|  |  |
| --- | --- |
|  | **CyberCrime@IPA**  **Заеднички проект на ЕУ и Советот на Европа за регионална соработка против компјутерски криминал**  **Обука за судии и јавни обвинители**  **Почетна обука за компјутерски криминал и електронски докази**  Прирачник и упатства за обучувачи – Верзија 1.0  Оддел за заштита на податоци и компјутерски криминал  Генерален директорат за човекови права и владеење на правото  Стразбур, Франција  5 април, 2013  [**www.coe.int/cybercrime**](http://www.coe.int/cybercrime)  eu_coe_JP1 |
|  |

|  |  |
| --- | --- |
| **Контакт:**  **Оддел за заштита на податоци и компјутерски криминал**  **Генерален директорат за човекови права и владеење на правото**  **Стразбур, Франција**  тел: +33-3-9021-4506 факс: +33-3-9021-5650 E-пошта: [alexander.seger@coe.int](mailto:alexander.seger@coe.int) | **Оградување**  **Гледиштата изнесени во овој технички извештај не ги претставуваат официјалните ставови на Советот на Европа, или на донаторите кои го финансираат овој проект, ниту пак на членките на тука наведените спогодби.** |

СОДРЖИНА

[1 Вовед 4](#_Toc358477570)

[2 Општ преглед 5](#_Toc358477571)

[2.1 Цел на обуката 5](#_Toc358477572)

[2.2 Потреба од ваква обука 5](#_Toc358477573)

[2.3 Наставен план 6](#_Toc358477574)

[3 Како се користи прирачникот за обучувачи 6](#_Toc358477575)

[4 Преглед на обуката 7](#_Toc358477576)

[4.1 Времетраење на обуката и за кого е наменет 7](#_Toc358477577)

[4.2 Кој ќе ја обди обуката 7](#_Toc358477578)

[4.3 Како се одвива наставата 7](#_Toc358477579)

[4.4 Задачи на обуката 8](#_Toc358477580)

[4.5 Целна група на студенти и група на обучувачи 8](#_Toc358477581)

[4.5.1 Студенти 8](#_Toc358477582)

[4.5.2 Претходно искуство 8](#_Toc358477583)

[4.5.3 Обучувачи 8](#_Toc358477584)

[4.5.4 Потребно претходно искуство 8](#_Toc358477585)

[4.6 Ресурси 8](#_Toc358477586)

[4.6.1 Потребни ресурси за одржување на обуката 8](#_Toc358477587)

[4.7 Оценување 9](#_Toc358477588)

[4.8 Задачи/Цели на обуката и сесиите 9](#_Toc358477589)

[5 Лица за контакт 14](#_Toc358477590)

[6 Наставен план 15](#_Toc358477591)

[6.1 Сесија 1.1. Вовед во обуката 15](#_Toc358477592)

[6.2 Сесија 1.1.2 Вовед во компјутерски криминал 17](#_Toc358477593)

[6.3 Сесија 1.1.3, 1.2.2 & 1.2.5 – Технологија 28](#_Toc358477594)

[6.4 Сесија 1.3.1 – Дневен преглед 55](#_Toc358477595)

[6.5 Сесија 1.2.3 Компјутерскиот криминал како кривично дело – Домашно законодавство 56](#_Toc358477596)

[6.6 Сесија 1.2.4 Домашно процесно право 78](#_Toc358477597)

[6.7 Сесија 1.3.1 Дневен преглед 83](#_Toc358477598)

[6.8 Сесија 1.3.2 и 1.3.3 Електронски докази 84](#_Toc358477599)

[5. Пакување, транспорт и складирање 101](#_Toc358477600)

[6.9 Сесија 1.3.4 Меѓународна соработка 110](#_Toc358477601)

[6.10 Сесија 1.3.5 Затворање на обуката 119](#_Toc358477602)

[7 Евалуација 122](#_Toc358477603)

[8 Оценување 122](#_Toc358477604)

# Вовед

Имајќи ја предвид поврзаноста на општествата ширум светот преку информатички и комуникациски технологии, судиите и обвинителите мора да бидат подготвени да се справуваат со компјутерскиот криминал и електронските докази. И додека во многу земји органите на законот ги засилуваат своите капацитети за следење на компјутерскиот криминал и обезбедување на електронските докази, се чини дека ова не е случај со судиите и обвинителите. Искуството покажува дека во многу случаи судиите и обвинителите се соочуваат со потешкотии во справувањето со новата реалност во светот на компјутерите. Затоа, се прават особени напори, преку обука, вмрежување и специјализација, да се оспособат судиите и обвинителите да знаат како да се гони и суди компјутерскиот криминал и како да се искористат електронските докази.

Концептот за поддршка на овие напори е подготвен од Советот на Европа како дел од проектот „Компјутерски криминал“, а во текот на 2009 година е остварена соработка со институциите од лисабонската мрежа за обука на судии во соработка со работната група составена од повеќе чинители.

Целта на концептот е да им помогне на судските институции за обука да оформат програми за обука поврзани со компјутерскиот криминал и електронските докази за судии и обвинители, и таквата обука да се интегрира во редовните почетни обуки во институциите за таа намена.

Целите на овој концепт за обука за судии и обвинители се:

* Да им овозможи на институциите за обука да подготват почетна и интерна обука заснована врз меѓународни стандарди
* Да се запознаат што поголем број идни и сегашни судии и обвинители со основите на компјутерскиот криминал и електронските докази
* Да обезбеди напредна обука за критичен број судии и обвинители
* Да обезбеди постојана едукација и техничка обука за судиите и обвинителите
* Да придонесе за поактивно знаење преку вмрежување на судиите и обвинителите
* Да го олесни пристапот до различни иницијативи за обука и мрежно поврзување

преку Заедничкиот регионален проект на Европската Унија и Советот на Европа *Компјутерски криминал@IPA* (Регионална соработка во областа на кривичното право: зајакнување на капацитетите во борбата против компјутерскиот криминал[[1]](#footnote-1)), институциите за обука од подрачјето каде што се одвива проектот (Албанија, Босна и Херцеговина, Хрватска, Црна Гора, Србија, „поранешна југословенска Република Македонија“, Турција и Косово\*), се поддржуваат во примената на овој концепт за обука.

Во овој контекст, материјалите за обука се конципирани да се користат од институциите за обука, а беше одржана „Програма за обука на обучувачите“. Последна верзија на пакетот за обука ги зема предвид повратните информации добиени од судиите и обвинителите кои учествувале на „Програмата за обука на обучувачите“, од обуката одржана во институциите за обука, а финалната верзија ја разгледаа членовите на Работната група задолжена за обука за судиите и обучувачи, на собир одржан токму за оваа намена.

