hetimit.  Ekspertët duhet të dorëzojnë raportet e tyre përpara se të shkojnë në gjykatë. Në një sistem ligjor inkuizitor, hetimi zakonisht drejtohet nga një gjyqtar hetues dhe/ose prokurori, dhe ekzekutohet nga policia. Gjyqtari hetues dhe/ose prokurori kanë përgjegjësi të plotë për cilësinë, besnikërinë dhe ligjshmërinë e hetimit, dhe janë të detyruar të kërkojnë prova për akuzën *dhe* për mbrojtjen.  Që nga momenti që prokurori vendos të sjellë çështjen në gjykatë me thirrjen për gjyq, thirrjen e dëshmitarëve dhe/ose aktakuzën, të gjitha provat duhet të jenë të disponueshme për të akuzuarin që ai/ajo të përgatisë mbrojtjen e tij me avokatët. Zakonisht në këtë pikë, hetimi konsiderohet i përfunduar, pa paragjykim për të drejtën e mbrojtjes që të bindë gjyqtarin për të kundërtën. Në procesin gjyqësor gjyqtari luan rolin qendror në gjetjen e të vërtetës dhe shqyrtimin e të gjitha provave (që janë mbledhur gjatë hetimit) që ose provojnë pafajësinë ose fajësinë e të akuzuarit përpara gjykatës. Nëse disa deklarata të dëshmitarëve kundërshtohen, dëshmitarët mund të thirren në gjyq. Është gjyqtari ai që i merr në pyetje dëshmitarët dhe madje mund t’i kërkojë prokurorit të thërrasë dëshmitarë për paraqitje, ndërkohë që akuza dhe mbrojtja mund të bëjnë pyetje pasuese.  Në shumicën e vendeve kontinentale Evropiane, nuk është procedurë standarde thirrja e dëshmitarëve dhe ekspertëve dëshmitarë në çdo gjykim.  Në një sistem ligjor inkuizitor, rregullat e pranueshmërisë së provave mund ta lejojnë gjithashtu gjyqtarin të veprojë më tepër si një hetues sesa si një arbitër i drejtësisë.  Sistemi i drejtësisë në vendet e sistemit common law bazohet në modelin adversar. Sistemi adversar nënkupton që dy palë janë në pozita të kundërta në debatimin e fajësisë ose pafajësisë së një individi. Në këtë skenar, gjyqtarit i kërkohet të jetë neutral në gjyqësinë që zhvillohet përpara tij/saj. Roli i gjyqtarit në këtë proces është të garantojë që gjyqi të procedojë në përputhje me rregullat procedurale të gjykimit ose procesit të drejtë gjyqësor dhe që provat e paraqitura të jenë në përputhje me udhëzimet dhe rregullat e miratuara.  Baza e kësaj qasjeje në çështjet penale, janë dy palë që debatojnë dhe luftojnë për fajësinë ose pafajësinë e një të akuzuari dhe meqë secila palë dëshiron të fitojë atëherë debati do të paraqesë një vështrim kritik mbi çështjet dhe paraqitjen e provave që do të shqyrtohen nga të dy palët. Duke u angazhuar në debat, e vërteta duhet të shfaqet ndërsa gjyqtari mbikëqyr procedurën. Kjo do të thotë se rolet e luajtura nga punonjësit e ndryshëm të gjykatës janë shumë të dallueshme. Avokati mbrojtës si një nga palët kundërshtare mbledh argumentet për të mbrojtur klientin e tij dhe sulmon kredibilitetin dhe vlerën e provave të paraqitura nga prokurori. Prokurori parashtron argumentet në emër të shtetit dhe mbledh dhe paraqet provat që demonstrojnë se i akuzuari e ka kryer veprën penale. Gjyqtari është arbitri në çështjet që lidhen me sqarimin se cili është ligji. Gjyqtari nuk ndërhyn për ndonjë palë përveçse kur vihet në rrezik drejtësia procedurale nga secila palë.  Provat dhe dëshmitarët që thirren i lihen dy palëve argumentuese, avokatit mbrojtës dhe prokurorit. Gjyqtari nuk përfshihet në atë çka i paraqitet gjykatës. Nëse prokurori dëshiron të mos paraqesë disa prova apo të mos thërrasë ndonjë dëshmitar edhe pse mund të hedhë dritë mbi çështjen, gjyqtari nuk mund të ndërhyjë. Kjo i lë palët në drejtim të çështjes dhe drejtimit që merr ajo.  Avantazhet e sistemit adversar përfshijnë:   * Gjyqtari i rezervon komentet derisa të jepen të gjitha provat nga të dy palët; * Kjo bën që gjyqtari të duket më neutral përderisa vendimi gjyqësor duhet të rezervohet derisa të paraqiten të gjitha provat.   Disavantazhet e sistemit adversar përfshijnë:   * Gjetja e provave mbetet tek të dy palët burimet e të cilave mund të mos jenë të barabarta; * Palët japin prova që janë të favorshme vetëm për argumentet e tyre.   Pra, në vendet e sistemit common law, kur shkohet në gjykatë, duhet të merren parasysh angazhime specifike:   * Thërret dëshmitarë nga juridiksione të tjera gjatë procedimit; * Thërret ekspertë si dëshmitarë; * Plotëson me saktësi dhe azhurnon dokumentacionin përkatës dhe procedurat; * Garanton që të jenë përgatitur dosjet e përshtatshme dhe dokumentet mbështetës dhe i paraqet ato në formën e kërkuar brenda afateve përkatëse; * Informon mbrojtjen për provat; * Merr në konsideratë se gjykimi do të jetë me juri;   Siç e thamë në shumicën e sistemeve ligjore kontinentale, shumica e këtyre aspekteve ndodhen në fazën e hetimit.  **Menaxhimi i ndjekjes ligjore**  Shihni kapitullin 9.2.2. të Guidës për Provat Elektronike të Këshillit të Evropës.  E drejta për një gjykim të drejtë e të paanshëm është e shenjtë, dhe përgjegjësia e grupeve hetimore në mbledhjen, ruajtjen dhe paraqitjen e provave elektronike në gjykatë mbetet më e larta. Secili anëtar i grupit hetimor ka një rol qartësisht të identifikuar për të luajtur. Duhet të ketë takime të përbashkëta të rregullta nga prokuroria dhe policia dhe personeli tjetër përkatës në lidhje me çështjen gjatë gjithë kohëzgjatjes së procedimit gjyqësor. Pas akuzimit, duhet të ketë sesione zyrtare informimi me të gjithë pjesëmarrësit që të identifikohen dhe përhapen mësimet e që dalin.  Krimi kibernetik nuk njeh kufij gjeografikë; prokurorët kanë një rol gjithnjë e më të madh në lehtësimin e ndërlidhjes ndërkufitare. Marrja e provave elektronike nëpërmjet ndihmës juridike dhe ekstradimit do të luajë një rol gjithnjë e më të madh se kriminelët përdorin rrjetin botëror për kryerjen e krimeve. Prokurorët do të duhet të punojnë përkrah hetuesve në juridiksionet e tyre dhe prokurorëve dhe hetuesve nga vende të tjera; duke u bërë kështu grup i vetëm për të qenë efiçent dhe për të kryer hetime dhe ndjekje ligjore të ndërlidhura.  Prokurorët duhet të japin udhëzime dhe konsulencë për hetuesit gjatë gjithë procesit të hetimit dhe procedimit gjyqësor. Kjo mund të përfshijë linjat e hetimit, kriteret e provave dhe ndihmën në procedurat paraprake të ngritjes formale të akuzës.  Prokurorët duhet të jenë proaktivë në identifikimin dhe ku të jetë e mundur korrigjimin e të metave tek provat dhe të arrijnë në konkluzione të shpejta në ato çështje që nuk mund të forcohen nga hetimi i mëtejshëm.  Është e rëndësishme të mbahet parasysh se secila çështje është unike dhe duhet të konsiderohet me faktet dhe meritat e saj për të qenë në gjendje të përcaktohet qartë se çfarë masash nevojiten për të garantuar rezultatin e hetimit.  Është e rëndësishme të vlerësohen provat dhe sasia e krimeve që janë zbardhur gjatë hetimit nga këndvështrimi i një ndjekjeje ligjore efektive dhe efiçente.  Një nga gabimet më të mëdha që mund të bëjë një prokuror është të ngarkojë ndjekjen ligjore me detaje dhe fakte të vogla.  Përpiquni të vlerësoni thënien e mirënjohur: «*De minimis non curat praetor*».  Nëse jeni në gjendje të provoni pa të meta në gjykatë 5 krime, përpiquni të fokusoheni tek ato 5 krime. Mos u tundoni të bëni ndjekje penale masive të krimeve për të cilat provat janë shumë të përcipta ose të pasigurta; kjo do të infektojë autoritetin dhe kredibilitetin e provave për krimet e tjera.  Pak është shumë, për sigurinë në krimin kibernetik.  Menaxhimi i ndjekjes ligjore do të thotë gjithashtu se duhet të vlerësoni jo vetëm sasinë e provave dhe gjetjeve por edhe cilësinë.  Duhet të bëheni gjyqtari i parë i punës tuaj! Është shumë e rëndësishme të mos dobësohet ndjekja ligjore me faktorë të pasigurtë:   * Nëse nuk jeni vetë i bindur, mos u përpiqni të bindni gjyqtarin; * Nëse ka ndonjë dyshim në lidhje me ligjshmërinë e disa provave, mos u përpiqni ti përfshini ato me patjetër;   **Bëni një plan për ndjekjen ligjore**  Bëni një plan për ndjekjen ligjore. Mendoni për vijën kryesore dhe themelet e ndjekjes ligjore. Përqendrohuni tek themelet.  Përmbajuni planit, dhe mos i lini avokatët mbrojtës t’ju nxjerrin nga balanca. Mbrojtja ka shumë mundësi të ketë bërë një plan mbrojtjeje. Nëse mbrojtja arrin t’ju bëjë që të ndiqni planin e tyre të mbrojtjes, ia kanë arritur pothuaj qëllimit të tyre. Qëndroni në linjën kryesore, mos i lini t’ju ç’orientojnë që të humbisni dhe ngatërroheni në detaje të parëndësishme që do ta ngatërronin gjyqtarin.  Mos lejoni që të provokoheni. Qëndroni të qetë dhe gjithnjë përmbajuni planit; ndryshojeni vetëm kur nevojitet absolutisht.  **Kontrollojini dyfish provat**  Integriteti dhe autenticiteti i provave është thelbësor.  Provat dixhitale (rezervat kriminalistike të provave, komponentët fizikë dhe programet kompjuterike të sekuestruara) nuk tregohen gjithmonë dhe përdoren në gjykatë përsa kohë që nuk sillen në vëmendje nga avokatët mbrojtës. Megjithatë, kontrollojini dyfish integritetin e provave. A ekziston akoma/ A janë akoma të paprekura rezervat kriminalistike në rast se avokatët mbrojtës i sjellin në qendër të vëmendjes? Këto pyetje duhet të jenë të panevojshme, por shpesh gabime ndodhin. Provat dixhitale janë të brishta.  **Zbulimi i provave**  Shihni kapitullin 7.4 dhe 9.2.3 të Guidës së Këshillit të Evropës për Provat Elektronike.  Secili juridiksion ka rregulla dhe procedura të ndryshme për informimin e mbrojtjes për provat e mbledhura. Zakonisht, prokurori dhe gjyqtari hetues kanë një detyrim për të ndjekur të gjitha linjat e arsyeshme të hetimit pavarësisht nëse këto linja drejtohen tek i dyshuari apo largohen prej tij. Fshirja e materialeve të sjella nga policia ose materiale të palëve të treta në posedim të policisë mund të përbëjë shkelje nëse këto materiale nuk janë gati për t’ju zbuluar mbrojtjes. Në praktikë kjo do të thotë se provat e prodhuara nga policia duhet të shoqërohen me listën e plotë të kontrollit, që nga momenti i kapjes së tyre deri sa i kalohen prokurorisë dhe gjatë gjithë procesit të administrimit të tyre.  Në çdo hetim do të sigurohen materiale që nuk do të mbështeten në provat elektronike. Një i akuzuar duhet të ketë një proces të drejtë ligjor në përputhje me nenin 6 të Konventës Evropiane për të Drejtat e Njeriut (KEDNJ). Hetuesi duhet të identifikojë materialin që ose mund t’ia minojë çështjen akuzës ose të ndihmojë çështjen për mbrojtjen.  Hetuesi e bën këtë duke përdorur metodën kërkimit të termave ose metodën e përzgjedhjes kuturu, dhe përshkruan materialin për programin e zbulimit dhe për shkak të volumit të madh të materialit dixhital të sekuestruar, mund të mos jetë i mundur identifikimi i të gjitha provave. Në raste të tilla, është e rëndësishme të regjistrohen vendimet përkatëse së bashku me justifikimin për miratimin e metodës që është ndjekur.  Në disa juridiksione, zbulimi i provave është një nga çështjet më të rëndësishme në sistemin e drejtësisë penale, dhe aplikimi i zbulimit të drejtë dhe të duhur është një komponent vital i një sistemi të drejtë të drejtësisë penale. “Rregulli i Artë” është që drejtësia kërkon që duhet të zbulohet i gjithë materiali i poseduar nga prokuroria: duke përfshirë provat që dobësojnë çështjen ose forcojnë mbrojtjen.  Hetuesit duhet të jenë të drejtë dhe objektivë së bashku me prokurorët për të garantuar se janë përmbushur detyrimet e zbulimit të provave për palën tjetër. Hetuesit duhet të mbajnë materialin që mund të duhet për hetimet.  Prokurorët duhet të bëjnë gjithçka që munden për të lehtësuar zbulimin e provave, si pjesë e përgjegjësisë personale dhe të përgjithshme profesionale për të vepruar në mënyrë të drejtë dhe të paanshme, në interes të drejtësisë dhe në përputhje me ligjin. Prokurorët duhet gjithashtu të jenë vigjilent për nevojën për të dhënë këshilla, dhe sipas nevojës, për të hetuar veprimet e ndërmarra nga hetuesit që të garantojnë se janë përmbushur detyrimet e zbulimit të materialeve të provave.  **Problemet me provat dixhitale** (gjithashtu shihni slajdin pasues):  Provat dixhitale nuk mund të trajtohen si provat e tjera, sepse janë të:  (1) paqëndrueshme, që do të thotë se mund të zhduken fare lehtë;  (2) lehta për tu manipuluar, që do të thotë se duhet të jemi gjithnjë të sigurtë dhe në gjendje të risigurohemi se provat nuk janë manipuluar;  (3) vështira për tu përftuar, për shkak të kodimit, madhësisë, vendndodhjes, ruajtjes fizikisht larg në Internet...;  (4) vështira për të provuar origjinën dhe autenticitetin, sepse shpesh i marrim në mënyrë virtuale (nuk i sekuestrojmë gjithmonë në mënyrë tradicionale, si për shembull siç sekuestrojmë një armë);  (5) nuk njohin kufij territorial që do të thotë se jo gjithmonë e dimë çfarë ligjesh zbatohen dhe nëse këto prova të huaja janë mbledhur në mënyrë të ligjshme…  **Praktikat më të mira për provat elektronike**  Si përballemi përpara gjykatës kur përdorim provat dixhitale? Siç e thamë, këto prova janë të veçanta dhe kanë nevojë për trajtim të veçantë. Ekzistojnë shumë sfida dhe probleme, por nuk do të ishim këtu nëse nuk mendojmë se shumë probleme kanë zgjidhje.  **Të paqëndrueshme ⮚ Jini të shpejtë dhe koshientë për rregullat e ndryshme në botë për ruajtjen e të dhënave**  Kur hetoni një vrasje me sëpatë, në një moment të caktuar do të sekuestroni sëpatën dhe jeni të sigurtë se kjo sëpatë nuk do të zhduket. Por nuk ndodh kështu me provat dixhitale. Përderisa kemi të bëjmë me prova optike ose elektromagnetike, mënyra sesi janë mbledhur provat është shumë e rëndësishme, siç është dhe mënyra sesi ruhen.  Por me provat elektronike sfidat janë akoma dhe më të mëdha. Përderisa të dhënat nuk ruhen gjithmonë ose ruhen vetëm për një kohë të shkurtër, duhet të veprojmë shpejt dhe të grumbullojmë gjithçka që na nevojitet ose që mund të na duhet më vonë për një debat në gjykatë. Ne mund të mos kemi një shans të dytë ose mundësinë të kthehemi në kohë. Sapo dikush të shtypë butonin “delete” të gjitha provat zhduken njëherë e përgjithmonë.  Gjithmonë duhet të mbajmë në konsideratë rregullat e ruajtjes së provave në vendin tonë dhe në vendet me të cilat duhet të punojmë.  Do të duhet të jemi të ndërgjegjshëm se për vendet Evropiane koha mund të jetë ndërmjet gjashtë dhe njëzet e katër muajve (Direktiva 2006/24/EC e Parlamentit Evropian dhe e Këshillit e datës 15 Mars 2006: “*Shtetet Anëtare duhet të garantojnë se kategoritë e të dhënave të specifikuara në Nenin 5 ruhen për periudha jo më shumë sesa gjashtë muaj dhe jo më shumë sesa dy vjet nga data e komunikimit*.”), por për shembull te Microsoft, në kompaninë e vendosur në Shtetet e Bashkuara të Amerikës, është vetëm nëntëdhjetë ditë (maksimumi)!  Kjo do të thotë se duhet të jeni të ndërgjegjshëm se që nga momenti që jeni në gjykatë, provat dixhitale dhe të dhënat nga koha e krimit me shumë mundësi nuk mund të mblidhen më. Kjo do të thotë se ju duhet të siguroheni, gjatë hetimit, që do të mblidhni gjithçka që ju nevojitet në kohën e duhur. Nuk do të keni një shans të dytë kur të jeni në gjykatë.  **Të lehta për tu manipuluar ⮚ Garantoni integritetin**  Interneti është një kënd lojërash për kriminelët:   * Anonymizers[[20]](#footnote-21):   + TOR (www.torproject.org)   + Proxies[[21]](#footnote-22) (ex. www.proxy4free.com - www.stopkinderporno.com)   = Sfida e **lokalizimit**   * Steganografia: Arti dhe shkenca të të shkruarit të mesazheve të fshehur * Kodimi: Prova dixhitale në kasafortë!   Një nga sfidat më të mëdha është të jesh në gjendje të provosh përpara gjykatës se asgjë nuk ka ndodhur me provat që janë mbledhur dhe se janë në gjendjen që ishin kur sapo u sekuestruan. Të gjithë e dinë se çfarë mund të bëjë një haker me kompjuterin tuaj, se çfarë mund të bëjë programi Photoshop me një imazh dixhital. Mbrojtja do të përpiqet të bëjë audience të besojë se provat janë manipuluar.  Merrni në konsideratë, për shembull, përdorimin e ‘**Mjeteve Hash**’: Funksioni Hashing është transformimi i një zinxhiri karakteresh në një çelës ose vlerë më të shkurtër me gjatësi fikse që përfaqëson zinxhirin fillestar. Hashing përdoret për të indeksuar dhe tërhequr të dhëna nga një databazë sepse është më e lehtë për të gjetur të dhënën duke përdorur funksionin e shkurtuar Hash sesa ta gjesh atë duke përdorur vlerën origjinale. Ky funksion përdoret gjithashtu në shumë algoritme kodimi, dhe për të garantuar autenticitetin dhe integritetin e provave dixhitale. Nëse siguroheni se provat tuaja dixhitale janë vlerësuar me funksionin Hash në momentin e sekuestrimit, ju mund të provoni me siguri matematikore në gjykatë se provat dixhitale të paraqitura në gjykatë dhe të analizuara nga ekspertët janë po të njëjtat të dhëna si ato që u sekuestruan; të dhënat do të kenë të njëjtën vlerë Hash.  **Të vështira për tu marrë ⮚ Përdorni ligjin e brendshëm, NNJ, LO, Rrjetin Gjyqësor Evropian, Pikat e Kontaktit të Këshillit të Evropës, Rrjetin Global të Prokurorëve për Krimin Kibernetik (GPEN), …**  E dimë se provat dixhitale në çështjet e krimit kibernetik ka më shumë të ngjarë të ruhen diku jashtë vendit sesa do të kishte të ngjarë të sekuestroheshin në distriktin tonë. Të dhënat e ruajtura fizikisht larg në Internet, në server që mund të ndodhen kudo në botë …  Një luftëtar i mirë kundër krimit kibernetik do të përpiqet që t’i mbledhë provat sidoqoftë. Ai mund të përdorë traktatet e Ndihmës së Ndërsjellë Juridike, mund të përdorë ndihmën e Oficerit të tij Ndërlidhës me Rrjetin Gjyqësor Evropian, pikat e kontaktit 24/7 (Konventa e Budapestit për Krimin Kibernetik e Këshillit të Evropës), e kështu me radhë.  