# Општ преглед

## Цел на обуката

Целта на оваа обука е да им обезбеди на судиите и обвинителите основно познавање за компјутерскиот криминал и електронските докази. Обуката обезбедува правни, како и практични информации за наведената материја со нагласка како овие прашања се одразуваат во секојдневната работа на судиите и обвинителите.

На крајот на обуката, судиите и обвинителите ќе се стекнат со основни познавања за:

* Компјутерскиот криминал и електронските докази
* Како судиите и обвинителите да се справат со нив
* Кои основни процесни закони и технологии можат да се применат
* Кои итни и ефикасни мерки, како и засилена меѓународна соработка, треба да се преземат

Обуката ги опфаќа следните области:

* Вовед во компјутерски криминал – трендови и алатки
* Технологијата поврзана со компјутерскиот криминал
* Компјутерскиот криминал како кривично дело во домашното законодавство
* Практика во електронските докази, постапки и законодавство
* Процесни закони/истражни мерки во домашното законодавство
* Меѓународна соработка

## Потреба од ваква обука

Судиите и обвинителите имаат значајна улога во истражувањето и судењето на поединци или групи кои извршиле криминал. Се почестиот број случаи на криминал во кои се присутни елементи на компјутерски криминал и електронски докази ја наметнуваат потребата од соодветна обука за судиите и обвинителите, со цел тие да ја сфатат природата на овој криминал и истовремено да се запознаат со законодавството и инструментите за меѓународна соработка кога се работи на вакви случаи.

Активностите на криминалците и криминалните групи не се ограничени во рамки на границите на една држава – за извршување на кривично дело поврзано со компјутерски криминал сторителот не мора да преминува граница, а тоа го отежнува и гонењето. Ова уште повеќе ја нагласува потребата од подобрувањето на меѓународната/регионалната соработка, како и соработката помеѓу агенциите задолжени за компјутерски криминал.

Случаите со компјутерскиот криминал најчесто бараат брза и многу ефикасна меѓународна или регионална соработка, преку која ќе се обезбеди навремена истрага и судско гонење на сторителите. Според тоа, институциите за обука во своите наставни планови треба да вклучат модули со упатства за инструментите на меѓународната соработка кои можат да се применат при истрагата на компјутерскиот криминал, вклучувајќи ги лицата за контакт 24/7, взаемната правна помош, активностите на судска соработка, платформите за судска соработка, итн.

## Наставен план

Наставниот план е основната алатка која институциите за обука треба да ја имаат предвид при обуката поврзана со компјутерски криминал. Целта на овој документ е да се оформат стандардизирани курсеви или модули кои би биле вклучени во почетната обука за судии и обвинители кои се занимаваат со судско гонење и судење на предмети поврзани со компјутерски криминал во опфатените земји/региони.

Предложениот образец на модулите за обука на судиите треба да послужи само како основа за обуката на судии и обвинители, а не како крајна цел. Проектот за наведените земји/региони треба да ги согледа потребите на национално ниво, и да побара дополнителна конкретна обука од областа на компјутерскиот криминал која ќе се процени за најпотребна.

Презентациите се подготвени по теми, а дадени се и детални објаснувања кои треба да ги даде обучувачот. Во обуката се нуди можност за дополнувања, за да се одговори на конкретните национални потреби, и на крајот да се постигне целта и поставените задачи. На овој начин се обезбедува конзистентност во модулите за обука во различни држави. На почетокот, обучувачите би требало да воведат одреден број вежби и дискусии за да на учесниците им го олеснат процесот на учење.

Основниот модул за обука е конципиран на начин на кој, по завршувањето на обуката, им дава можност на судиите и обвинителите да се здобијат со основно познавање за природата на компјутерскиот криминал, термините и технологијата. Истовремено, преку овој модул се добиваат информации за меѓународната соработка, електронските докази, процесното право, истражните мерки, итн.

Постои и напреден модул за обука кои претставува продолжение и надградба на основниот модул, и содржи подетални информации за веќе презентираните теми, при што се користат случаи од практиката, со цел да се утврди знаењето стекнато со основниот модул. Целта на напредниот модул за обука е да им овозможи на судиите и обвинителите да се здобијат со дополнително знаење кое може да се примени во практиката, а е во врска со функционирањето на компјутерите и мрежното поврзување, компјутерскиот криминал, законодавството за компјутерскиот криминал, судската надлежност, начините на истрага, електронските докази и меѓународната соработка.

# Како се користи прирачникот за обучувачи

Целта на прирачникот е на обучувачите да им се дадат информации во врска со структурата и содржината на обуката. Во овој пакет се вклучени содржината на информациите што треба да се опфатат, методологијата за одржување на обуката и сите релевантни помагала. Целта на прирачникот е да обезбеди стандардизиран и конзистентен тек на предавањата.

Прирачникот дава и одредени насоки за нивото и технолошкото знаење што судиите и обвинителите треба да го имаат за делотворно исполнување на работните задачи. Секако, тој не претставува комплетна анализа на прашањата, ниту пак е конечен извор за информации.

Се препорачува лицата кои ја подготвуваат обуката, при подготовката на материјалите да ги опфатат и најновите технолошки предизвици што влијаат врз криминалното однесување, како и нивното влијание врз правните процеси и доказните постапки во правосудните системи каде што се спроведува обуката. Технолошките промени, како што се складирањето во полупроводници и Веб 2.0, влијаат врз кривичното право. Ова се значајни прашања кои треба да бидат вклучени во програмите за обука, особено кога ваквите случаи се се позачестени.

Како и секоја друга програма, така и обуките за судии и обвинители треба да имаат строго определени задачи кои треба да се *СМАРТ* - *SMART* (конкретни, мерливи, достижни, релевантни и временски ограничени). Само на ваков начин е можно да се утврди дали тие се исполнети. Задачите не треба да се дефинираат со термините „разбира“ или „знае“, бидејќи тие не ги задоволуваат горе-наведените критериуми. На пример, како ќе се одреди или измери дали се е остварена задачата „знае“? Подобро е да се користат термини како „наброј“ или „идентификувај“, кои се мерливи.

Користењето на случаи од практиката во процесот на учење се смета за посоодветен начин за обука, и повеќе одговара на начинот на учење кај возрасните од чисто дидактичката настава.

Клучна задача за лицето кое ја подготвува обуката е да ја постигне општата цел и конкретните задачи зададени за секој нејзин дел. Во ова поглавје се дадени информации со кои може да се олесни одвивањето на тој процес.