Do të jetë e rëndësishme t’i shpjegohet gjyqtarit se nga vijnë provat, dhe nëse janë të marra nga jashtë shtetit, nëse procedura e marrjes ka qenë e drejtë dhe e ligjshme. A është ruajtur integriteti i provave edhe në vendin nga erdhën…?  E gjitha kjo do të kundërshtohet nga mbrojtja.  **Vështirë të provohet origjina dhe autenticiteti ⮚ dokumentoni plotësisht të gjitha veprimet, kërkesat dhe ekzaminimin kriminalistik**  Nëse ka ndonjë sekret për një mbyllje të suksesshme të një çështjeje, ai është dokumentimi i plotë – asgjë për të fshehur – i gjithçkaje që ka ndodhur gjatë hetimit.  Sigurohuni që të gjitha raportet të përmendin të gjitha hapat të provojnë logjikën e veprimeve investigative.  Nëse kjo gjë bëhet, atëherë jemi plotësisht në përputhje me nenin 6 të KEDNJ.  **Nuk ka kufij territorialë ⮚ Ndiqni rregullat e bashkëpunimit ndërkufitar**  Përpiquni të realizoni vetë sa më shumë që të mundeni, megjithatë përdorini dhe mundësitë e bashkëpunimit ndërkufitar. Për çdo veprim që do të ndërmerret, ai duhet të dokumentohet plotësisht.  Pranueshmëria e provave që janë mbledhur nga jashtë shtetit është një çështje e vështirë gjyqësore.  Disa vende mendojnë se kur provat merren nga një vend tjetër, ata mund të mbështeten mbi këto prova përderisa nuk mund të ketë diskutime sesi vendi tjetër i organizon hetimet e tij (bazuar në besim). Vende të tjera lejojnë që provat e huaja të kundërshtohen, dhe krahasojnë mënyrën në të cilën provat u mblodhën me rregullat e tyre. Jini të ndërgjegjshëm dhe të përgatitur për këtë. Do të bisedojmë për garantimin e integritetit dhe ligjshmërisë së provave dixhitale të marra nga jashtë shtetit më vonë.  **Gjyqtarët nuk janë mësuar me provat dixhitale**  Duhet të kuptohet se kur flasim për prova dixhitale dhe prezantimin e një çështjeje të krimit kibernetik përpara gjykatës, edhe sot duket një diçka e re për shumicën e gjyqtarëve dhe prokurorëve. Pra, duhet të jemi të kujdesshëm. Shumë përpjekje janë bërë për trajnimin e oficerëve të policisë, prokurorët, avokatëve dhe gjyqtarëve që të mund të jenë në gjendje të trajtojnë çështjet e krimit kibernetik dhe provat elektronike. Jo vetëm që janë organizuar në nivel kombëtar, por gjithashtu edhe në nivel Evropian dhe ndërkombëtar (arsyeja se pse jemi këtu apo jo).  Fatkeqësisht, e dimë se fakti që sot çështjet e krimit kibernetik hetohen nga punonjësit e specializuar dhe të trajnuar të policisë, nuk do të thotë se çështja do të çohet në gjykatë nga një prokuror i specializuar ose do të gjykohet nga një gjyqtar i specializuar.  Shumica e magjistratëve janë trajnuar në një kohë jo dixhitale dhe madje edhe kur janë juristë të shkëlqyer ata prapëseprapë mund të mos e kenë idenë e provave elektronike, sesi janë mbledhur ato apo shkurt sesi funksionon kompjuteri ose Interneti.  Sigurisht avokatët mbrojtës do të duan të përfitojnë nga kjo situatë.  Po përveç problemeve që mund të dalin në lidhje me personat që trajtojnë këto çështje të krimit kibernetik, problemeve që mund të zgjidhen me mënyrën sesi prezantohet çështja në gjykatë (shihni më tej), vetë provat dixhitale duhet të trajtohen në një mënyrë të veçantë përpara gjykatës.  Kjo ka të bëjë me karakteristikat e provave dixhitale.  **Përdorimi i provave dixhitale në procedimin gjyqësor**  Shihni Kapitullin 7 të Guidës së Këshillit të Evropës për Provat Elektronike.  Përdorimi i provave elektronike është rritur gjatë viteve të fundit se gjykatat kanë pranuar prova elektronike në formën e mesazheve elektronike, fotografive dixhitale, regjistrimeve të transaksioneve nga bankomatët, dokumente teksti, mesazhe të menjëhershme, fletët e punës, historitë e navigimit në Internet, bazat e të dhënave, përmbajtjet e memories së kompjuterëve, rezervimi i skedarëve të kompjuterit, dokumente kompjuterike të printuara dhe skedarë dixhitalë audio dhe video – të gjitha këto përbëjnë të dhëna dixhitale.  Një pajisje dixhitale e përdorur në një krim duhet të sigurohet njësoj si do të siguronit forma të tjera të provave materiale që do të gjendeshin në skenën e krimit, sepse të gjitha këto pajisje mbeten prova materiale. Njësoj si gjurmët e gishtërinjve dhe provat e ADN-së, provat dixhitale janë të brishta dhe humbasin apo modifikohen me lehtësi nëse nuk ndërmerren masat e duhura. Në ditët e para të provave dixhitale, punonjësit e patrajnuar të forcave të zbatimit të ligjit ndiznin kompjuterët për të kërkuar prova përpara se t’i dorëzonin ato për ekzaminim kriminalistik.  Është e rëndësishme të regjistrohet se ku u gjet dhe u sekuestrua prova dixhitale, sepse mund të zbulojë shumë në lidhje me synimin e keqbërësit të dyshuar. Është praktikë e mirë të regjistrohet kontrolli dhe sekuestrimi me video. Kjo do të tregojë pozicionin e pajisjeve dixhitale, në mënyrë që të mos ketë diskutime, për shembull, se pajisja pa kabull u gjet e fshehur në raft dhe jo në vend të hapur në dhomën e ndenjes.  **Cilësia me Tre A është e detyrueshme**  **Pranueshmëria**  Provat kompjuterike janë të pranueshme nëse janë konform me një sërë rregullat dhe ligjesh që garantojnë se ato janë të pranueshme në gjykatë. Duhet të ndiqen procedurat e duhura gjatë marrjes së provave. Këto trajtohen në kapitujt 4, 5 dhe 6 të Guidës së Këshillit të Evropës për Provat Elektronike.  Provat dixhitale në çështjet penale duhet të jenë të pranueshme, autentike, të sakta dhe të plota. Ato duhet të jenë konform me një seri ligjesh dhe rregullash dhe duhet të jenë të pranueshme në gjykatë.  Në rishikimin e çështjes, prokurori do të konsiderojë nëse është e mundur të lidhen në mënyrë të qartë skedarë, të dhëna për individë dhe ngjarje specifike, dhe të shpjegojë sesi u krijua një provë materiale duke demonstruar një sekuencë të pandërprerë provash, duke e ruajtur zinxhirin e ruajtjes së provave.  Gjatë gjykimeve penale, prokurori duhet të përdorë provat për të provuar çështjen ‘përtej dyshimit të arsyeshëm’. Si pjesë e rregullave të provave, gjykata ka gjithnjë të drejtë që t’i paraqiten provat më të mira. Tradicionalisht, provat më të mira janë dokumentet origjinalë, por në disa rrethana të caktuara, mund të pranohen edhe provat dytësore. Zakonisht provat dytësore përfshijnë kopje ose ekstrakte të provave më të mira.  Një rishikim i hershëm i provave elektronike nga prokurori lejon për një përgjigje të shpejtë, që do të ndihmojë për të përcaktuar se ku kërkohen prova të tjera elektronike ndërkohë që ka akoma mundësi që ato të merren nga juridiksionet e tjera.  **Autenticiteti, saktësia, dhe plotësia**  I takon palës që kërkon që provat të pranohen të përgatisë dhe paraqesë prova për autenticitetin e të dhënave.  Provat elektronike nuk janë të ndryshme nga provat materiale fizike, të tilla si një dokument i regjistruar në një copë letër. Është e nevojshme të garantohet se provat janë autentike. Ndryshimi ndërmjet provave elektronike dhe provave fizike është zakonisht lehtësia me anë të të cilës mund të ndryshohet ose modifikohen provat elektronike, ose me qëllim ose pa qëllim.  Provat elektronike i nënshtrohen rregullave dhe ligjeve të njëjta që zbatohen për provat dokumentare. Doktrina e provave dokumentare mund të shpjegohet kështu: barra i takon prokurorisë për ti treguar gjykatës se provat e paraqitura nuk janë as më shumë e as më pak por ato që u morën në fillim në posedim nga policia. Sistemet e operimit dhe programet e tjera shpesh ndryshojnë dhe shtojnë të dhëna në përmbajtjen e të dhënave elektronike. Kjo mund të ndodhë automatikisht pa domosdoshmërisht dijeninë e përdoruesit se të dhënat po ndryshohen.  Për t’iu përmbajtur parimeve të provave elektronike, sipas rastit, duhet t’i bëhet një imazh të gjithë pajisjes në objektiv. Si alternativë në rrethana të caktuara mund të merret parasysh edhe kopjimi i pjesshëm ose me përzgjedhje i skedarëve, për shembull kur sasia e të dhënave, të cilave duhet t’u bëhet imazhi e bën këtë jo praktike. Megjithatë, hetuesit duhet të jenë të kujdesshëm për të garantuar marrjen e provave përkatëse nëse miratohet kjo metodë.  Në një pakicë çështjesh, mund të mos jetë e mundur të merret një imazh duke përdorur një pajisje për marrjen e imazhit. Në këto rrethana, mund të bëhet e domosdoshme të merret aksesi për tek makina origjinale për rikuperimin e provave. Me këtë në mendje, është thelbësore që provat të merren nga një specialist i kualifikuar për provat dixhitale që është kompetent në këtë fushë.  Është e domosdoshme që në gjykatë të tregohet objektiviteti si dhe vazhdimësia dhe integriteti i provave. Është gjithashtu e domosdoshme të demonstrohet sesi u mblodhën provat, duke treguar secilin proces nëpërmjet të cilit u morën ato. Provat duhet të ruhen në një masë të tillë saqë një palë e tretë të jetë në gjendje të përsërisë të njëjtin proces me të njëjtin rezultat si ai i paraqitur në gjykatë.  **Bindja**  Në rastin kur ekziston dyshim për të dhënat e shtuara tek provat elektronike, i takon mbrojtjes të kundërshtojë pranueshmërinë e provave. Sapo të ngrihet si çështje, prokuroria duhet ta trajtojë këtë, zakonisht duke dhënë prova të mjaftueshme se “integriteti i të dhënave është i besueshëm, dhe për rrjedhojë ato janë të besueshme”. Provat duhet të jenë bindëse.  Një aspekt tjetër i provave është mënyra sesi u morën ato, dhe nëse është përcaktuar metoda e trajtimit të tyre, për shembull, me anë të rishikimit shkencor. Për shembull, nëse prokuroria paraqet një faturë telefoni, për të treguar se i akuzuari ishte lidhur me ISP-në në një moment të caktuar të ditës, atëherë kjo zakonisht pranohet. Nga ana tjetër, nëse prokuroria pretendon se “i akuzuari i ka fshirë të gjithë skedarët nga disku i tij i kompjuterit, e ka riformatuar atë, dhe më pas e ka hedhur nga dritarja e katit të 10-të, por ne kemi mundur të rindërtojmë skedarët me ndihmën e një firme për rikuperimin e të dhënave”, atëherë mbrojtja mund të vendosë pikëpyetje mbi vlefshmërinë e metodës së rikuperimit të të dhënave. I takon akuzës të demonstrojë se metodat e përdorura për rikuperimin e provave ishin të vlefshme dhe të bindë gjykatën se provat duhet të pranohen.  Është e domosdoshme të vendoset balanca e duhur. Nga njëra anë, nuk është e arsyeshme të presësh që një gjyqtar (pavarësisht nëse mund të jetë anëtar i jurisë së gjykimit apo një gjyqtar i vetëm) të kuptojë procesverbalin teknik. Nga ana tjetër, nuk është e përshtatshme të presësh që gjyqtari të pranojë se teknikat e rikuperimit të të dhënave janë “magjike”. Në disa vende, përgjigjja është rishikimi i materialeve nga kolegët – nëse specialistë të tjerë të fushës e kanë studiuar këtë teknikë, e kanë testuar atë, dhe kanë vlerësuar rezultatet atëherë gjykata do të pranojë provat.  Në thelb, provat elektronike shqyrtohen në të njëjtën mënyrë si dhe format e tjera të provave. Prokuroria do të duhet të provojë se dokumenti është autentik dhe se përmbajtja e tij është e pranueshme. Të gjitha shqyrtimet e provave elektronike duhet të jenë konform me parimet e provave elektronike të përcaktuara në hyrje të kësaj guide.  Parimet vendosin themelet për përdorimin e provave elektronike dhe duhet të merren në konsideratë gjithmonë gjatë shqyrtimit të burimeve potenciale të provave të tilla.  **Kategorizoni provat dixhitale në 3 grupe:**   * Regjistrime të aktiviteteve që kanë dokumente të shkruara nga një apo më shumë persona (P.sh. mesazhet elektronike, skedarët Word, Mesazhet e menjëhershme). Mund të jetë e nevojshme të demonstrohet se përmbajtja e dokumentit është e dhënë e besueshme e deklarimeve njerëzore, e cila mund të besohet. * Të dhënat e gjeneruara nga një kompjuter që nuk ka pasur ndonjë ndikim nga ndonjë njeri (p.sh. skedarë me regjistrime të të dhënave, veprimet në bankomate, lidhjet telefonike). Çështja kryesore provuese me të dhëna të tilla mund të jetë demonstrimi se programi kompjuterik që i gjeneroi të dhënat po funksiononte në vazhdimësi në kohën e caktuar. * Të dhëna që përfshijnë një kombinim të të dhënave të futura nga njerëzit dhe përllogaritje të gjeneruara dhe të memorizuara nga kompjuteri (p.sh. një fletë pune financiare). Nga këndvështrimi i provave, çështja është nëse përmbajtja e të dhënave u krijua nga njeriu apo nga kompjuteri, dhe sasia e krijuar nga njeriu dhe sasia e krijuar nga kompjuteri. Është e mundur që të dhënat e futura mund të jenë fjalë të dëgjuara, dhe autenticiteti i përpunimit kompjuterik mund të jetë çështja.   **Roli i rëndësishëm i ekspertëve/specialistëve të provave dixhitale**  Zemra e rolit të një eksperti kriminalist si dëshmitar qëndron në prodhimin e raporteve që lidhen me provat elektronike të marra, deklaratat dhe kundërshtimi i raporteve të kundërta ku të jetë e përshtatshme. Duhet të inkurajoni përdorimin e thënieve të shkurtra, qartësisht të ndara ndërmjet faktit dhe mendimit, në mënyrë që të mund të ketë një kuptim të saktë se cilat janë proceset e mendimit dhe argumentet që ngrihen. Kërkoni dokumentacion mbështetës si shtojcat p.sh. dhe jo dokumente voluminozë të panevojshëm.  Një raport i shkurtër mund të jetë një raport i mirë; një raport i gjatë nuk është i nevojshëm nëse askush nuk është në gjendje ta lexojë deri në fund.  Kërkoni informacion dhe shpjegime specifike nëse dihen ose për udhëzim nga dëshmitari përpara deklarimeve nëse nuk dihen, dhe nëse dihen bëni pyetje specifike që dalin nga deklarimet kundërshtuese që kërkojnë kundërshtim ose shpjegim. Më e rëndësishmja kërkoni që dëshmitarët të nxjerrin dhe të bien dakord për një fjalorth termash që do të përdoren gjatë çështjes.  Ekspertët e kriminalistikës kur janë si dëshmitarë inkurajohen që të përcaktojnë pikat e përbashkëta dhe diferencat e rëna dakord ndërmjet pozitave të akuzës dhe mbrojtjes në lidhje me interpretimin e provave dixhitale, dhe është gjithashtu e dobishme që të bihet dakord për një fjalorth termash të fushës.  Është thelbësore që përfaqësuesit e të dy anëve të ndjekin takimet ndërmjet ekspertëve kriminalistë si dëshmitarë. Në takime duhet të mbahet procesverbal, i cili duhet të nënshkruhet nga të dy palët.  Provat që eksperti dëshmitar jep duhet të kenë karakteristikat e mëposhtme me qëllim që të garantohet vlerësimi i saktë në Gjykatë:  a. të Besueshme  b. të Paanshme  c. të Qarta  **Zinxhiri i Ruajtjes së Provave Elektronike**  Shihni kapitullin 9.4.3 të Guidës së Këshillit të Evropës për Provat Elektronike.  Zinxhiri i ruajtjes së provave fillohet me përshkrimin e sekuestrimit nga punonjësi i zbatimit të ligjit dhe ka për qëllim të regjistrojë të gjitha veprimet që ndodhin me provat elektronike që do të analizohen.  Sapo klonohet një pajisje për mbajtjen e të dhënave, rekomandohet shumë që nëse është e mundur pajisja origjinale të mbahet në ruajtje nga punonjësi i zbatimit të ligjit. Në rast se kjo gjë nuk është e mundur, atëherë është e mundur që të bëhet një kopje e dytë gjatë procesit të sekuestrimit për ta çuar tek punonjësi i zbatimit të ligjit, ndërsa pajisja e parë e klonuar do të përdoret për ekzaminimin kriminalistik. Nëse nevojiten më shumë kopje të klonuara për ekzaminime shtesë ose për specialistin e palës kundërshtare, atëherë kopje të tilla mund të bëhen nga pajisja që është në ruajtje nga punonjësi i zbatimit të ligjit.  Duke lënë në ruajtje origjinalin ose kopjen, ne lejojmë që përmbajtja e diskut të kompjuterit të jetë e aksesueshme për palët e tjera që mund të duan të provojnë manipulimin ose mos-manipulimin e rezultateve të paraqitura duke aksesuar origjinalin dhe duke bërë një kopje identike për të kryer një ekzaminim të dytë kriminalistik.  Sekuestrimi i pajisjes origjinale të ruajtjes së të dhënave me punonjësin e zbatimit të ligjit është e mundur vetëm kur largimi i pajisjes nga vendi i sekuestrimit nuk do të shkaktojë ndonjë dëmtim ekonomik për shembull privimin e një biznesi nga të dhënat e tij dhe vetëm kur është zgjedhja më pragmatike dhe në proporcion me rrethanat e çështjes. Në të gjitha rastet e tjera, pajisja origjinale e ruajtjes së të dhënave nuk duhet të sekuestrohet, por në vend të saj duhet të bëhet një kopje ekzakte sepse kjo është e mjaftueshme për garantimin e ruajtjes së përmbajtjes së pajisjeve elektronike të të dhënave.  Punonjësi i ligjit më pas do t’i mbajë të dhënat e sekuestruara në ruajtje, ose pajisjen origjinale të të dhënave ose një kopje identike, dhe do të krijojë një dokument që përshkruan secilën kohë që u administruan të dhënat, nga kush, dhe për çfarë qëllimi për të përshkruar zinxhirin e ruajtjes së provave.  **Garantimi i integritetit të provave që vijnë nga jashtë shtetit:**  Është e domosdoshme që të përfshini në kërkesën për Ndihmë të Ndërsjellë Juridike që të gjitha veprimet dhe metoda e hetimit të dokumentohet.  Shumë shtete, për shembull SHBA dhe MB (ku janë përqendruar lojtarët më të shumtë në Internet), janë të gatshme të marrin në konsideratë procedime të posaçme dhe kritere me qëllim garantimin që provat të mblidhen në përputhje me ligjin kombëtar.  Për shembull ju mund të specifikoni në kërkesën tuaj për NNJ se keni nevojë që provat dixhitale të sekuestruara të jenë me kopje rezervë dhe të vulosura në një mënyrë të caktuar. Ju, madje, mund të kërkoni që të gjitha provat të kalojnë procesin “Hash”.  **Garantoni pranueshmërinë dhe ligjshmërinë e provave që vijnë nga jashtë shtetit:**  Ju mund të merrni në konsideratë se jo të gjitha provat që vijnë nga jashtë shtetit mund të konsiderohen të pranueshme.  Jo të gjitha shtetet nga të cilat do të kërkonit prova dixhitale e kanë ratifikuar KEDNJ-në.  Duhet të merrni në konsideratë çështje si:  Klauzola e vetë-inkriminimit: Në disa shtete, legjislacioni e mundëson të detyrosh një të dyshuar të bashkëpunojë me drejtësinë (p.sh. të japë një çelës ç’kodimi, një fjalëkalim,…). Kjo mund të mos jetë e pranueshme në Gjykatë në vendin tuaj.   * Përdorimi i provokimit (i pranueshëm në SHBA, i papranueshëm në Evropë) * Ndihma e avokatit (vendimi Salduz i KEDNJ) * Mund të specifikoni në kërkesën tuaj për NNJ se dëshironi që shteti i kërkuar të marrë parasysh detyrimet procedurale.   **Juridiksioni dhe kombësia e provave:**  Shihni Kapitullin 8 të Guidës së Këshillin të Evropës për Provat Elektronike që flet për **JURISDIKSIONIN**  **Dimensioni Ndërkombëtar i Krimit Kibernetik**  Rrjeti botëror është një kënd lojërash i mirë për keqbërësit. Me mijëra fëmijë dhe të rritur në të gjithë globin dëmtohen çdo ditë nga keqpërdorimi i Internetit; të pafajshëm që iu vidhen paratë, dhe hajdutët që kryejnë krime të mëdha pa kufizim kufijsh ndërkombëtarë. Për këtë arsye, është e rëndësishme për autoritetet e hetimit që të lehtësohet ndërlidhja ndërkufitare. Marrja e provave nëpërmjet ndihmës së ndërsjellë juridike dhe ekstradimit luan një rol të rëndësishëm në punën e forcave të policisë dhe prokurorëve. Prokurorët punojnë me hetuesit dhe prokurorët nga vendet e tjera për të çuar përpara hetimet dhe ndjekjen ligjore. Bashkëpunimi ndërkombëtar për hetimin e krimeve kibernetike duhet të theksohet gjithnjë e më shumë.  Hetimet ndërkufitare duhet të trajtojnë një çështje të rëndësishme: rrethanat në të cilat një punonjës i zbatimit të ligjit mund të hetojë në mënyrë të ligjshme jashtë vendit të tij/saj (duke përfshirë provat e ruajtura në ‘re’, të cilat mund të jenë kudo), veçanërisht nëse ai/ajo duhet të veprojë me urgjencë. Është e rëndësishme të dihet nëse është e mundur të merren dhe mblidhen provat elektronike që ruhen diku jashtë kufijve të një shteti, veçanërisht nëse provat ka të ngjarë të zhduken.  Ka dy kategori rrethanash që janë të rëndësishme për tu dalluar kur trajtohen provat elektronike që nuk janë fizikisht brenda juridiksionit:  1. Kur një hetues ka marrë kontrollin e një kompjuteri të lidhur në Internet. Në rrethana të tilla, hetuesi mund të ketë autoritetin për të klikuar në uebsajte ose të hyjë në kompjuterë në juridiksione të tjera. Autoriteti për të vepruar kështu mund t’i jepet hetuesit në bazë të ligjit të brendshëm ose një kombinimi të ligjit të brendshëm dhe dispozitave të nenit 32 të Konventës së Budapestit për Krimin Kibernetik.  2. Kur provat elektronike gjenden në “re” – dmth kur për shembull mesazhet elektronike të një të dyshuari nuk janë ruajtur në kompjuterin e shtëpisë por janë ruajtur diku tjetër, në një disk të posaçëm në Shtetet e Bashkuara të Amerikës.  Është e rëndësishme të kuptohet ndryshimi ndërmjet këtyre dy lloj rrethanash, sepse autoritetet hetimore do të duhet të ndërmarrin veprime të ndryshme në secilën rrethanë në varësi të legjislacionit vendas.  **Përgjigjja ndaj krimit kibernetik**  Ka masa të ndryshme që janë ndërmarrë nga Evropa si përgjigje ndaj krimit kibernetik. Ato më të fundit përfshijnë Interpolin, Këshillin e Evropës dhe zhvillimet nga Bashkimi Evropian (Rrjeti i Pikave të Kontaktit, Europoli, Eurojust-i dhe Rrjeti Gjyqësor Evropian në çështjet penale). Burimet e këtyre institucioneve mund të jenë të disponueshme për aktorë të ndryshëm në sistemin e drejtësisë penale për t’i ndihmuar ata në hetime dhe ndjekje penale.  **Ndihma e Ndërsjellë Juridike**  Shtetet sovrane gjithmonë kanë pasur nevojë të bëjnë kërkesa shteteve të tjera sovrane në lidhje me mbledhjen e provave për krimet që përfshijnë një komponent ndërkombëtar. Në këto çështje, mund të bëhet një aplikim për Ndihmë të Ndërsjellë Juridike (NNJ), ose të kërkohen forma të tjera bashkëpunimi. Kërkesat për ndihmë ndërkufitare janë veçanërisht të rëndësishme në çështjet që kanë të bëjnë me provat elektronike sepse ekziston mundësia që provat të fshihen ose të modifikohen. Sfida reale në këto çështje është të jesh në gjendje të veprosh me mjaft shpejtësi.  Kur bëhet një kërkesë për NNJ, është e nevojshme të fillohet me një kërkesë formale nga autoritetet e prokurorisë, ose nganjëherë nga autoritetet gjyqësore. Megjithatë, suksesi i një kërkese të tillë shpesh varet nga vullneti i mirë dhe niveli i ekspertizës së atyre që janë përfshirë, edhe nga autoritetet kërkuese edhe nga autoritetet që u dërgohet kërkesa. Krahas kësaj, mund të duhen ca kohë që kërkesa të plotësohet.  Për këtë arsye, autoritetet e hetimit dhe ndjekjes ligjore mund të provojnë të marrin provat nga një rrugë tjetër në çështjet që kanë prova elektronike me qëllim që të kenë një rezultat më të mirë.  **Çështje Ndërkufitare**  Kur një çështje kalon një numër juridiksionesh duhet të merren parasysh edhe ligji material, por edhe diskutimet ndërmjet institucioneve të ndryshme përgjegjëse për hetimin e veprave penale në secilin juridiksion. Kjo mund të jetë një zonë komplekse, dhe nganjëherë merret një vendim për të lejuar një grup të vetëm hetuesish në një juridiksion të marrin drejtimin në hetimin dhe procedimin e veprave penale. Institucionet përkatëse në juridiksionet e tjera do të bien dakord me institucionin që drejton hetimin për sigurimin e provave në juridiksionin e tyre.  Neni 35 i Konventës së Budapestit ofron pak ndihmë praktike për hetuesit sepse kërkon që secila palë nënshkruese të “caktojë një pikë kontakti të disponueshme njëzet e katër orë në ditë dhe shtatë ditë në javë”. Synimi për këtë është parashikimi i “ndihmës së menjëhershme për qëllime të hetimeve ose procedimeve në lidhje me veprat penale që lidhen me sistemet dhe të dhënat kompjuterike, ose për grumbullimin e provave në formë elektronike për një vepër penale”.  Palëve në Konventë iu kërkohet të ndërmarrin një numër masash, me kusht që praktika dhe legjislacioni i brendshëm t’ju lejojë si më poshtë:  1. Dhënien e konsulencës teknike;  2. Ruajtjen e të dhënave sipas Neneve 29 dhe 30;  3. Grumbullimin e provave, dhënien e informacionit ligjor dhe vendndodhjen e të dyshuarve.’  Kjo është një pjesë e rëndësishme e lehtësimit të punës efektive dhe efiçente në procedimin e krimeve që përfshijnë një element të provave elektronike në juridiksione të ndryshme.  **Kompetenca territoriale (e mbledhjes së provave) në hapësirën kibernetike:**  **Një përpjekje Belge për një zgjidhje dhe një ftesë për reflektim për të gjithë**  *A keni frikë nga lufta kundër krimit kibernetik?*  *Një histori nga jeta reale për të treguar disa probleme.*  Kristian B., i cili jeton pranë ndërtesës së Parlamentit Evropian në Bruksel, nuk i pëlqen gjithë këto institucione Evropiane dhe dëshiron që në Bruksel të jetonin vetëm belgët që janë aty. Ai vendos të fillojë një fushatë terrori dhe dëshiron të shkaktojë frikë që të largohen Evropianët. Ai fillon me dërgimin e disa mesazheve elektronike, në të cilat ai pretendon se është një organizatë me bazë në Gjermani që lufton për një Bashkim Evropian më të vogël dhe se ai nuk është vetëm, dhe është i përgatitur madje të vendosë bomba për arritjen e synimit final.  Kristiani nuk di shumë nga kompjuterët, por në Internet mësoi se mund të bëhet totalisht anonim duke përdorur instrumente lirshmërisht të disponueshme.  Mesazhet e tij elektronike u dërguan nga llogaria e Hotmailit bessermit8@hotmail.com, që do të thotë se llogaria e tij e postës elektronike është në serverët e uebsajtit Hotmail në SHBA (Kristiani dëgjoi se bashkëpunimi me SHBA-në është i ngadaltë dhe jo efektiv kur policia dëshiron të marrë përmbajtjen e mesazheve për shkak të rregullave të posaçme *“probable cause”[[22]](#footnote-23)*). Llogaria në Hotmail u krijua duke përdorur Rrjetin TOR (the Onion Ring Router[[23]](#footnote-24)) dhe çdo lidhje më pas u realizua duke përdorur këtë rrjet. Nga të dhënat teknike në kokën e mesazhit elektronik dhe nga të dhënat e regjistruara nga Kompania Microsoft, policia është e mendimit se mesazhet elektronike u dërguan nga Gjermania por llogaria ishte krijuar në Kazakistan.  Policia Belge nuk e di nëse është e mundur të vazhdojë hetimin, sepse mendojnë se kjo është një çështje për policinë Gjermane (personi thotë se i përket një organizate Gjermane, dhe mesazhet elektronike duket sikur dërgohen nga Gjermania); atyre nuk iu pëlqen të dërgojnë letër porosie në SHBA dhe në Kazakistan, sepse e dinë se nuk do të marrin përgjigje ose do të marrin përgjigje shumë vonë në lidhje me rregullat e mbajtjes së të dhënave në Evropë që thonë se provat dixhitale nga Kompanitë Shërbimofruese të Internetit duhet të eliminohen mbas një periudhe prej 12 muajsh.  Autoritetet e zbatimit të ligjit dhe gjyqësori në Belgjikë u detyruan nga qeveria belge të ndërmarrin veprime.  Po ku të fillonin?  A është kompetente territorialisht policia Belge?  A është policia Belge kompetente t’i mbledhë vetë provat në Gjermani, SHBA, Kazakistan apo nga ndonjë shtet tjetër?  **Kur jemi territorialisht kompetentë për të trajtuar një çështje të krimit kibernetik?**  Në Belgjikë, neni 3 i Kodi Penal Belg thotë se gjykatat duhet të jenë kompetente për të gjitha krimet në territorin Belg, pavarësisht nëse janë kryer nga Belgët apo të huajt (kompetenca territoriale).  Neni 4 thotë se gjykatat do të jenë kompetente për krimet e kryera jashtë shtetit vetëm kur parashikohet kështu nga Kodi i Procedurës Penale Belge (p.sh. neni 10 i Titullit Paraprak të Kodit Penal të Belgjikës: shfrytëzimi seksual, përdhunimi, sulmi ndaj personit, terrorizmi) (kompetenca jashtëterritoriale). Shumë vende kanë dispozita të ngjashme për kompetencën territoriale.  Kur e konsiderojmë veten kompetentë territorialisht, avantazhet e kësaj kompetence territoriale janë të shumta: ajo bazohet në sovranitetin kombëtar; nuk ka kushte bashkëngjitur për tu bërë kompetent; kombësia e keqbërësit ose viktimës janë irelevante (madje edhe kur të dy janë të huaj ose nuk janë të ndëshkueshëm në një shtet tjetër (p.sh. bigamia). Një gjykim i bazuar në të njëjtat fakte në një shtet tjetër nuk është domosdoshmërisht një pengesë dhe legjislacioni i huaj nuk ka pse të merret në konsideratë (nuk kërkohet kriminalizim i dyfishtë).  Çështja kryesore në gjykimin e krimit kibernetik mbetet lokalizimi i veprës penale kibernetike. Deri më sot askush nuk ka vendosur ndonjë flamur (akoma) në hapësirën kibernetike. Askush nuk e di në të vërtetë se ku është hapësira kibernetike dhe askush nuk e di në të vërtetë sesi të trajtojë *“realitetin virtual”* në drejtësi. Mendjet gjyqësore shpesh nuk duket të jenë gati për implementimin e mënyrës së tyre tradicionale të materializuar në mjedisin virtual kibernetik. Hapësira kibernetike nuk ka kufij dhe krimi kibernetik nuk ka kufij. Si mund ta pajtojmë këtë fakt me rregullat tona të ngushta të kompetencës kombëtare dhe gjyqësore? Si mund ta lidhim një krim (në hapësirë) kibernetik me tokën e një kombi?  Në Belgjikë, si në shtetet e tjera, çështja e lokalizimit të një vepre penale nuk rregullohet me ligj por me doktrinën juridike. Për të lokalizuar një vepër penale, janë nxjerrë në dritë teori të ndryshme. Ekziston teoria e ngjarjeve kriminale sipas të cilës, përcaktuese duhet të jetë ku filloi vepra penale ose *itercriminis*. Në përputhje me teorinë e instrumentit, është e rëndësishme se ku ka ndodhur akti kriminal dhe ku u ekzekutua. Teoria e pasojës së drejtpërdrejtë e vë theksin tek rezultati i krimit.  E përkthyer në gjuhën e hapësirës kibernetike, kjo do të thotë se në përputhje me teorinë e instrumentit, vendi i banimit (dhe kompjuteri) i hakerit përcakton prokurorin dhe gjykatën kompetente. Në përputhje me teorinë e instrumentit, vendndodhja e serverit me anë të të cilit u krye veprimi i paligjshëm është përcaktues. Dhe së fundi, në përputhje me teorinë e pasojës së drejtpërdrejtë, do të ishte shteti në të cilin viktima është përballur me veprimin e paligjshëm.  Shumica e shteteve zbatojnë një kombinim i këtyre teorive. Për shembull në SHBA gjykatat zbatojnë gjerësisht teorinë e efekteve, që përfshijnë gjithashtu efekte të largëta, me qëllim që të deklarohen kompetente.  Në Belgjikë, përdoret një kombinim i të gjitha teorive, e quajtur “theory of objective ubiquity” (*“théorie de l’ubiquité objective”*), në përputhje me të cilën vepra e paligjshme ndodhet në të gjitha vendet ku ekziston një element konstituiv i shkeljes. Kjo teori është plotësuar nga “teoria e pandashmërisë”, e cila bën të mundur që Gjykatat të marrin në konsideratë të gjitha elementët që janë pandashmërisht të lidhura me një vepër të paligjshme në Belgjikë me qëllim që të deklarohen kompetentë. Kjo është shumë e krahasueshme me teorinë e efekteve. Teoria Belge është përcaktuar qartë nga Gjykata e Kasacionit e Belgjikës (Gjykata e Lartë) në 23 Janar 1979 (në çështjen Ghavami-Lahidji). Një çek i keq u shkrua dhe u lëshua në Teheran, por llogaria tek e cila ata u përpoqën të ngarkonin çekun (në Teheran) ishte një llogari bankare Belge. Gjykata Belge e Kasacionit vendosi që gjykatat Belge ishin kompetente.  Kjo ishte në vitin 1979, shumë përpara se të zbuloheshin hapësira kibernetike dhe krimi kibernetik. Tani, si mund t’i zbatojmë këto rregulla dhe teori në çështjet e krimit kibernetik?  Në vitin 2008, filloi një çështje në gjykatën e shkallës së parë të Dendermonde në Belgjikë. Një grua u ndoq ligjërisht për hyrje të paautorizuar në llogarinë e Hotmail-it dhe disa llogari të tjera në Internet të ish të dashurit të saj që e kishte tradhtuar. Punë e madhe, mund të mendojë dikush. Megjithatë problemi ishte se kjo grua jetonte në një rreth gjyqësor tjetër, dhe se ajo kishte kryer hyrjen e paautorizuar nga ai distrikt në serverë që ndodheshin në SHBA dhe Holandë. Gjyqtari dha vendim në 29 Shtator 2008 se ai ishte kompetent se viktima u përball së pari me hyrjen e paautorizuar kur ai kontrollonte llogarinë e tij të postës elektronike dhe llogaritë e tjera kur ishte në distriktin e Dendermondes. Me sa duket, në përputhje me këtë vendim, aktivizimi i kompjuterit tuaj dhe të provuarit e krimit kibernetik është e mjaftueshme për të përcaktuar juridiksionin. Gjyqtari siç duket gjeti në distriktin e tij një udhëkryq ndërmjet botës reale dhe botës virtuale.  Në Belgjikë, duket se është e mjaftueshme të aktivizohet një kompjuter dhe të hyhet në Internet në një vend të caktuar me qëllim që të sigurohet kompetenca. Kjo mund të ketë kuptim se Belgjika pretendon të ketë një lloj kompetence globale në lidhje me krimin kibernetik. Kjo gjithashtu do të thotë se çdo shtet tjetër mund të jetë njësoj kompetent. Sado absurde mund të duket në pamje të parë, ne duhet të marrim në konsideratë mundësinë që krimi kibernetik shkakton një formë të kompetencës globale.  I njëjti gjyqtar i çështjes së përmendur më lart dha vendim në 2 Mars 2009 se Kompania YAHOO Inc.! ishte virtualisht dhe ekonomikisht e pranishme në Belgjikë (nëpërmjet Internetit) dhe për rrjedhim duhet gjithashtu të konsiderohet e pranishme gjyqësisht në një mënyrë të tillë që Kompania YAHOO Inc.! duhet t’i bindet urdhrit direkt të prokurorit për të bashkëpunuar me drejtësinë. Vëreni se prokurori ia kishte dorëzuar kërkesën e tij për bashkëpunim Kompanisë YAHOO Inc.! nëpërmjet Internetit (!). Më pas Kompania YAHOO Inc.! u shpall e pafajshme nga Gjykata e Apelit të Gentit; pafajësia u anulua nga Gjykata Belge e Kasacionit, dhe mbas asaj Kompania YAHOO Inc.! u shpall e pafajshme nga gjykata e apelit e Brukselit. Çështja shkoi për herë të dytë në Gjykatën e Kasacionit. Ndërkohë, edhe Gjykatat e Apelit që deklaruan të pafajshme Kompaninë YAHOO Inc.! e deklaruan veten kompetente për kryerjen e procedimit gjyqësor të Kompanisë YAHOO Inc.!, edhe pse Kompania YAHOO Inc.! mund të konsiderohet virtualisht e pranishme në Belgjikë vetëm kur aktivizohet kompjuteri dhe i has ato në Internet. Me sa duket gjykatat ranë dakord që prokurori bëri takim me YAHOO Inc.! në zyrën e tij. Në 4 Shtator 2012, gjykata e kasacionit vendosi që: “*Rrethana që Prokurori dërgon nga Belgjika kërkesën e tij me shkrim, sipas kuptimit të Nenit 46bis të Kodit Belg të Procedurës Penale, ku kërkon bashkëpunimin e një operatori të një rrjeti të komunikimeve elektronike ose të shërbimofruesit të komunikimeve elektronike të vendosura jashtë territorit Belg, në një adresë të huaj, nuk e zhvlerëson kërkesën*.”  Ne jemi në favor të vendimeve dhe rregullave të gjera të kompetencës ,të cilat dematerializojnë parimet klasike të kompetencës territoriale. Kjo mënyrë të menduari është e domosdoshme për përballimin e realitetit virtual dhe krimit kibernetik në çështjet e drejtësisë.  Në shembullin e mësipërm e konsiderojmë policinë belge si kompetente territorialisht.  **A jemi kompetentë të mbledhim vetë prova në një shtet tjetër?**  Sapo të kemi deklaruar veten kompetentë për hetimin e një çështjeje dhe dërgimin e çështjes në gjykatë, është e rëndësishme që provat dixhitale të mund të mblidhen për të ndërtuar çështjen.  