Концептот на обуката е општ, и не се однесува конкретно на одредена земја. Но, важно е обучувачите соодветно да ги прилагодат материјалите на себе, и со тоа да постигнат поголема делотворност во одржувањето на обуката. Користењето на случаи од практиката се смета посоодветно за овој тип на учење и повеќе одговара на начинот на учење кај возрасните, отколку чисто дидактичка настава. Примероци на технологијата и користењето на интернетот може исто така да го забрзаат учењето. Конкретно за сесиите посветени на материјалното и процесното право на национално ниво, дадени се обрасци кои треба да се пополнат со соодветни информации за одредена земја, и обврска на обучувачите е нив да ги внесе пред одржувањето на обуката во таа земја.

# Преглед на обуката

## Времетраење на обуката и за кого е наменета

Курсот е предвидено да трае три дена, а е наменет за судии и обвинители како дел од почетната програма за обука.

## Кој ќе ја води обуката

Конципирано е овој курс да го водат обучувачи од центрите за обука за судии и обвинители во земјите кад што ќе се одржува обуката. Каде што тоа е потребно, се препорачува вклучување и на експерти за одредени теми кои ќе се ангажираат за конкретни технички прашања, доколку такви профили на стручни лица не постојат во самите институции. Со оглед на тоа дека се работи за почетно ниво, се очекува овој курс да ги опфати сите нови судии и обвинители.

## Како се одвива наставата

Структурата а курсот предвидува негово одржување во училница, каде што обучувачите ќе вршат настава. Но, не постои причина материјалите да не се прилагодат и за учење од далечина, или како модули за е-учење, доколку се јави потреба од тоа. Како што се објаснува погоре во Дел 1, обучувачите треба да ја разгледаат можноста за вклучување вежби и други наставни методи во програмите за национално ниво.

## Задачи на обуката

Задачите што се задаваат во овој курс се презентираат на традиционален начин, со што на обучувачите им се дава можност да користат разни наставни методи за нивно постигнување. Сите задачи се СМАРТ. За оние кои не се запознаени со СМАРТ задачите, следи следното објаснување:

С – специфичност, конкретност. Точно се прецизира што треба да се постигне.

М – мерливост. Треба да сте во можност да измерите дали ги постигнувате зададените задачи или не.

А – остварливост. Дали поставените задачи се остварливи и достижни.

Р – реалистичност. Дали е реално да се постигнат задачите со расположливите ресурси?

Т – време. Кога сакате да ги постигнете зададените задачи?

Врз основа на ова, зададените задачи треба да се разгледуваат во рамките на пошироките цели на оваа обука. .

## Целна група на студенти и група на обучувачи

### Студенти

Обуката е наменета за судии и обвинители како дел од нивната почетна обука.

### Претходно искуство

Не се претпоставува претходно знаење од дадената област.

### Обучувачи

Обучувачите треба да се вработени во центрите за обука на судии каде што ќе се одвива обуката.

### Потребно претходно искуство

Обучувачите треба да поседуваат солидно знаење од областа на компјутерскиот криминал и новите трендови, како и од домашното законодавство поврзано со компјутерскиот криминал во дадената земја. Исто така, потребно е да имаат претходно теоретско и практично искуство со настава.

## Ресурси

### Потребни ресурси за одржување на обуката

За одржување на курсот во училница, потребно е следното:

* Соодветна просторија според предвидениот број на студенти
* Персонален компјутер или преносен компјутер со *Windows 7* и *MS Office* Професионален проектор и екран
* Пристап до интернет (доколку постои)
* Примероци на компјутерски хардвер (доколку постојат)
* Видео клип (*Воини на интернет*)
* Конвенцијата од Будимпешта за борба против компјутерскиот криминал, заедно со коментари
* Копија од Прирачниот за е-докази финансиран од *OISIN* програмата на ЕК
* Бела табла
* Маркери за бела табла (најмалку по два сини, црни, црвени и зелени)
* Две табли со блокови хартија
* Тетратки и пенкала за студентите
* Хефталка, дупчалка за хартија и ножички
* Лепливи траки или друг материјал за привремено лепење на ѕид.

## Оценување

Во рамките на оваа пилот обука не се предвидува оценување на знаењето на студентите. Доколку сакаат, земјите во кои таа се одвива можат да спроведат и оценување. Но, без оглед на тоа, обучувачите треба да го проверуваат знаењето на студентите во текот на наставата, преку прашања, квизови и други методи, за да се утврди дали поставени задачи се остваруваат.