Përderisa kriminelët kibernetikë operojnë duke injoruar kufijtë ose në shumë raste nga kompjuterë jashtë shtetit ku duan të kryejnë krimin, është e qartë se më shumë prova do të gjenden në vendet e tjera sesa në vendin që dëshiron t’i nxjerrë kriminelët përpara gjykatës.  Pavarësisht nga të gjitha përpjekjet e bëra për të lehtësuar bashkëpunimin ndërkombëtar, në jetën reale, shpesh të përballuar me krimet ndërkufitare, ndihma e ndërsjellë juridike funksionon shumë ngadalë, nëse funksionon.  Deri tani komisionet e letërporosive kanë shumë punë për përgatitjen e letrave dhe shpesh nevojiten përkthime që duhet të bëhen. Në hapësirën kibernetike ku provat dixhitale janë shumë të paqëndrueshme (një shtypje e tastit “delete” dhe gjithçka humbet përgjithmonë) çdo sekondë ka rëndësi.  Krahas sa më sipër, komisionet e letërporosive kërkojnë faktin se një autoritet i huaj jo vetëm duhet të jetë i kontaktueshëm (preferueshmërisht 24/7), por gjithashtu duhet të jepet një përgjigje e shpejtë dhe tërësore. Sot fatkeqësisht nuk ndodh kështu në shumicën e rasteve.  Autoritetet Evropiane të zbatimit të ligjit më së shumti përballen me kompani dhe server që janë vendosur në SHBA, tokën e njerëzve të lirë. Jo vetëm shumë Shërbimofrues gjenden në SHBA (Yahoo!, Google, Microsoft...), por gjithashtu është dhe amendamenti i parë që përfshin lirinë e shprehjes që tërheq shumë njerëz për të vendosur përmbajtjen (e ligjshme dhe të paligjshme) në serverët e vendosur në SHBA.  Kur nevojitet vetëm informacion për abonentin, ose thjesht të dhënat e komunikimit (jo përmbajtja e të dhënave), marrëveshjet unilaterale ndërmjet autoriteteve lokale të zbatimit të ligjit dhe kompanive të vendosura në SHBA janë një rrugë e shkurtër e çmuar. Por kur kërkohet përmbajtja e të dhënave, duhet të ndiqen kanalet e zakonshme diplomatike dhe duhet të provohet një *“shkak i mundshëm”* (një figurë gjyqësore e panjohur në shumicën e vendeve Evropiane). Dërgohen shumë letërporosi dhe jo shumë prej tyre ekzekutohen me sukses.  Bashkëpunimi me shumë shtete të huaja të tjera, të vështira për tu ndërlidhur, tregon të njëjtat vështirësi.  Për rrjedhojë do të ishte shumë më e lehtë të sekuestroheshin të dhënat nga një vend i caktuar në Internet, në hapësirën kibernetike, pa u marrë me gjithë ato lloje të ndryshme ndihmash të ndërsjella.  Konventa e Budapestit për Krimin Kibernetik nuk deshi të shkonte aq larg akoma, por nuk përjashtoi që shtete të tjera anëtare mund të mendojnë në atë mënyrë. Legjislatori Belg bëri një ligj që është inovativ dhe ndihmon në marrjen e provave nga jashtë shtetit. Zgjidhja ligjore belge hap diskutimin dhe tregon se sa shpejt mund të sekuestrohen provat dixhitale dhe kriminelët kibernetikë mund të sillen në gjykatë. Zgjidhja belge shpesh përdoret dhe deri tani në gjykatë nuk ka hasur asnjë problem.  **Konventa e Budapestit për Krimin Kibernetik**  Në nenin 19.2 të Konventës së Budapestit për Krimin Kibernetik shkruhet:  *“Secila Palë duhet të miratojë masa të tilla legjislative dhe masa të tjera siç mund të jetë e nevojshme për të garantuar se aty ku autoritetet kërkojnë ose në mënyrë të ngjashme aksesojnë një sistem kompjuterik specifik ose pjesë të tij, në përputhje me paragrafin 1.a, dhe kanë arsye të besojnë se të dhënat e kërkuara ruhen në një sistem tjetër kompjuterik ose pjesë të tij në territorin e saj, dhe këto të dhëna janë ligjërisht të aksesueshme ose të disponueshme në sistemin fillestar, autoritetet duhet të jenë në gjendje të shtrijnë me shpejtësi kontrollin ose aksesin e ngjashëm në sistemin tjetër”*.  Me këtë nen Këshilli i Evropës pranoi se shpesh të dhënat nuk ruhen në kompjuterin e përdorur nga i dyshuari, por kompjuteri i të dyshuarit është vetëm një pikë aksesi tek të dhënat faktike që ruhen diku tjetër në një sistem kompjuterik tjetër. Këshilli i Evropës thekson se në këto raste, dhe deri në njoftimin pasues vetëm kur të dhënat janë të ruajtura në territorin e shtetit anëtar që po shqyrton çështjen, duhet të jetë e mundur që kontrolli i kompjuterit të parë të shtrihet me shpejtësi tek sistemi kompjuterik tjetër, i lidhur me të.  Kjo është e dobishme, por kur të dhënat janë të ruajtura në një shtet tjetër, kjo nuk shkon shumë larg.  Pra kur neni 19.2 i Konventës së Budapestit për Krimin Kibernetik flet vetëm për territorin e tij, neni 32 i Konventës së Budapestit për Krimin Kibernetik shkon një hap më tej:  *“Një mundet, pa autorizimin e Palës tjetër:*  *a. të aksesojë të dhëna kompjuterike (burim i hapur) të disponueshme publikisht, pavarësisht se ku ndodhen të dhënat gjeografikisht; ose*  *b. të aksesojë ose marrë, nëpërmjet një sistemi kompjuterik në territorin e saj, të dhëna kompjuterike të ruajtura tek një Palë tjetër, nëse Pala merr pëlqimin e vullnetshëm dhe të ligjshëm të personit, i cili ka autoritetin ligjor t’i zbulojë të dhënat Palës nëpërmjet atij sistemi kompjuterik”.*  Është shkruar qartësisht se informacioni ose të dhënat e aksesuara në një shtet (anëtar) tjetër mund të përdoren pa autorizimin e Palës tjetër vetëm kur të dhënat janë ose (1) të disponueshme publikisht ose (2) kur pëlqimi (i) i ligjshëm dhe (ii) i vullnetshëm është dhënë nga personi që ka (iii) autoritetin e ligjshëm për zbulimin e të dhënave.  Mjaft trishtueshëm, këto situata shpesh nuk ndodhin në hetimet penale. Kriminelët nuk priren të zbulojnë vullnetarisht provat që mund t’i fusin ata në burg. Është e kuptueshme se informacioni që u intereson autoriteteve të zbatimit të ligjit nuk është pothuaj kurrë i disponueshëm publikisht.  Është e qartë se për të bërë një mjet të dobishëm për luftën kundër krimit kibernetik, Këshilli i Evropës duhet të ketë zgjeruar mundësitë e mbledhjes së të dhënave nga jashtë shtetit. Me sa duket kjo është diskutuar por pa rezultate akoma.  Në raportin shpjegues jepet një moment nga diskutimi për vendosjen e kompetencës ndërkufitare:  *“293. Çështja se kur një Palë lejohet të aksesojë në mënyrë të njëanshme të dhëna kompjuterike të ruajtura tek një Palë tjetër pa kërkuar ndihmë të ndërsjellë është një çështje që hartuesit e Konventës e kanë diskutuar gjerësisht. Ka pasur shqyrtim të detajuar të rrethanave në të cilat mund të jetë e pranueshme që Shtetet të veprojnë në mënyrë të njëanshme dhe të rrethanave kur ato nuk munden të veprojnë kështu. Hartuesit në fund përcaktuan se nuk ishte akoma e mundur të përgatitej një regjim përfshirës detyrues ligjor që të rregullonte këtë pjesë. Pjesërisht, kjo vinte për shkak të një mungese të përvojës konkrete me situata të tilla deri tani; dhe pjesërisht, kjo vinte për shkak të kuptimit se zgjidhja e duhur shpesh dilte në rrethana të përcaktuara të rastit individual, duke e bërë të vështirë kështu formulimin e rregullave të përgjithshme. Së fundmi, hartuesit vendosën të përcaktojnë vetëm situatat e Nenit 32 të Konventës për të cilat të gjithë ranë dakord se veprimi i njëanshëm ishte i lejueshëm. U ra dakord të mos rregulloheshin situatat e tjera derisa të mblidhej përvojë dhe të mbaheshin diskutime të tjera në këtë drejtim. Në lidhje me këtë, Neni 39, paragrafi 3 parashikon se situatat e tjera as nuk autorizohen e as nuk përjashtohen.”*  Shkruhet qartësisht se ekziston nevoja për kompetencë ndërkufitare, por që nuk ishte akoma e mundur të gjendej një marrëveshje ndërmjet shteteve anëtare dhe ishte akoma shumë shpejt për shkak të mungesës së përvojës dhe kohës për të diskutuar.  Në lidhje me zgjidhjet e mundshme për këtë problem të kërkuara dhe ndoshta të gjetura nga shtetet anëtare, u shkruajt se zgjidhjet e tjera në atë pikë as nuk autorizoheshin dhe as nuk përjashtoheshin.  **Zgjidhja Belge: Neni 88 i Kodit Belg të Procedurës Penale**  Një vit përpara nënshkrimit të Konventës së Budapestit për Krimin Kibernetik në 23 Nëntor 2001, legjislatori Belg miratoi Ligjin për Krimin Informatik në 28 Nëntor 2000; dhe nenin 88 të Kodit të Procedurës Penale (KBPP).  Aty ku ligji belg i vitit 2000 solli legjislacionin belg në linjë me Konventën e Budapestit për Krimin Kibernetik që duhej nënshkruar, neni 88 i KBPP ishte një përgjigje ndaj neneve të sipërpërmendura 19.2 dhe 32 të Konventës së Budapestit për Krimin Kibernetik.  Neni 88 i KBPP i lejon një gjyqtari hetues (ky është gjyqtar me detyrën e posaçme të drejtimit të hetimit dhe me kompetenca të posaçme investigative), që kur ai urdhëron të bëhet kontroll në një sistem kompjuterik të caktuar, të shtrihet kërkimi edhe tek një sistem tjetër kompjuterik ose tek një pjesë e një sistemi tjetër kompjuterik të ndodhur diku tjetër.  Kjo kompetencë vjen me kushte. Gjyqtari investigativ mund të vendosë për këtë kompetencë vetëm kur (1) është e domosdoshme të gjendet e vërteta në një hetim dhe (2) kur (i) masa të tjera hetimore nuk janë proporcionale (për shembull duhet të autorizohen urdhra kontrolli të ndryshëm për vendndodhje të ndryshme) ose (ii) ka një risk të qartë se provat do të zhduken (në çështjet kibernetike është një kusht që pothuaj gjithmonë përmbushet sepse provat dixhitale janë shumë të paqëndrueshme (tasti delete)).  Meqë legjislatori Belg preokupohej për faktin se policia do të shkonte shumë larg dhe shumë lehtë (për shembull nga llogaria bankare e një të dyshuari tek të gjitha llogaritë bankare në të njëjtën bankë), u shtua një kusht shtesë në kuptimin që Gjyqtari Investigativ duhet të kufizonte kontrollin e zgjeruar tek pjesa e sistemit tjetër kompjuterik, tek i cili kanë akses përdoruesit e sistemit fillestar (ky kusht përmbushet më së shumti ku Gjyqtari Investigativ lejon policinë të shkojë tek një kompjuter tjetër me të dhënat e aksesit dhe fjalëkalimin e të dyshuarit; këto të dhëna dhe fjalëkalimi përcaktojnë kufizimin e aksesit).  Mbas kontrollit të zgjeruar, personi përgjegjës për sistemin kompjuterik duhet të informohet nga Gjyqtari Investigativ nëse ai/ajo mund të identifikohet në mënyrë të arsyeshme (në shumë raste nuk ndodh kështu).  Por pjesa më inovative e nenit 88 të KBPP qëndron tek nënseksioni i paragrafit 3 të nenit që thotë se kur duket se të dhënat që zbulohen nuk ruhen në territorin Belg, këto të dhëna vetëm kopjohen. Kur ndodh kjo Gjyqtari Investigativ duhet vetëm të informojë Ministrinë e Drejtësisë nëpërmjet Prokurorisë së Përgjithshme; Ministria e Drejtësisë informon Shtetin në fjalë, nëse mund të përcaktohet (shpesh nuk ndodh kështu).  Në përputhje me nenin 39 të KBPP, të dhënat e kopjuara janë po aq të vlefshme përpara gjykatës po aq sa të dhënat origjinale (të dhënat nuk sekuestrohen fizikisht, por konsiderohen si të sekuestruara).  Në çështjen si shembull, kjo do të thotë se policia Belge mund të mbledhë prova nga kompjuterët Belg (jo domosdoshmërisht kompjuteri i të dyshuarit) dhe të shkojë prej aty tek serverët e vendosur në Gjermani, SHBA, Kazakistan, në pjesën tjetër të botës... Ata mund të fillojnë ekzaminimin e llogarisë bessermit8@hotmail.com, në momentin që kanë të dhënat e hyrjes dhe fjalëkalimin.  Ky është qartësisht një avantazh me qëllim ruajtjen e kohës së çmuar dhe me qëllim që të mos humben provat dixhitale ndërkohë që bëhen shkresat.  Duhet të theksohet se sado të fuqishme duken në pamje të parë instrumentet e nenit 88 të KBPP, puna e policisë mbetet po aq e rëndësishme. Pa gjurmët e të dhënave dhe fjalëkalimeve, për shembull të zbuluara nga një përgjim i zakonshëm, llogaria [bessermit8@hotmail.com](mailto:bessermit8@hotmail.com) në hotmail nuk do të ishte e aksesueshme përveçse kur ligji të ofron mundësinë ligjore të hysh pa lejen e përdoruesit në llogarinë e tij.  Megjithatë zgjidhja Belge ofron mundësi të mëdha për trajtimin e të dhënave të ruajtura në “re”. Meqë kompanitë dhe individët privatë po ruajnë jo vetëm të dhëna por edhe sisteme në “re” dhe për pasojë as vetë nuk e dinë si ruhen ekzaktësisht të dhënat apo në cilin vend ndodhen të dhënat, zgjidhja Belge e bën të qartë se nuk është e rëndësishme të dihet se *ku* ruhen të dhënat, por *nga ku* janë të aksesueshme ato.  Një qasje klasike ndaj kompetencës territoriale për marrjen e provave do të paralizonte tërësisht çdo hetim, kur vetëm deklarimi i të dyshuarit se ai/ajo vetë nuk e di se në cilin shtet ruhen të dhënat do të bënte që të ndërpritej çdo veprim i mëtejshëm.  **Konkluzionet?**  Është shumë e qartë se me Internetin erdhi dhe globalizimi i krimit (kibernetik). Nëse autoritetet kompetente dëshirojnë të luftojnë krimin kibernetik dhe nuk duan të ndalojnë në ndonjë kufi hipotetik, janë të nevojshme rregullat për kompetencën. Kjo bën të domosdoshme pasjen e marrëveshjeve të qarta ndërkombëtare në lidhje me se çfarë të bëhet nëse më shumë se një shtet e konsideron veten kompetent për të vajtur në gjykatë.  Krahas kësaj, ekziston nevoja për rregulla të qarta ligjore për të qenë në gjendje të merren me shpejtësi provat e ruajtura jashtë shtetit. Në ditët e sotme, përvojat e përditshme personale nuk duken premtuese. Për këtë arsye, është i nevojshëm një përpunim i mëtejshëm i neneve 19.2 dhe 32 të Konventës së Budapestit për Krimin Kibernetik. Ndërkohë vijnë në ndihmë zgjidhjet e dhëna nga shtetet. Zgjidhja Belge e përcaktuar në nenin 88 të KBPP mund të përdoret si shembull sesi të merren me shpejtësi provat dixhitale.  Është e qartë se në një kontekst të krimit kibernetik, duhet të zbatohet një qasje tjetër. Krimi kibernetik nuk ka kufij. Ofrimi i shërbimeve në distancë dhe ruajtja e informacioni në Internet e bëjnë akoma dhe më të vështirë të kuptohet se ku ruhen të dhënat (apo pjesë të tyre). Një qasje klasike e sovranitetit dhe kufijve duhet të konsiderohet si mure betoni që bëjnë luftën kundër krimit kibernetik të pamundur. Duhet të bëhen zgjedhje politike.  RUFR8?  Belgjikë, Prill 2012 (azhurnuar në Shtator 2012)  Prezantimi është i rëndësishëm sikur nga këndvështrimi i avokatëve, gjyqtarëve dhe më e rëndësishmja nga këndvështrimi i prokurorëve juria t’iu japë provave të specializuara peshën që meritojnë. Prokurorët duhet të marrin në konsideratë natyrën, vendin dhe volumin e materialit që do të përdorin si provat për mbrojtjen e interesave të klientëve të tyre në Gjykatë, të planifikojnë sesi do ta prezantojnë këtë material, dhe së fundmi të prezantojnë të gjitha çështjet përpara fillimit të procedurës në mënyrë që materiali të jetë i menaxhueshëm.  Prezantimi i provave elektronike gjyqtarit dhe jurisë (në sistemet adversare) nevojitet të jetë vizual, duke përdorur demonstrimet kompjuterike, grafikat kompjuterike, demonstrimin me video, programet dhe tabelat. Prokurorët duhet të jenë të ndërgjegjshëm për paragjykimin që krijohet nga përdorimi i teknologjisë, dhe duhet të jenë gati të diskutojnë këto çështje me autoritet nëse mbrojtja e kundërshton përdorimin e një teknologjie të tillë.  Kërkimet kanë zbuluar se njerëzit i kushtojnë më shumë vëmendje asaj që shohin sesa asaj që dëgjojnë. Meqë detyra e prokurorit është të çojë përpara çështjen në mënyrën më të mirë të mundshme, për rrjedhim duhet të realizojmë një prezantim vizual të provave veçanërisht në çështje të komplikuara; për shembull duke përdorur demonstrimet kompjuterike.  **Provat do të kundërshtohen: jini të përgatitur**  Një nga gjërat më të rëndësishme për të ditur është fakti se të gjitha provat do të kundërshtohen. Jo vetëm nga avokatët mbrojtës, por gjithashtu edhe gjatë shqyrtimit nga gjyqtari. Gjyqtari duhet ta shohë se provat janë mbledhur në mënyrë korrekte, janë të besueshme dhe nëse nuk ka shkaqe ligjore për përjashtimin e provave nga vendimmarrja.  Jo çdo provë lejohet të përdoret në gjykatë. Shumë gjera varen nga sistemi ligjor, përsa i takon legjislacionit që rregullon mbledhjen e provave dhe jurisprudencën për këtë temë në vendin tuaj. Në disa vende ekzistojnë rregulla specifike në Kodin e Procedurës Penale që mund të shkaktojnë pavlefshmërinë e provave. Në disa vende të tjera provat në çështjet penale janë tërësisht të lira dhe i takon palëve të përfshira në proces të diskutojnë përpara gjyqtarit për provat dhe se ç’duan të bëjë gjyqtari me to. Disa shtete kombinojnë dy qasjet e mësipërme të trajtimit të provave.  Është e kuptueshme që avokatët mbrojtës do të bëjnë çmos që t’i shpjegojnë Gjyqtarit se provat nuk janë të besueshme ose janë marrë në mënyrë të paligjshme. Është detyra e tyre ta bëjnë këtë. Nuk do të ishte me mënd të mendohet se çështjet e ngritura nga mbrojtja mund të zgjidhen lehtësisht në momentin që do të jemi në gjykatë. Sigurisht është e rëndësishme të jesh i përgatitur për gjykatë dhe të jesh i përgatitur dhe në gjendje të demonstrohet logjika dhe ligjshmëria e veprimeve dhe sesi u mblodhën provat. Është akoma më e rëndësishme që të kujdesemi madje përpara se çështja të shkojë në gjykatë, që të jemi të përgatitur të përballemi me të gjitha sfidat që avokatët mbrojtës mund të ngrenë gjatë debateve gjyqësore. Sigurohuni se punonjësit e policisë dhe ekspertët që thirren si dëshmitarë të jenë të përgatitur për t’ju përgjigjur të gjitha pyetjeve të mbrojtjes. Në gjykatë shansi favorizon mendjen e përgatitur.  Është shumë e rëndësishme që prokurori të jetë në dijeni të çdo dobësie ose kufizimi të provave që paraqiten. Prokurori nevojitet të jetë në dijeni të çdo shpjegimi alternativ, jo thjesht më të mirin, ose atë që shpresonte të dëgjonte.  Duhet të inkurajohet ideja që edhe prokurorët dhe gjyqtarët janë në gjendje të trajtojnë çështjet teknike të kriminalistikës, kështu që të mund të përballen me çështjet në këtë fushë të ngritura nga avokatët mbrojtës.  Hetuesit, prokurorët, përfaqësuesit e mbrojtjes, gjyqtarët dhe juritë, të gjithë duhet të kuptojnë informacionin dhe teknologjinë. Çështjet mund të dështojnë nëse prokurori nuk është në gjendje të identifikojë çështjet që nevojitet të vendosen në një çështje gjyqësore dhe ta paraqesë atë çështje në mënyrë të thjeshtë dhe precize përpara gjykatës, veçanërisht nëse ka të përfshira aty aspekte teknike. Prokurorët dhe hetuesit duhet të trajnohen dhe pajisen me aftësi dhe njohuri të specializuara për hetimin dhe ndjekjen ligjore, veçanërisht kur kemi të bëjmë me teknologji të reja.  Prokurorët duhet të mësojnë sesi funksionojnë kompjuterët dhe shërbimet e Internetit; të kuptojnë raportet e ekspertëve dëshmitarë dhe të jenë në gjendje të japin konsulencë (dhe instruksione në disa juridiksione) policisë në lidhje me hetimin, dhe të mbikëqyrin mbledhjen dhe mbrojtjen e integritetit të provave dixhitale në përputhje me parimet për sekuestrimin e provave dixhitale edhe brenda edhe jashtë juridiksionit.  Një çështje e përgatitur mirë ka një numër përfitimesh; është e rëndësishme që edhe prokurori edhe hetuesi të kuptojnë se çfarë është në fakt çështja e tyre.  Vetëm atëherë prokurori do të jetë në gjendje të mbrojë provat e kundërshtuara në gjykatë.  Nëse jo vetë provat, mund të kundërshtohet personi që i mblodhi ato dhe mënyra sesi u mblodhën.  Zyrtarët e policisë që duhet të dëshmojnë në gjykatë duhet të kuptojnë se kur provat flasin vetë dhe kur ato inkriminojnë të dyshuarin, rruga e fundit për mbrojtjen do të jetë sulmi direkt i personit që i mblodhi provat dhe mënyra në të cilën ai/ajo e realizoi këtë.  Sigurisht në sistemet juridike anglo-saksone, kundërpyetja e oficerëve të policisë është një pjesë e rëndësishme e procesit të të provuarit përpara gjykatës. Në sistemet juridike kontinentale kjo realizohet më pak. Sigurisht që duhet të kuptojnë se sa më shumë prova të kundërshtohen aq më shumë të ngjarë ka që të bëhet ekzaminimi i ekzaminuesve.  Më tej në këtë prezantim do të trajtojmë karakteristikat specifike të provave dixhitale. Dhe në këtë pikë do të bëhet më e qartë se ka shumë për të sfiduar…  **Neni 6 KEDNJ – E Drejta për një Proces të Rregullt**  Neni 6 i Konventës Evropiane për të Drejtat e Njeriut përcakton se gjithë duhet të gëzojnë të drejtën për një proces të rregullt dhe shpjegon se çdo të thotë kjo.  NENI 6 KEDNJ: E Drejta për një Proces të Rregullt:  1. Çdo person ka të drejtë që çështja e tij të dëgjohet drejtësisht, publikisht dhe brenda një afati të arsyeshëm nga një gjykatë e pavarur dhe e paanshme, e krijuar me ligj, e cila do të vendosë si për mosmarrëveshjet në lidhje me të drejtat dhe detyrimet e tij të natyrës civile, ashtu edhe për bazueshmërinë e çdo akuze të natyrës penale që i është drejtuar. Vendimi duhet të jepet publikisht, por prania në sallën e gjykatës mund t’i ndalohet shtypit dhe publikut gjatë tërë procesit ose gjatë një pjese të tij, në interes të moralit, të rendit publik ose të sigurimit kombëtar në një shoqëri demokratike, kur kjo kërkohet nga interesat e të miturve ose mbrojtja e jetës private të palëve në proces ose në shkallën që çmohet tepër e domosdoshme nga gjykata, kur në rrethana të veçanta natyra e publicitetit do të dëmtonte interesat e drejtësisë.  2. Çdo person i akuzuar për një vepër penale prezumohet i pafajshëm, derisa fajësia e tij të provohet ligjërisht.  3. Çdo i akuzuar për një vepër penale ka, së paku,të drejtat e mëposhtme:  (a) të informohet, brenda një afati sa më të shkurtër, në një gjuhë që ai e kupton dhe në mënyrë të hollësishme, për natyrën dhe për shkakun e akuzës që ngrihet ndaj tij;  (b) t’i jepet koha dhe lehtësitë e përshtatshme për përgatitjen e mbrojtjes;  (c) të mbrohet vetë ose të ndihmohet nga një mbrojtës i zgjedhur prej tij dhe, në qoftë se ai nuk ka mjete për të shpërblyer mbrojtësin, t’i mundësohet ndihma ligjore falas nga një avokat i caktuar, kryesisht kur këtë e kërkojnë interesat e drejtësisë;  (d) të pyesë, ose të kërkojë që të merren në pyetje dëshmitarët e akuzës dhe të ketë të drejtën e thirrjes dhe të pyetjes të dëshmitarëve në favor të tij, në kushte të njëjta me dëshmitarët e akuzës;  (e) të ndihmohet falas nga një përkthyes, në qoftë se nuk kupton ose nuk flet gjuhën e përdorur në gjyq.  Shkurt, kjo do të thotë se kur dikush ndiqet ligjërisht dhe kur ky person përballet me gjykim në gjykatë, ai/ajo duhet të ketë mundësinë të kuptojë për çfarë po ndiqet ligjërisht dhe duhet gjithashtu të ketë mundësinë dhe lehtësirat për përgatitjen e mbrojtjes së tij dhe të kundërshtojë jo vetëm dëshmitarët por të gjitha provat që janë kundër tij. Varet nga shteti në shtet sesi është organizuar kjo dhe se në cilën kohë i paraqitet mbrojtjes (avokatëve).  **Si të paraqiten provat në gjykatë?**  Edhe kur ndiqni bazat e strategjisë së procesit gjyqësor, duhet prapëseprapë të mbani parasysh se **jo të gjithë në sallën e gjyqit kanë të njëjtën ekspertizë**.  Kur filloni të prezantoni çështjen tuaj, duhet të ndërtoni provat mbi baza solide: sigurohuni që të dokumentoni çdo hap dhe tregoni logjikën e ngjarjeve përpara se t’i tregoni provat gjyqtarit. Mbani parasysh thirrjen e ekspertëve dëshmitarë që janë në gjendje të përkthejnë ekzaminimet kriminalistike në gjuhën e zakonshme. Si kujtesë, kjo është në përputhje me të gjitha kriteret e nenit 6 të Konventës Evropiane të të Drejtave të Njeriut.  Mos harroni të mësoni së pari të ecni përpara se të vraponi. Së pari shpjegoni bazat (ndoshta duke përdorur një prezantim me Power Point, ose një leksikon) dhe më pas kaloni në pjesën e vështirë të kriminalistikës (nuk ka asnjë dobi të përpiqeni të bindni një gjyqtar në lidhje me provat e teknologjisë së lartë, kur gjyqtari nuk e ka idenë se çdo të thotë një adresë IP).  **Ndërtoni çështjen duke u nisur nga niveli i gjyqtarit**.  **Mos provokoni debate**  Ligjshmëria e ndjekjes ligjore prezumohet në shumicën e vendeve të Evropës Kontinentale. Kjo gjë mund të jetë e ndryshme në vendet anglo-saksone.  Sigurisht gjyqtari zyrtarisht duhet të ekzaminojë të gjitha aspektet e pranueshmërisë së akuzës.  Në varësi të ligjit kombëtar për Provat, pranueshmëria dhe ligjshmëria e provave duhet të përfshihen në aktakuzë.  Nëse ligji kombëtar nuk ua kërkon që të provoni ligjshmërinë dhe/ose pranueshmërinë e provave ose mbledhjen e tyre, mos e bëni ju vetë; mund të ngacmoni avokatët mbrojtës që ta ngrenë në diskutim.  **Vendosni ritmin**  Bëni një plan procedimi. Mendoni për linjën kryesore dhe bazën e procedimit. Përqendrohuni tek baza.  Përmbajuni planit, dhe mos lejoni që avokatët mbrojtës t’ju ç’orientojnë.  Mbrojtja më shumë mundësi e ka një plan mbrojtjeje. Nëse mbrojtja arrin t’ju bëjë që të shkoni pas planit të saj, e ka arritur gjysmën e suksesit.  Qëndroni në vijën kryesore, mos i lejoni t’ju mënjanojnë që të humbisni dhe ngatërroheni në detaje pa rëndësi që do ta ç’orientonin gjyqtarin.  Mos bini pre e provokimeve. Qëndroni të qetë dhe gjithmonë kthejuni planit; modifikojeni vetëm kur duhet domosdoshmërisht.  Përcaktoni ritmin. Përpiquni të përvetësoni kadencën e procedurës. Përpiquni të vendosni ritmin dhe menaxhoni axhendën procedurale.  Për shembull: nëse mbrojtja provokon një shtyrje me anë të dorëzimit të deklaratave me shkrim/konkluzioneve në momentin e fundit, ju duhet të merrni parasysh të mos kërkoni shtyrje për të studiuar deklaratën e tyre. E nesërmja nuk vjen kurrë.  **Specialistët e kriminalistikës dixhitale si dëshmitarë**  Hetuesi ose prokurori mund të ketë nevojë që të mbajë një specialist të kriminalistikës gjatë një hetimi. Kjo mund të jetë e nevojshme sepse kërkohet një lloj specifik specializimi, për shembull njohuri për një sistem të caktuar operativ ose një program Interneti.  Çështja kryesore që do përgjigje në përzgjedhjen e një dëshmitari është nëse ata kanë njohuritë e kërkuara që janë fituar me studim ose përvojë për ta bërë mendimin e tyre të vlefshëm në zgjidhjen e çështjeve.  Një lloj akreditimi mund të jetë i dobishëm sepse rrit kredibilitetin e dëshmitarëve kriminalistë të thirrur edhe nga akuza edhe nga mbrojtja, si dhe dhënia e një vlerësimi të pavarur dhe objektiv të kredencialeve të ekspertëve mbi të cilët do të mbështetet gjykata.  Janë thelbësore konsultimet e hershme ndërmjet oficerëve investigativ, specialistëve dëshmitarë dhe prokurorit për një hetim dhe procedim të suksesshëm. Policia dhe prokurorët duhet të garantojnë që ekzaminuesit kriminalistik ti jepen udhëzime të qarta. Hetuesit duhet të japin axhenda të sakta dhe të detajuara.  Përzgjedhja e dëshmitarëve të jashtëm konsultativ, me shumë mundësi në zonat e pazakonta ose shumë teknike, mund të jetë problem për hetuesin. Procesi i përzgjedhjes nuk duhet të jetë kuturu, por aktiv dhe i strukturuar që nga fillimi. Njësitë e krimit kibernetik mund të jenë në gjendje të ofrojnë më shumë konsulencë në lidhje me kriteret e përzgjedhjes.  Udhëzimet e mëposhtme duhet të përfshihen në realizimin e përzgjedhjes dhe fushat e mëposhtme konsiderohen të jenë baza e aftësive konsultative të pavarura për dëshmitarët.  **Ekspertizë e Specializuar**  Kjo është një aftësi apo zotësi për të bërë një punë të caktuar, dhe përfshin çështje të tilla si:  a. Kualifikimet përkatëse të personit.  b. Aftësinë e personit në këtë punë specifike.  c. Aftësitë specifike që ka.  d. Nëse aftësia bazohet në kualifikimet teknike ose kohëzgjatjen e përvojës, ose të dyja.  **Përvoja e Specializuar**  a. Natyra e përvojës së këtij lloji pune që ka individi.  b. Numri i çështjeve që është përfshirë ai/ajo.  c. Lloji i çështjeve në të cilat është përfshirë individi.  d. Sasia e kohës që individi ka punuar në këtë fushë.  e. Provat për të provuar përvojën.  **Njohuri Investigative**  Kuptimi i natyrës së hetimeve në drejtim të konfidencialitetit, lidhjes dhe dallimit ndërmjet:  a. Të dhënave.  b. Informacionit të përpunuar (rrjedhim i analizave)  c. Provave.  **Njohuri Kontekstuale**  Kuptimi i qasjeve të ndryshme, gjuhëve, filozofive, praktikave dhe roleve të policisë, ligjit, dhe njohuritë teknike të Teknologjive të Informacionit është esenciale për garantimin e qëndrueshmërisë së provave elektronike në Gjykatë. Themelore për këtë është të kuptuarit e probabilitetit në kuptimin e tij më të gjerë dhe ndryshimet ndërmjet provave shkencore dhe provave ligjore.  **Njohuritë Juridike**  Të kuptuarit e aspekteve përkatëse të tilla si konceptet dhe procedurat ligjore në lidhje me to:  a. Deklaratat.  b. Vazhdimësinë.  c. Procedurat Gjyqësore.  d. Një kuptim të qartë të roleve dhe përgjegjësive të ekspertëve dëshmitarë është thelbësor.  **Aftësitë e Komunikimit**  Aftësia për të shprehur dhe shpjeguar në gjuhën e zakonshme, edhe me gojë edhe me shkrim:  a. Natyra e specializimit.  b. Teknikat dhe pajisjet e përdorura.  c. Metodat e interpretimit.  d. Pikat e forta dhe pikat e dobëta të provave.  e. Shpjegimet alternative.  **Të Përgjithshme**  a. Me autoritetin deri në nivelin e duhur për të administruar materialet provuese.  b. I ndërgjegjshëm për çdo udhëzim në lidhje me materialet përkatëse për pedofilinë.  c. I ndërgjegjshëm për efektin mbi anëtarët e stafit të këtij materiali dhe vlerësimit të duhur të riskut.  **Roli i ekspertit**  Shihni kapitullin 9.3.2 të Guidës së këshillit të Evropës për Provat Elektronike.  Në proceset gjyqësore penale është e mundur të lejohet mendimi i një eksperti ku çështjet që duhet të zgjidhë gjykata janë larg përvojës dhe njohurive të gjykuesit. Kur një çështje kërkon prova të tilla, vetëm një ekspert i kualifikuar siç duhet mund t’i paraqesë ato.  Nuk ka asnjë kriter specifik për kualifikimet e ekspertëve si dëshmitarë. Ajo që kërkohet është që eksperti, për shkak të përvojës së tij, studimeve ose të dyjave, të mund të japë mendimin e tij të vlefshëm për një çështje që gjykata nuk mund ta zgjidhë vetëm. (Ky pozicion është i ndryshëm në një numër vendesh Evropiane).  Një ekspert dëshmitar duhet gjithashtu të jetë i pavarur dhe i paanshëm. Një dëshmitar ka detyrim ndaj gjykatës, jo ndaj klientit. Ai/ajo duhet të identifikojë dhe sjellë në vëmendje çdo dobësi ose kufizim për provat që do paraqiten. Prokurori duhet të jetë i ndërgjegjshëm për çdo shpjegim alternativ, jo thjesht më të mirin, ose shpjegimin që prokurori shpresonte të dëgjonte. Deklarimet e ekspertëve duhet të jenë sa më të thjeshta që të munden, me fotografi.  Eksperti i kriminalistikës si dëshmitar është një dëshmitar ekspert nëse çmohet i tillë nga gjyqtari mbas dëgjimit të kualifikimeve dhe përvojës së dëshmitarëve. Pavarësisht se cila nga palët në proces e ka udhëzuar atë, eksperti dëshmitar është shërbyes i gjykatës dhe është aty për të ndihmuar gjykatën të kuptojë provat komplekse, që janë jashtë përvojës së zakonshme të gjykatës.  Kur edhe prokuroria edhe mbrojtja kanë një ekspert kriminalistik si dëshmitar, dëshmitarët do të lejohen të japin opinionin e tyre të specializuar për faktet e çështjes. Kjo është në kontrast me të gjithë dëshmitarët e tjerë, që zakonisht japin dëshmi vetëm për atë që kanë parë personalisht. Ekspertët si dëshmitarë do të paguhen zakonisht nga pala që i thërret dhe pritet që të kenë shkëmbyer raportet, të kenë rënë dakord për çështjet që nuk janë në konflikt dhe të kenë rënë dakord për një fjalorth termash.  Ka një numër në rritje çështjesh që përfshijnë provat elektronike të ruajtura në sisteme kompjuterike ose në pajisje të tjera. Gjyqtarët (si prokurorët dhe hetuesit) duhet të jenë të përgatitur të përballen me krimin kibernetik dhe provat elektronike. Në shumicën e çështjeve, gjyqtarët (si prokurorët dhe hetuesit) hasin vështirësi në përballjen me këtë realitet të ri të botës kibernetike dhe duhet të trajnohen për njohuritë dhe të kuptuarin e krimit kibernetik dhe të provave elektronike. Ata duhet gjithashtu ta vazhdojnë zhvillimin e tyre profesional në mënyrë të pavarur. Për këtë arsye, gjyqtarët dhe prokurorët duhet të inkurajohen të kontribuojnë për rritjen e njohurive dhe përvojës së tyre nëpërmjet lidhjes në rrjet në vend dhe jashtë shtetit me gjyqtarët dhe prokurorët e tjerë.  **Mendoni për mënyrat e prezantimit**  Si një prokuror apo hetues i krimit kibernetik, mos harroni të përdorni instrumentet që na solli ICT.  Kini parasysh një prezantim me power point për ta bërë çështjen “të gatshme”, ofroni një fjalorth ku të jenë përkufizuar të gjitha termat specifike dhe teknike, ofroni një përmbledhje të çështjes për ta bërë historinë të lexueshme dhe së fundmi tregoni provat. Gjithashtu, kini parasysh të bëni një shpjegim të shkurtër të teknologjisë/provave elektronike të çështjes, të vendosni një standard për të gjithë ata në gjykatë, kështu që të paktën ata të kenë një shans të kuptojnë çështjen.  **Gjërat për tu mbajtur në konsideratë kur e lejon sistemi ligjor dhe mjetet në dispozicion**  Siç u përmend ka një diferencë të madh ndërmjet sistemit inkuizitor dhe sistemit adversar. Në sistemin adversar, çdo gjë ndodh në gjykatë, përpara gjyqtarit dhe jurisë; ata me siguri nuk kanë asnjë njohuri paraprake për çështjen. Ju duhet të rregulloni metodat e prezantimit në përputhje me situatën.  **Demonstroni një foto/sistemin e të dyshuarit në gjykatë për të demonstruar prezencën e provave në sistem ose për të qenë në gjendje të tregoni sesi u krye krimi**  Disa mënyra prezantimi që sugjerohen nuk përdoren ose përdoren rrallë në një gjykatë të sistemit inkuizitor. Në një procedurë inkuizitore e gjithë mbledhja e provave dhe mostrat e provave tregohen dhe përshkruhen në raportet e policisë. Nëse një avokat dëshiron të kundërshtojë raportet, ai shkon tek regjistrimi dhe kërkon akses tek provat e sekuestruara, e cila i lejohet. Ai/ajo do të kontrollojë nëse mund të gjejë një argument për kundërshtim. Nëse jo, ai/ajo kurrë nuk do të ngrejë çështjen e “tregimit dhe demonstrimit” të provave në gjykatë. Në një procedurë inkuizitore, ne zakonisht nuk do të marrim në konsideratë tregimin e sistemit të të dyshuarit për të treguar se ç’ka në të ose për të treguar sesi u krye krimi; kjo gjë është në raportet e policisë, dhe nuk ka asnjë juri pa njohuri paraprake që duhet të bindni.  **Paraqitjani provat palëve duke i demonstruar në monitor**  Do të ishte ëndërr që çdokush në gjykatë të kishte kompjuter, por për momentin kjo nuk është e mundur në gjykatat e sistemit inkuizitor. Prezantimet e çështjeve/provave bëhen me mjete konvencionale siç përshkruhet në slajdet e mëparshme (një prezantim me power point dhe/ose një projektor (nëse keni ndonjë regjistrim për të demonstruar)), nëse mund të ketë ndonjë vlerë të shtuar me qëllim që të jepni një përmbledhje apo vështrim të përgjithshëm të çështjes). Në shumicën e çështjeve, prokurori e paraqet çështjen me gojë. Në një gjykatë të sistemit inkuizitor, nganjëherë deri në 20 çështje duhet të trajtohen deri përpara mesditës... | |
|  | **Ushtrime Praktike (nëse ka)** Nuk ka asnjë ushtrim praktik për këtë sesion. | |
|  | **Kontrolli i Njohurive**  Për këtë kurs nuk është parashikuar asnjë kontroll specifik i njohurive krahas atij të renditur më lart. | |