## Задачи/Цели на обуката и сесиите

|  |  |  |
| --- | --- | --- |
| Број на лекција | Наслов на лекција | Цели/задачи |
| 1.1.1 | Вовед во обуката | * Запознавање со обучувачите и студентите * Дефинирање на структурата и содржината nа курсот * Комплетирање на соодветни административни задачи * Поделување на материјали за курсот * Запознавање со просторот каде ќе се одржува курсот, вклучително и прашања поврзани со здравјето и безбедноста |
| 1.1.2 | Вовед во компјутерски криминал | * Да се идентификуваат различните видови компјутерски криминал и нивното значење * Да се набројат заканите, трендовите и алатките поврзани со компјутерскиот криминал и одговорите на овој криминал * Да се објаснат концептите на компјутерски криминал кои согласно националното законодавство и меѓународните стандарди се сметаат за кривични дела * Да се анализира потребата и предноста од усогласување на домашното законодавство и меѓународните инструменти , со акцент врз Конвенцијата од Будимпешта |
| 1.1.3  1.2.2  1.2.5 | Вовед во технологијата | * Да се набројат составните делови на компјутерските системи * Да се идентификуваат различните видови уреди за складирање на податоци * Да се утврдат можните последици од експоненцијалното зголемување на капацитетите за складирање податоци во контекст на кривичното право * Да се идентификуваат различни компјутерски оперативни системи * Да се објаснат основите на функционирањето на мрежите * Да се објасни функцијата на интернетот * Да се идентификуваат најмалку 5 главни интернет апликации * Да се објасни развојот на интернетот, од неговите почетоци до денес * Да се диференцираат различни интернет апликации * Да се идентификува како криминалците користат разни интернет апликации |
| 1.2.3 | **Компјутерскиот криминал како кривично дело во домашното законодавство** | * Да се идентификуваат клучните фактори што се користат за опишување на кривичните дела согласно Конвенцијата од Будимпешта. * Да се наведат одредбите од кривичното материјално право и да се идентификуваат клучните фактори што се користат за опишување на кривичните дела согласно постојното национално законодавство. * Да се анализираат потребите и предностите од усогласување помеѓу националното законодавство и меѓународните инструменти, особено Конвенцијата од Будимпешта. * Да се идентификуваат релевантните одредби од материјалното право во дискусиите за случаите од практиката. |
| 1.2.4 | **Процесно право и истражни мерки во домашното законодавство** | * Да се објаснат процесните одредби во Конвенцијата од Будимпешта * Да се објаснат процесните одредби во националните закони |
| 1.3.3  1.3.4 | Прибирање електронски докази; процесни и истражни мерки | * Да се дискутира за различните видови електронски докази * Да се објаснат принципите на најдобрата практика поврзана со заплената и работењето со електронските докази * Да се идентификуваат предизвиците поврзани со „статични податоци“, „живите податоци“ и интернет изворите на електронски докази * Да се идентификуваат предизвиците при добивањето на докази од друга јурисдикација * Да се дискутира прашањето на прифатливост на електронските докази во судските постапки, во однос на автентичноста, точноста и целовитоста * Да се објаснат процесните одредби на Конвенцијата од Будимпешта |
| 1.3.4 | **Меѓународна соработка** | * Да се препознае глобалната димензија на интернетот и меѓународната димензија на компјутерскиот криминал * Да се објасни важноста од меѓународна соработка и да се препознаат расположливите инструменти за меѓународна соработка во полето на компјутерскиот криминал * Да се идентификува потребата од брзи и ефикасни канали на меѓународна соработка и расположливи инструменти, начините тие како се користат, временските рамки и делотворноста * Да се опишат напорите на меѓународните организации за спроведување на модалитетите на меѓународната соработка * Да се дискутира Конвенцијата од Будимпешта за борба против компјутерскиот криминал – да се идентификуваат општите принципи, времените мерки и мрежата за взаемна правна помош која функционира 24 часа, седум дена во неделата |
| 1.3.5 | Заокружување на обуката | * Да се дадат соодветни повратни информации во врска со обуката и нејзината делотворност * Да се пополнат формуларите за евалуација * Да се идентификува наредното ниво на едукација што учесниците треба да го преземат за да го подобрат нивното знаење и вештини за оваа тема. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Совет на Европа**  **Обука за судии и обвинители за компјутерски криминал** | | | | | | | | | | | | |
| **Распоред– Модул 1** | | | | | | | | | | | | |
|  | **09:00 - 10:00** | | **10:00 - 11:00** | | **11:00 - 12:00** | | **12:00 - 13:00** | **13:00 - 14:00** | **14:00 - 15:00** | **15:00 - 16:00** | | **16:00 - 17:00** |
| **Ден 1** | **1.1.1**  **Отворање и вовед** | | | **1.1.2**  **Вовед во заканите, трендовите и предизвиците на компјутерскиот криминал** | | | | **ПАУЗА** | **1.1.3 Вовед во технологија**  **Дел 1** | | | |
| **Ден 2** | **1.2.1**  **Дневен преглед** | **1.2.2 Вовед во технологија**  **Дел 2** | | | | **1.2.3**  **Компјутерски криминал како кривично дело во домашното законодавство** | | **ПАУЗА** | **1.2.4**  **Процесно право и истражни мерки во домашното законодавство** | | **1.2.5 Вовед во технологија**  **Дел 3** | |
| **Ден 3** | **1.3.1**  **Дневен преглед** | **1.3.2 Електронски докази**  **Практика и процедури** | | | | **1.3.3**  **Електронски докази**  **Процесно и истражно право** | | **ПАУЗА** | **1.3.4**  **Меѓународна соработка** | | **1.3.5**  **Повратни информации од учесниците и затворање на обуката** | |

Забелешка – Во текот на одржувањето на обуката во соодветно време ќе има паузи за кафе

# Лица за контакт

Лица за контакт за какви било прашања поврзани со обуката и нејзината содржина:

Александар Сегер

Раководител на Одделот за заштита на податоци и компјутерски криминал

Генерален директорат за заштита на човековите права и владеењето на правото (ГД 1)

Совет на Европа

Council of Europe

F-67075 Strasbourg Cedex

Tel. +33 3 90 21 4506

Fax +33 3 90 21 56 50

[alexander.seger@coe.int](mailto:alexander.seger@coe.int)

Мустаф Ферати

Програмски офицер

Генерален Директорат за заштита на човековите права и владеењето на правото (ГД 1)

Council of Europe  
67075 Strasbourg Cedex, FRANCE  
Tel.: +33 (0)3 90 21 45 50  
Fax: +33 (0)3 90 21 56 50

[Mustafa.Ferati@coe.int](mailto:Mustafa.Ferati@coe.int)

# Наставен план

|  |  |  |  |
| --- | --- | --- | --- |
| Сесија 1.1. Вовед во обуката | | **Времетраење: 90 минути** | |
| **Потребни средства:**   * Персонален компјутер или преносен компјутер со Windows 7 и со MS Office * Професионален проектор и екран * Пристап до интернет (доколку постои) * Примероци на компјутерски хардвер (доколку постојат) * Бела табла * Маркери за бела табла (најмалку по два сини, црни, црвени и зелени) * Две табли со блокови хартија * Тетратки и пенкала за студентите * Хефталка, дупчалка за хартија, и ножички * Лепливи траки или друг материјал за привремено лепење на ѕид. | | | |
| **Цел:**  Да се информираат учесниците за потребата од ваква обука и нејзините цели и задачи. Да се дадат соодветни информации за програмата на активности и распоредот. Да се дадат соодветни информации за здравствените, безбедносните и административните детали. Да се запознаат учесниците со обучувачите и другите учесници. | | | |
| **Задачи:**  На крајот на сесијата, учесниците ќе бидат во можност да:   * Ги препознаваат обучувачите и другите учесници * Дискутираат за општите цели на курсот * Објаснат зошто е потребна оваа обука * Ги наведат роковите и активностите на обуката * Ги наведат здравствените и безбедносните процедури на местото каде што се одржува обуката | | | |
| Слајд | **Содржина** | | |
| 1 - 23 | **Вовед**  Оваа е сесија со која се отвора курсот и се врши преставување на обучувачите и другите учесници. Се објаснуваат целите и задачите на курсот и методите на предавање.  Обучувачот може да започне и со некоја досетка, за да го „скрши мразот“ и ги охрабри учесниците што повеќе да се заинтересираат за курсот и што подобро да се запознаат на почетокот на обуката. | | |
|  | ***PowerPoint* презентација (или друг вид презентација)**  За оваа сесија има PowerPoint презентација (или друг вид презентација). Се работи за општа презентација која не се бави со конкретни национални прашања кои ќе се обработуваат кога ќе се разговара за состојбите на националното ниво. Обучувачот треба да води сметка презентацијата да биде соодветна на местото каде што ќе се презентира. | | |
| 2 | На овој слајд се дадени прашањата поврзани со здравствените и безбедносните аспекти, кои зависат од местото каде што се одржува обуката. Обучувачот е задолжен на учесниците да им пренесе точни информации во врска со овие аспекти. | | |
| 3 | Курсот е насловен „Вовед во компјутерски криминал и електронски докази – обука за судии и обвинители“. Изработен е од Европската унија/Советот на Европа, како Заеднички проект за регионална соработка на компјутерски криминал во ИПА регионот. | | |
| 4 | Целите на ова сесија е на учесниците да им се дадат соодветни информации за:   * потребата од ваква обука и нејзините цели и задачи * програмата на активности и распоредот. * здравствените, безбедносните и административните детали * запознавање со обучувачите и другите учесници. | | |
| 5 | На крајот на одредена сесија, учесниците треба да можат да ги исполнат зададените задачи. Овие задачи можат да се користат и за тестирање на знаењето што го стекнале учесниците и за евалуација на обуката.  На крајот на оваа сесија, учесниците ќе бидат во можност да:   * Ги препознаваат обучувачите и другите учесници * Дискутираат за општите цели на курсот * Објаснат зошто е потребна оваа обука * Ги наведат распоредот и активностите на обуката * Ги наведат здравствените и безбедносните процедури на местото каде што се одржува обуката | | |
| 6 | Оваа обука е потребна затоа што судиите и обвинителите имаат значајна улога при истрагата и судските процеси за поединци или групи кои извршиле кривични дела. Растечкиот број случаи на криминал со елементи на компјутерски криминал и електронски докази ја наметнуваат потребата од соодветна обука за судиите и обвинителите, со цел тие да ја сфатат природата на овој криминал и истовремено да се запознаат со законодавството и инструментите за меѓународна соработка кои можат да се користат во вакви случаи. | | |
| 7 | Важно е на учесниците да им се објасни сеопфатната цел и значење на оваа обука уште од самиот почеток. Тоа ќе им овозможи да ја согледаат и ценат причината зошто ја посетуваат. Целта на оваа обука е да им обезбеди на судиите и обвинителите основно познавање од компјутерскиот криминал и електронските докази. Обуката предвидува правни, како и практични информации за дадената тема со нагласка на тоа како овие прашања се одразуваат врз секојдневната работа на учесниците. | | |
| 8 | Во оваа фаза, на учесниците им се образложува распоредот – времето на одржувањето на наставата, паузите за ручек, други паузи, а им се дава и краток опис на секоја сесија. Во оваа фаза треба се одлучи дали ќе има оценување. Доколку се одлучи дека треба да има оценување, тогаш тоа треба детално да се објасни, вклучително и материјалот што се очекува од учесниците да го совладаат. | | |
| 9 -17 | На овие слајдови се дадени детално наведените задачи за секоја сесија. Во оваа фаза, тие треба да им се објаснат учесниците. Објаснувањето ги содржи основите елементи на секоја сесија. | | |
| 20 | Следна фаза е запознавањето на обучувачите и учесниците. Ова е прилика студентите уште на почетокот да почнат да комуницираат меѓу себе и со обучувачите. Од учесниците се бара да работат во парови, со лице кое претходно не го познавале. Потоа, треба да го замолат „партнерот“ да одговори на следните прашања:   * Нивното име и земја * Каде работат * Што работат * Нивното искуство како обучувачи * Нешто интересно за нив * Одговорот на „прашањата за степенот на знаење“ | | |
| 21 | Прашањата за степенот на знаење треба да овозможат комуникација, а на обучувачите им дава можност да научат повеќе за знаењето и искуството на учесниците во однос на технологијата и компјутерскиот криминал. На наредниот слајд е даден список, а од учесниците се бара да покажат кој број најмногу одговара на нивните познавања од дадените категории. Работните парови меѓусебно си ги поставуваат истите прашања. Потоа, едниот учесник го претставува колегата на останатите учесници. | | |
|  | **Практични вежби (доколку се предвидени)** | | |
|  | Единствената практична вежба во оваа сесија е запознавањето на учесниците и обучувачите, а барањата поставени во врска со тоа се дадени во претходниот дел. | | |
|  | **Проверка на знаење**  За оваа сесија не е предвидена проверка на знаење. | | |
| 23 | **Преглед/Резиме**  Обучувачот треба да изврши преглед на знаењето на учесниците за овие точки и да увиди дали учесниците ги совладале целите зададени со оваа сесија. Во рамки на сесијата, треба да се издвои соодветно време за прашања. | | |
| Сесија 1.1.2 Вовед во компјутерски криминал | | | **Времетраење: 120 мин.** |
| **Потребни ресурси:**   * Персонален компјутер или преносен компјутер со *Windows 7* и *Office 2010* * Проектор * *PowerPoint* презентација | | | |
| **Цели:**  Целта на оваа сесија е на учесниците им се даде општ преглед за компјутерскиот криминал и од правна гледна точка и од гледна точка на новата реалност. Ги опфаќа состојбите во повеќе земји и правната рамка на меѓународно ниво. | | | |