|  |  |  |
| --- | --- | --- |
| Mësimi: 1.2.5–Punë në Grup – Finalizimi i çështjes | | **Kohëzgjatja: 60 Minuta** |
| **Burimet materiale të kërkuara:**   * Një sallë e përshtatshme për një numër të parashikuar pjesëmarrësish. Kjo sallë duhet të rregullohet duke vendosur një tryezë të rrumbullakët për çdo grup, ku është e mundur, bazuar në një numër prej 6 pjesëmarrësish në grup. * Kompjuter tavoline/laptop me Windows 7 ose 8 dhe me Programin MS Office Professional të instaluar * Projektor dhe ekran për shfaqje imazhesh * Akses në Internet (nëse është i disponueshëm) * Kopje të Guidës për Provat Elektronike të Këshillit të Evropës * Dërrasë të Bardhë për secilin grup * Markera për Dërrasë të Bardhë (të paktën 2 për secilën ngjyrë: blu, të zezë, të kuqe dhe jeshile) për secilin grup * 1 Tabelë Flipchart me letër të mjaftueshme për secilin grup * Stilolapsa dhe blloqe për pjesëmarrësit * Kapëse aktesh, vrimahapëse dhe gërshërë për secilin grup * Ngjitës Blu ose një produkt të ngjashëm me të për ngjitjen e përkohshme të letrës në mure për secilin grup * Një kompjuter laptop për secilin grup të ngjashëm me kompjuterin e trajnerit dhe me akses në Internet që të realizohen kërkimet hetimore. * Të gjitha materialet mbështetëse të dhëna me paketën e trajnimit. | | |
| **Synimi:** Ky sesion është hartuar t’i lejojë pjesëmarrësit të organizojnë të gjitha provat në një mënyrë që do të realizojë një çështje bindëse kundër të akuzuarve. Ata do të ekzaminojnë pranueshmërinë e provave të mbledhura si dhe do të sigurohen se provat janë mbledhur në përputhje me legjislacionin dhe praktikën e mirë kombëtare dhe ndërkombëtare. | | |
| **Objektivat:**  Në përfundim të këtij sesioni pjesëmarrësit do të jenë në gjendje të:   * Shqyrtojnë të gjitha aspektet në menaxhimin e ndjekjes ligjore. * Garantojnë integritetin e provave të marra nga jashtë shtetit. * Vërtetojnë se nuk ka pengesa për pranueshmërinë e provave të mbledhura. * Thërrasin dëshmitarë nga juridiksionet e tjera gjatë procedimit gjyqësor. * Garantojnë pajtueshmërinë me KEDNJ dhe dispozitat e tjera. | | |
| **Nr. i Slajdit** | **Përmbajtja:** | |
|  | Nuk ka prezantim të lidhur me këtë sesion. | |
|  | **Ushtrime Praktike (nëse ka)**  Ky sesion është tërësisht praktik në natyrë dhe grupet do të punojnë së bashku me provat që janë mbledhur për të përgatitur dosjen e çështjes për prezantim përpara grupit të trajnimit. Trajneri duhet të sigurohet se pjesëmarrësit i kanë marrë në konsideratë të gjitha provat dhe të identifikojë ndonjë çështje të mbetur që do të kërkonte vëmendje.  Gjatë këtij sesioni të gjitha provat do t’i bëhen të disponueshme pjesëmarrësve, edhe sikur ata të mos identifikojnë disa pjesë të tyre gjatë hetimit. Në varësi të kohë së disponueshme, secili grup pune duhet të hartojë një raport të shkurtër ku të detajojë gjetjet e tij. Në çdo rast, secili grup duhet të japë një prezantim për të tjerët ku të detajojë çështjet kryesore dhe mësimet e mësuara si rezultat i ushtrimeve praktike. | |
|  | **Kontrolli i Njohurive**  Për këtë kurs nuk është parashikuar asnjë kontroll specifik i njohurive krahas atij të renditur më lart. Nuk është kërkuar asnjë vlerësim zyrtar. | |

|  |  |  |
| --- | --- | --- |
| **Mësimi Nr: 1.2.6 – Mbyllja e Kursit** | | **Kohëzgjatja: 60 Minuta** |
| **Burimet materiale të kërkuara:**   * Kompjuter Laptop ose Kompjuter Tavoline me Windows 7 dhe me Office 2010 * Projektor * Prezantim me PowerPoint * Formularët e vlerësimit të pjesëmarrësve | | |
| **Synimi:**  Ky sesion është hartuar t’i lejojë pjesëmarrësve të japin vlerësimet e tyre për kursin dhe të ndihmojë trajnerin në identifikimin e çdo përmirësimi që mund të bëhet. I takon trajnerit të bëjë përmbledhjen e përmbajtjes së kursit duke iu referuar synimit dhe objektivave. | | |
| **Objektivat:**  Në përfundim të këtij sesioni pjesëmarrësit do të jenë në gjendje të:   * Japin vlerësimin e duhur për kursin dhe efektivitetin e tij * Plotësojnë formularët e vlerësimit të kursit të Këshillit të Evropës * Identifikojnë nivelin tjetër të mësimit që iu nevojitet për përmirësimin e njohurive dhe aftësive të tyre në këtë fushë. | | |
| **Hyrje**  Ky është një sesion i rëndësishëm i kursit dhe duhet të përdoret për marrjen e konsideratave nga pjesëmarrësit në lidhje me përmbajtjen dhe metodologjinë e përdorur për zhvillimin e tij. Çdo formular vlerësimi duhet të plotësohet dhe finalizohet gjatë sesionit. Trajneri duhet të bëjë përmbledhjen e të gjithë sesionit dhe të kontrollojë që janë përmbushur objektivat. Sapo të përfundojë sesioni trajneri është përgjegjës për garantimin që të gjitha vlerësimet janë marrë në konsideratë dhe se çdo ndryshim i nevojshëm është zbatuar gjatë kursit ose si një modifikim i vogël ose gjatë azhurnimit të programuar të tij. | | |
| **Slajdi 1**  **Slajdet**  **2 & 6**  **Slajdi 7** | **Prezantim me PowerPoint** (ose prezantim i ndonjë lloji tjetër)  Është përgatitur një prezantim me PowerPoint për të ndihmuar trajnerin në inkurajimin e diskutimit në lidhje me të gjitha sesionet e kursit. Trajneri duhet të shpërndajë formularët e vlerësimit përpara fillimit të këtij sesioni. Në disa rrethana, mund të jetë e përshtatshme të jepen formularët e vlerësimit në fillim të kursit me qëllim që pjesëmarrësit të mund t’i plotësojnë ato gjatë zhvillimit të kursit dhe kur sesionet t’i kenë të freskëta në mendje. Ka gjithashtu një tendencë që nga fundi i kursit pjesëmarrësit nuk i mbushin ato plotësisht.  Si me mësimet e mëparshme edhe ky duhet të ndjekë një formë të ngjashme me axhendën dhe objektivat e sesionit të përcaktuara në fillim të mësimit.  Axhenda është një mënyrë e dobishme për të kujtuar pjesëmarrësit për përmbajtjen e kursit dhe është përfshirë për të ndihmuar trajnerin.  Trajneri duhet të rishikojë secilin prej sesioneve dhe të marrë shënim vlerësimet e pjesëmarrësve në mënyrë që të bëjë përmirësime të kursit.  Është përgjegjësia e trajnerit që të garantojë se pjesëmarrësit i kanë plotësuar formularët e vlerësimit. | |
|  | **Ushtrime Praktike** (nëse ka)  Përveç plotësimit të formularëve të vlerësimit, nuk ka asnjë ushtrim praktik të lidhur me këtë sesion**.** | |
|  | **Kontrolli i Njohurive**  Sesioni i jep mundësinë trajnerit që të jetë në gjendje të kontrollojë njohuritë e fituara nga pjesëmarrësit me anë të bërjes së pyetjeve gjatë fazës së vlerësimit. | |
|  | **Përmbledhje**  Trajnerët duhet të sigurohen që pjesëmarrësve u janë dhënë mundësi të mjaftueshme për të dhënë vlerësimet e tyre dhe se këto vlerësime janë mbledhur. | |