| **Задачи:**   * Во рамките на сесијата на учесниците ќе им се даде појаснување на терминот компјутерски криминал и опасностите од него, со осврт на заканите, трендовите и алатките на компјутерскиот криминал кои се предизвик за судиите и обвинителите. Освен тоа, во текот на сесијата ќе се објаснат националните и меѓународните одговори на овој феномен. * Кон крајот на оваа сесија, учесниците ќе бидат во можност да ја идентификуваат реалноста што се крие зад изразот „компјутерски криминал“ и да ги разберат концептите кои потпаѓаат под кривични дела согласно повеќе национални законодавства и меѓународни стандарди. * Во текот на сесијата ќе се покријат одредбите на кривичното материјално право кои се поврзани со најновиот развој на настани кај компјутерскиот криминал, и ќе се истакнат некои клучни фактори кои се користат за опис на кривичните дела согласно Конвенцијата од Будимпешта и релевантната правна рамка на ниво на ЕУ. * Во врска со горенаведеното, потребно внимание ќе се посвети на потребата и предноста од усогласување помеѓу националното законодавство и меѓународните инструменти, особено Конвенцијата од Будимпешта. | | | |
| **Број на слајд** | **Содржина:** | | |
|  | **Вовед**  Оваа сесија има конкретна задача на учесниците да им даде еден општ преглед за компјутерскиот криминал, и од правна гледна точка и од гледна точка на постојната реалност. Ги опфаќа состојбите во повеќе земји и правната рамка на меѓународно ниво. | | |
| **2** | **Агенда**  Дел 1 на презентацијата ја опишува новата реалност на информатичкото општество и се осврнува на новите нелегални активности на мрежите.  Дел 2 дава преглед на приодите на одредени меѓународни организации кон компјутерскиот криминал во минатото.  Дел 3 прави обид да ја се одгатне новата реалност што потпаѓа под концептот компјутерскиот криминал  Дел 4 ја објаснува Конвенцијата од Будимпешта за борба против компјутерскиот криминал и ја подвлекува важноста од постоење на единствен и обврзен меѓународен инструмент за борба против компјутерскиот криминал.  Дел 5 се осврнува на најсериозните нелегални онлајн активности што се среќаваат денес. | | |
| **3** | **Задачи на сесијата**  Целта на оваа сесија е да ги презентира општо, или како вовед, прашањата поврзани со компјутерскиот криминал.  Во текот на дискусијата ќе се објасни концептот компјутерски криминал, и причините за загриженост што произлегуваат од него . Ќе се дискутира за посериозните закани, трендови и алатки на компјутерскиот криминал, но и за некои одговори на овој феномен.  Ќе биде презентиран општ преглед за тоа што се покрива под терминот „компјутерски криминал“. Ќе се дискутира и за некои од концептите што согласно повеќето законодавства и меѓународни стандарди се сметаат за видови компјутерски криминал.  Една од најзначајните теми што ќе се дискутира се однесува на одредбите во кривичното материјално право и на некои клучни фактори што се користат за дефинирање на компјутерскиот криминал, кои потекнуваат од Конвенцијата од Будимпешта и релевантните правни рамки на Европската Унија.  Уште еднаш ќе се нагласи потребата и предностите од усогласување помеѓу националните законодавство и меѓународните инструменти, пред се Конвенцијата од Будимпешта. | | |
| 4 | **Дел 1 - Информатичкото општество и компјутерскиот криминал** | | |
| 5 - 7 | Информатичкото општество, модел на општествени и економски развој заснован на прием и размена на информации преку комуникациски мрежи, преовладува во секојдневниот живот на граѓаните, на работното место, дома, и во слободните активности.  Во вакво општествено и економско опкружување, физичката оддалеченост помеѓу луѓето од различни страни на светот губи значење. Со одреден број на добро познати исклучоци, овој нов „отворен свет“ има потенцијал да биде место без политички граници (помеѓу државите) што ги делат лицата кои пребаруваат на интернет. Секој може на демократски начин да се стекне со информации и знаење, независно од тоа каде тие се чуваат. А тоа значи и конкуренција помеѓу сите економски оператори.  Информациите се достапни секому, со слободен и отворен пристап. Интернет корисниците сметаат дека никој нема суверенитет над мрежите. | | |
| 8 | Како што интернетот пристигнува на сите места и кај сите луѓе на светот, така расте и криминалот, а криминалците откриваат нови можности за нелегални активности. Кривичните дела извршени со помош на мрежите имаат развиена транс-националнална димензија.  Токму поради ваквата природа, овој вид криминални активности предизвикува особени потешкотии за лицата кои го истражуваат: на другата страна на светот доказите можат да исчезнат доколку веднаш не реагира за да тие се зачуваат, а органите на законот мора да ги почитуваат политичките граници и да се придржуваат до законски утврдените постапки и јавни канали за барање меѓународна помош за кривични истраги. | | |
| 9 | Затоа, неопходен е меѓународен пристап. Мултинационалниот или меѓународниот пристап нуди многу повеќе можности од националниот, па дури и регионалниот пристап, а глобалното сфаќање на овој феномен го проширува опсегот на соработка. Меѓународната соработка помеѓу органите на законот –полицијата и/или обвинителствата – е од особено значење за постигнување резултати во кривичните истраги. | | |
| 10 | Сите познавачи се согласуваат дека компјутерскиот криминал е глобален феномен, и дека единствениот соодветен одговор на феноменот на непостоење граници на глобалните мрежи, е заедничкиот пристап. Со ваквиот пристап напорите на национално ниво се надополнуваат со специфични форми и канали на меѓународна соработка која може да се справи со глобалната димензија на компјутерскиот криминал, чии последици може да се почувствуваат во кој било дел од светот.  Сосема е јасно дека компјутерскиот криминал е глобален феномен со глобални димензии. Вообичаено, нелегалните активности поврзуваат повеќе територии: сторителите на овие кривични дела се под јурисдикација на одредена земја, а нивните дејствија допираат до компјутерите и жртвите во многу други земји низ светот.  Ова е заедничка карактеристика за сите модерни форми на криминал, но општо земено, кај компјутерскиот криминал и е-доказите тоа е составен дел од нивната природа. Со ширењето на комуникациските мрежи, особено интернетот, станува невозможно за која било земја во светот сама да се справува со овој проблем. | | |
| 11 | Современите општества зависат од информатичките технологии. Државите, граѓаните и економиите се поврзани преку интернет, и тоа многу плодна почва за појава на нови нелегални активности. Тие нелегални активности можат да се преземаат во самите комуникациски мрежи, со користење на мрежите и против мрежите. | | |
| 12 | Насекаде во светот, компјутерскиот криминал се идентификува со феномените како што се *хакерството*, ширењето на малициозен софтвер (претежно вируси или црвчиња), или компјутерски напади, особено популарни кај медиумите (*DoS* или *DDos*). Меѓутоа, денес дури и обичните граѓани се свесни и за многу други криминални активности на мрежите, чија цел најчесто е стекнување профит (пр. обични измами и компјутерски измами). Исто така, секој знае за огромните можности што постојат за користење на компјутерската средина, т.е. компјутерскиот екосистем, за извршување или потпомагање на обични кривични дела. | | |