1. Vlerësimi nga pjesëmarrësit

Vlerësimi është pjesë e rëndësishme e një kursi trajnimi dhe duhet të caktohet koha e duhur që pjesëmarrësit të japin vlerësimin e tyre për përvojën e të mësuarit.

Ky kurs është zhvilluar si një kurs i përgjithshëm dhe si i tillë shumë prej materialeve të mësimit janë në formatin PowerPoint dhe pa nivelin e ushtrimeve praktike që zakonisht lidhen me këtë lloj kursi.

Është përgatitur një formular vlerësimi dhe ai jepet si model për tu përshtatur në kushtet lokale. Trajnerët janë përgjegjës për të garantuar se formularët janë plotësuar dhe kthyer tek organizatorët me qëllim që të bëhen përmirësime për zhvillim të mëtejshëm të kursit.

1. Vlerësimi i pjesëmarrësve

Për këtë kurs nuk është kërkuar asnjë vlerësim; megjithatë ata që do ta zhvillojnë këtë kurs në të ardhmen, veçanërisht në ato vende ku kursi mund të jetë pjesë e një programi mund ta rimendojnë këtë. Nëse bëhet një vlerësim i pjesëmarrësve, duhet të përdoren metodologjitë e vendit ku zhvillohet kursi.

**Shtojcat**

**Materialet e Trajnimit dhe Materialet e Pjesëmarrësve**

**Prezantimet**

FINAL Presentation - Session 1.1.1 - Course Opening.pptx

FINAL Presentation - Session 1.1.2 - Developing an Investigation plan

FINAL Presentation - Session 1.1.4 - International Cooperation

FINAL Presentation - Session 1.2.1 - Daily Review

FINAL Presentation - Session 1.2.2 - Digital Forensics

FINAL Presentation - Session 1.2.2 - Digital Forensics - Evidence

FINAL Presentation - Session 1.2.4 - Preparing the Case for Court

FINAL Presentation - Session 1.2.6 - Course Closure

**Profilet**

2012-08-20 am - Scenario and evidence for advanced course.docx

2012-08-20 - Spare Mules.docx

Mule Contact List.docx

Profile - EPIMCA.docx

Profile - Humor Products.docx

**Mesazhet Elektronike të Kërcënimit**

2012-08-11 - Email 1 - 00007 to Humor products extortion email - no headers.pdf

2012-08-16 - Email 2 - 00007 to Humor products extortion email - no headers.pdf

2012-08-16 - Email 2 - 00007 to Humor products extortion email- headers.pdf

2012-08-17 - Email 3 - Humor to 00007 - We cannot pay criminals email - no headers.pdf

2012-08-19 - Email 4 - 00007 to Humor Products - instruction email and attachments - headers.pdf

2012-08-19 - Email 4 - 00007 to Humor Products - instruction email and attachments - no headers.pdf

2012-08-19 - Email 4 - attachment 387\_237 pixels.pdf

2012-08-19 - Email 4 - attachment 547\_558 pixels.pdf

2012-08-19 - Email 4 - attachment car-original.jpg

2012-08-21 - Email 5 - Humor Products to 00007 querying instructions for advertising car- no headers.pdf

2012-08-21 - Email 6 - 00007 to Humor Products - Apologies - no headers.pdf

2012-08-21 - Email 7 - Advert Placed - no headers.pdf

2012-08-25 - Email 8 - rgrealestate to Humor Products - Mercedes Advert has expired.pdf

2102-08-21 - Email 6 - 00007 to Humor Products - Apologies - headers.pdf

**Deklaratat Bankare për Kompaninë Humor Products**

2012-10-25 - HSBC Bank Statements - Master Copy Transactions to 28th Oct 2012.pdf

**Mesazhet Elektronike për Korrierët**

**Ftesat për Korrierët nga Ralf Myler**

Invite 2 from 00007 to Bertram Klausen - headers.docx

Invite 2 from 00007 to Bertram Klausen - no headers.pdf

Invite 2 from 00007 to Jacob Wright - headers.docx

Invite 2 from 00007 to Jacob Wright - no headers.pdf

Invite 2 from 00007 to Johan Lauritsen - headers.docx

Invite 2 from 00007 to Johan Lauritsen - no headers.pdf

Invite 2 from 00007 to Khalid Abrahamsson - headers.docx

Invite 2 from 00007 to Khalid Abrahamsson - no headers.pdf

Invite 2 from 00007 to PetrHaluza - headers.docx

Invite 2 from 00007 to PetrHaluza - no headers.pdf

Invite from 00007 to Alexander Ponomaryov - headers.docx

Invite from 00007 to Alexander Ponomaryov - no headers.pdf

Invite from 00007 to Bertram Klausen - headers.docx

Invite from 00007 to Bertram Klausen - no headers.pdf

Invite from 00007 to David Boholyubov - headers.docx

Invite from 00007 to David Boholyubov - no headers.pdf

Invite from 00007 to Doreen Kirsch - headers.docx

Invite from 00007 to Doreen Kirsch - no headers.pdf

Invite from 00007 to Gabriyel Kozlowski - headers.docx

Invite from 00007 to Gabriyel Kozlowski - no headers.pdf

Invite from 00007 to IvankaPavlovic - headers.docx

Invite from 00007 to IvankaPavlovic - no headers.pdf

Invite from 00007 to Jacob Wright - headers.docx

Invite from 00007 to Jacob Wright - no headers.pdf

Invite from 00007 to Johan Lauritsen - headers.docx

Invite from 00007 to Johan Lauritsen - no headers.pdf

Invite from 00007 to KarelVachon - headers.docx

Invite from 00007 to KarelVachon - no headers.pdf

Invite from 00007 to Kensel Duarte - headers.docx

Invite from 00007 to Kensel Duarte - no headers.pdf

Invite from 00007 to Khalid Abrahamsson - headers.docx

Invite from 00007 to Khalid Abrahamsson - no headers.pdf

Invite from 00007 to Kuntz Koppany - headers.docx

Invite from 00007 to Kuntz Koppany - no headers.pdf

Invite from 00007 to Layton Murray - headers.docx

Invite from 00007 to Layton Murray - no headers.pdf

Invite from 00007 to Luka Berggram - headers.docx

Invite from 00007 to Luka Berggram - no headers.pdf

Invite from 00007 to Marija Slatic - headers.docx

Invite from 00007 to Marija Slatic - no headers.pdf

Invite from 00007 to NadanSibincic - headers.docx

Invite from 00007 to NadanSibincic - no headers.pdf

Invite from 00007 to PetrHaluza - headers.docx

Invite from 00007 to PetrHaluza - no headers.pdf

Invite from 00007 to RuzenaStepankova - headers.docx

Invite from 00007 to RuzenaStepankova - no headers.pdf

Invite from 00007 to SiiriHurmerinta - headers.docx

Invite from 00007 to SiiriHurmerinta - no headers.pdf

Invite from 00007 to Turner Desilets - headers.docx

Invite from 00007 to Turner Desilets - no headers.pdf

Invite from 00007 to Tyler Metcalfe - headers.docx

Invite from 00007 to Tyler Metcalfe - no headers.pdf

**Përgjigjet nga Korrierët për Ralf Myler**

Reply to 00007 - hushmail - from Layton Murray - no headers.pdf

Reply to 00007 - hushmail bounced message - from Layton Murray - no headers.pdf

Reply to 00007 from Alexander Ponomaryov - no headers.pdf

Reply to 00007 from Doreen Kirsch- no headers.pdf

Reply to 00007 from Gabriyel Kozlowski - no headers.pdf

Reply to 00007 from IvankaPavlovic - no headers.pdf

Reply to 00007 from Johan Lauritsen - no headers.pdf

Reply to 00007 from KarelVachon - no headers.pdf

Reply to 00007 from Kensel Duarte - no headers.pdf

Reply to 00007 from Kuntz Koppany - no headers.pdf

Reply to 00007 from Luka Berggren - no headers.pdf

Reply to 00007 from Marija Slatic - no headers.pdf

Reply to 00007 from RuzenaStepankova - no headers.pdf

Reply to 00007 from SiiriHurmerinta - no headers.pdf

Reply to 00007 from Tyler Metcalfe - no headers.pdf

Reply to Ralph Muller - Yahoo - from Layton Murray - no headers.pdf

**Udhëzimet për Bankomatet për Korrierët nga Myler**

ATM Instructions email - Alexander Ponomaryov - no headers.pdf

ATM Instructions email - Doreen Kirsch - no headers.pdf

ATM Instructions email - GabriyelKoslowski - no headers.pdf

ATM Instructions email - IvankaPavlovic - no headers.pdf

ATM Instructions email - Kensel Duarte - no headers.pdf

ATM Instructions email - Kuntz Koppany - no headers.pdf

ATM Instructions email - Marija Slatic - no headers.pdf

ATM Instructions email - RuzenaStepankova - no headers.pdf

ATM Instructions email - SiiriHurmerinta - no headers.pdf

**Mesazhet Elektronike me Koka nga Korrierët**

alexander\_ponomaryov.txt

berggrenluka.txt

gabkoz.txt

ivankapav.txt

kenselduarte.txt

kirschdoreen.txt

kuntzkoppany.txt

lauritsenjohan.txt

siirihurmenrinta.txt

slaticmarija.eml

slaticmarija.txt

sruzena.txt

tylermetcalfe12.txt

vachonkarel.txt

**Provat nga Kompjuteri i të Dyshuarit**

U krijua një makinë virtuale që pretendon të jetë imazhi i kompjuterit të keqbërësit kryesor Ralf Myler. Kjo pajisje është e disponueshme në një USB.

**Skedarë shtesë:**

mule-tracking-emails-headers.docx

mule-tracking-emails.docx

**Skedarët Steganografik**

car-original.JPG

car-original.png

car-original2.jpg

car-stego-new.png

car-stego.png

Card data for photo.docx

Card stripe information.docx

creditcards.txt

Setup-OpenStego-0.5.2.exe

stego-instruction.png

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. Pikat Qendrore Kombëtare të Referencës së Interpolit. Shën. i Përkthyesit [↑](#footnote-ref-4)
4. Kriminalistika Dixhitale [↑](#footnote-ref-5)
5. Bllokuesit e të shkruarit (psh në një disk). Shën. i Përkthyesit [↑](#footnote-ref-6)
6. Shih nr.4. Shën. i Përkthyesit. [↑](#footnote-ref-7)
7. Hashing është një funksion kriptografik që merr disa të dhëna si input dhe prodhon një “gjurmë” të këtyre të dhënave, e cila quhet përmbledhje. Kjo gjurmë nuk mund të kthehet në formën origjinale pasi është konvertuar, duke e bërë kështu funksionin e hashing ideal për ruajtjen e fjalëkalimeve që ato të mos vidhen. Për shembull: Inputi: “sells”; rezultati: “205 93, 0, 158, 133, 9, 66, 132, 42, 23, 220, 107, 20, 29, 195, 98, 20, 113, 141, 53, 167”. Shën i Përkthyesit. [↑](#footnote-ref-8)
8. Zbulimi i të dhënave. Shën i Përkthyesit. [↑](#footnote-ref-9)
9. Slack and unallocated space – Hapësirë e papërdorur/e lirë në sistemin e skedarëve në kompjuter. Shën i Përkthyesit. [↑](#footnote-ref-10)
10. Koshi i plehrave. Shën i Përkthyesit. [↑](#footnote-ref-11)
11. Njësi logjike në ruajtjen e skedarëve në diskun e kompjuterit. Shën i Përkthyesit [↑](#footnote-ref-12)
12. Kopjo nga Koshi i Plehrave. Shën i Përkthyesit [↑](#footnote-ref-13)
13. Rikuperimi i skedarëve ose fragmenteve të skedarëve. Shën i Përkthyesit [↑](#footnote-ref-14)
14. Hapësira të papërdorura (bosh) në strukturën e skedarëve. Shën i përkthyesit [↑](#footnote-ref-15)
15. Slack Space – Hapësirë e papërdorur nga skedari. Shën i Përkthyesit [↑](#footnote-ref-16)
16. Hapësirë e papërdorur nga skedari. Shën i Përkthyesit [↑](#footnote-ref-17)
17. Si të bësh një sulm DDOS. Shën i Përkthyesit. [↑](#footnote-ref-18)
18. Steganografia. Shën i Përkthyesit. [↑](#footnote-ref-19)
19. Programi kompjuterik tor. Shën i Përkthyesit. [↑](#footnote-ref-20)
20. Shërbime anonime në Internet që mundësojnë bërjen e navigimit të pagjurmueshëm. Shën i Përkthyesit [↑](#footnote-ref-21)
21. Kompjuterë ose serverë që shërbejnë si ndërmjetës. Shën i Përkthyesit [↑](#footnote-ref-22)
22. Shkak i mundshëm. Shën i Përkthyesit [↑](#footnote-ref-23)
23. Teknika e komunikimit në mënyrë anonime në një rrjet kompjuterik. Shën i Përkthyesit [↑](#footnote-ref-24)