| 13 | Изразот „*компјутерска средина“* , иако се уште не е јасно дефиниран, ниту во правната ниту во стручната литература, секој ден станува се побогат и по сложен. Со технологијата се зголемува бројот и видот на уреди со кои се комуницира на мрежите и со кои може да се врши пренос или снимање на податоци. | | |
| **15 - 16** | **Дел 2 – Меѓународни организации и компјутерскиот криминал**  Многу меѓународни организации веќе со години се занимаваат со прашањето на компјутерски криминал и електронски докази. | | |
| 17 - 20 | Обединетите нации се еден од повеќето форуми што се занимаваат со компјутерски криминал. Уште во 2000 г. Генералното собрание на ООН изгласа формални резолуции за Борба против криминалната злоупотреба на информатичките технологии (првата е Резолуцијата на ГС 55/63 за борба против криминалната злоупотреба на информатичките технологии, усвоена на 81-то пленарно заседание на ГС на 4 декември 2000 г).  Овие формални резолуции укажуваат на потребата земјите членки на ОН да усвојат национални регулативи со кои се криминализираат одредени активности и се елиминираат т.н. засолништаза криминалците кои вршат компјутерски криминал.  Резолуцијата на ГС на ОН 64/211 (март 2010 г.) за „создавање глобална култура на компјутерска безбедност“, содржи алатка за самостојна проценка на активностите што се преземаат на национално ниво за заштита на критичната информатичка инфраструктура. Резолуцијата, меѓу останатото, им препорачува на државите да усвојат кривично законодавство кое ќе ги земе предвид рамките дадени со Конвенцијата од Будимпешта за борба против компјутерскиот криминал.  Секој пет години, ОН организира Конгрес на тема превенција на криминалот и кривичното право. На Конгресот во Банког во 2005 година и на Конгресот во Салвадор (Бразил) во 2010 година, беше укажано на потребата од техничка помош и градење капацитети.  Предлозите за изработка на нови договори не наидоа на консензус. | | |
| 21 | ОЕЦД – Организацијата за економска соработка и развој, исто како и ОН, покажува загриженост за феноменот на компјутерски криминал. Но, ОЕЦД има развиено поинаков пристап. Од 1983 г., ОЕЦД ја проучува потребата од постоење на национално законодавство за борба против компјутерскиот криминал и издаде препораки во врска со тоа, во кои се укажува дека истите кривични дејствија треба да се квалификуваат во слични рамки и на меѓународно и на национално ниво. | | |
| 22 | Пристапот на Г-8 групата оди уште понатаму, избирајќи повеќе проактивни опции. Г-8 оформи мрежа на лица за контакт кои се референтни во услови на меѓународна соработка. Во основа, се работи за список на имиња – лица за контакт кои можат да покренат итни акции доколку тоа е потребно.  Г-8 се пионери во справувањето со компјутерскиот криминал и заедно со Советот на Европа, имаат најмногу направено на меѓународно ниво за борбата против компјутерскиот криминал до ден денес. | | |
| 23 – 24 | Европската унија исто така работи на оваа проблематика. Во 2005 г., ЕУ усвои задолжителен инструмент – Рамковна одлука на Советот 2005/222/JHA[[2]](#footnote-2)од 24 февруари 2005 г. во врска со напади врз информатички системи. Рамковната одлука им наложува на сите земји членки да криминализираат одредени кривични дела, како што се: нелегален пристап до информатичките системи, нелегален упад во системи и нелегален упад во податоци. Во одлуката исто така се внесени и правила во врска со поттикнување, помагање и поддржување и обиди на вакви кривични дела.  Што се однесува до меѓународната соработка, Рамковната одлука утврдува дека земјите членки на ЕУ ќе ги користат постојните мрежи на оперативни лица за контакт кои се достапни 24 часа на ден, седум дена во неделата.  Во јануари 2011 година, започна ревидирањето на Рамковната одлука 2005/222/JHA (првата јавна нацрт верзија на Предлог одлуката е објавена во октомври 2011 г). | | |
| 25 | Значајно е да се разгледа што работи и ОБСЕ, Организацијата за безбедност и соработка во Европа, во врска со компјутерскиот криминал.  ОБСЕ издава препораки до членките на организацијата. Со Одлуката бр. 7/06, ОБСЕ укажува дека сите земји членки треба да ја разгледаат можноста за пристапување кон Конвенцијата од Будимпешта против компјутерскиот криминал. Со оваа одлука, земјите членки се поттикнуваат да се приклучат кон мрежата за борба против компјутерскиот криминал (24/7), со која што раководат земјите на Г-8, и да номинираат соодветно лица за контакт со цел поедноставување на меѓународната соработка за спроведување на законите во борбата против злоупотреба на компјутерскиот простор. | | |
| 26 | Советот на Европа се занимава со проблемот на компјутерскиот криминал од 1980-те години. Подготвителните работи и незадолжителните препораки доведоа до одлука за преговори за правно обврзен меѓународен договор: Конвенцијата од Будимпешта за борба против компјутерскиот криминал (за овој договор ќе се дискутира подоцна).  Пристапот на Советот на Европа се состои од три дела:   1. Стандарди како Конвенцијата од Будимпешта 2. Следење и „мониторинг“ на имплементацијата од страна на Комитетот на Конвенцијата за компјутерски криминал (T-CY) 3. Програми за техничка соработка со цел да им се овозможи на земјите да ги изградат погребните капацитети | | |
| 28 - 29 | **Дел 3 – Што е компјутерски криминал?** | | |
| 30 | **Технологијата како жртва**  Технологијата како цел на криминалот традиционално се смета за вистински „компјутерски криминал“ и опфаќа кривични дела како што се: хакирање, ускратување на услуги и ширење вируси | | |
| 31 | **Технологијата во поддршка на криминалот**  Технологијата во поддршка на криминалот – компјутерите и други уреди се користат како поддршка за извршување на традиционални кривични дела, како што се: фалсификување документи, испраќање на заканувачки смртни пораки или уцена, или дистрибуција на нелегални материјали, на пр. од злоупотребени деца | | |
| 32 | **Технологијата како комуникациска алатка**  Технологијата како комуникациска алатка – криминалците ја користат технологијата за меѓусебна комуникација на начин што ги намалува шансите за нивно откривање, на пример со користење технологија за шифрирање | | |
| 33 | **Технологијата како уред за складирање**  Технологијата како медиум за складирање– намерно и ненамерно складирање информации на уреди што се користат и за други намери, а зафаќаат податоци што се чуваат на компјутерскиот систем на жртвата, сведоците или осомничените лица. | | |
| **34** | **Технологијата како сведок на криминалот**  Технологијата како сведок на криминалот – се среќава кога доказите од ИТ уредите се користат како поддршка на други докази, иако не постои директна врска со нив, на пример да се потврди или оспори одредено алиби на осомничено лице или изјава на сведок | | |
| 35 | **Технолошки криминал ?**  Овој слајд може да се искористи за резимирање и за проверка на знаењето за поминатото градиво. Се предлага обучувачот да започне само со насловот и да ги праша учесниците да ги идентификуваат видовите кривични дела што потпаѓаат под терминот компјутерски криминал. Би било добро обучувачот да е веќе добро запознает со различните видови кривични дела од Конвенцијата од Будимпешта, за да може да ги користи како пример, или да одговори на прашањата евентуално ќе ги постават учесниците. | | |
| 36 | Во 1984 година, авторот Вилијам Гибсон прв пат го употребил изразот компјутерски простор во научно фантастичниот роман *Neuromancer,* во кој се зборува за интернет и други мрежи. Од тогаш, бројот на слични термини со истиот префикс рапидно се зголемува. Еден од нив секако е и терминот компјутерски криминал. Но, и по скоро триесет години, се уште не постои договор за точната дефиниција на терминот компјутерски криминал, и покрај многубројната литература што се бави со оваа тематика. Не постои ни согласност околу тоа дали компјутерскиот криминал е навистина нов и посебен сегмент од казненото право, или пак е само дел од одредбите на кривичното право што се однесуваат на дигиталната средина. | | |
| **37 - 44** | Меѓутоа, од социолошка гледна точка, криминалот во компјутерската средина веќе претставува значајна и автономна реалност. Низ цела Европа, во рамки на полицијата има специјални истражни единици, а постојат и посебни обвинителства за таа цел. Меѓународните јавни организации и приватните компании се повеќе изразуваат загриженост за последиците од нелегалните и штетните дејствија кои се вршат со помош на комуникациските мрежи, или внатре во самите мрежи.  Кога станува збор за оваа нова реалност, правниците немаат постигнато консензус околу терминот *компјутерски криминал.* Некои автори говорат за *компјутерски криминал*, или  *информатички криминал*. Други пак, го претпочитаат терминот *високо технолошки криминал*. Сето тоа носи ризик од прешироко дефинирање или пак непотребно стеснување на дефиницијата.  Криминалот кои вклучува компјутери не е задолжително „високо технолошки“. За многу криминални активности во компјутерскиот простор се користат релативно едноставни методи, и предизвикуваат релативно мал број технолошки проблеми при истрагата. Меѓутоа, тоа можеби е и непотребно прашање, бидејќи денес, кај сите постои согласност за постоење за една нова општествено криминална реалност, која се одвива внатре во, или со помош на компјутерските системи.  Компјутерскиот криминал честопати се дефинира и во потесна и во поширока смисла: обично, терминот се користи доста рестриктивно, за да се опише криминална активност каде што компјутерот или мрежата се суштински дел од кривичното дело: но, терминот компјутерски криминал се користи и опишување на други, традиционални кривични дела, каде што истите тие компјутери или мрежи се користат за овозможување на незаконски активности.  Според тоа, случаи на компјутерскиот криминал имаме кога:   * компјутерот служи како алатка за извршување криминал, како на пример *спам* (несакана пошта), повреда на авторските права преку P2P мрежи, итн.; * компјутерот или мрежата се цел на криминалните дејствија, како на пример неовластениот пристап и злонамерните компјутерски кодови; * компјутерот или мрежата се местото каде се одвива криминалната активност (пр. телекомуникациска измама); и, * кривичното дело се овозможува со употреба на компјутери или мрежи (пр. нигериска измама, хакирање, фишинг, детска порнографија, кражба на идентитет, итн.).   Во првата категорија, компјутерот има суштинска улога во извршувањето на кривичното дело, а во последната категорија, кривичното дело може да се изврши и на друг начин, но компјутерите го олеснуваат неговото извршување.  Некои кривични дела на *новото* време се нови само во однос на модалитетот на нивното извршување; тоа се традиционални кривични дела кои се вршат внатре во дигиталната средина. Всушност, тие и не можат да се извршат надвор од виртуелниот свет, туку се генерираат внатре во него. Тоа се однесува, на пример, на компјутерската измама или компјутерското фалсификување.  Други, пак, кривични дела теоретски не се разликуваат од традиционалните кривични дела, иако се вршат со користење на компјутерски систем.  Самото тоа што тие кривични се направени *онлајн*, не ги прави овие дела некаков нов вид криминал, и тие по ништо не се разликуваат од конвенционалните кривични дела. На пример, клеветата извршена преку електронски весник, или заканата испратена преку е-пошта, дури и перењето на пари извршено преку *онлајн* банка, не е се разликуваат од истите дела извршени со конвенционални средства.  Во овој контекст, има и уште една, дури и по основна категорија, а тоа се конвенционалните *офлајн* кривични дела, кои сепак генерираат дигитални докази. На пример, извршителот на делото „снимање шамар“ *(happy slapping)* – физички напад на жртва заради снимање на делото) го снимал тоа на мобилен телефон, и потоа го постирал клипот на *Youtube*. Иако овој настан не може да се карактеризира како *компјутерски криминал,* се покренуваат истите доказни и истражни прашања како и кај т.н.. вистински компјутерски криминал.  Сепак, вообичаено, во компјутерски криминал се сместуваат дела кои се насочени против компјутерската средина или екосистем. Класичен пример на овој вид криминал се случаите на упад во податоци и упад во системот, како на пример ускратување на услуги, па дури и против правен пристап. Сите овие престапи се кривични дела против компјутерски системи, со што се загрозува доверливоста, интегритетот или достапноста на компјутерските податоци или компјутерскиот систем.  Честопати, во „реални“ услови , неколку видови кривични дела се јавуваат заедно. На пример, криминалец и се заканува на одредена компанија со ускратување на услуги на веб страницата на компанијата (кривично дело против компјутерски систем), доколку не му се исплатат средства (нов вид уцена, каде што компјутерите се користат како алатка), а заканата се врши преку е-пошта, но исто така може да се испрати и со обично писмо.  Реално гледано, се шири спектарот на модалитети: типичниот компјутерски криминал како што се *фишинг-от*  или *ботнети-те* (систем на заразени мрежи) е во постојан пораст, а се поголем е и бројот на креативни дела на компјутерски криминал чија цел е остварување профит. Исто така, има значителна пиратерија на софтвер и други дела поврзани со интелектуалните права на сопственост. Се зголемува и ширењето на материјали со детска порнографија, како и перењето на пари преку интернет. Општо земено, секој ден организираниот криминал и илегалните организации, како на пример терористичките организации, се повеќе ги користат можностите што ги нудат компјутерите. | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 46 - 49 | **Дел 4** - **Конвенцијата од Будимпешта за борба против компјутерскиот криминал** | | | | | |
|  | Конвенцијата од Будимпешта за борба против компјутерскиот криминал на Советот на Европа (ETS 185), позната и како Конвенцијата од Будимпешта, е отворена за потпишување на 23 ноември, 2001 г. во Будимпешта, а стапи на сила во јули 2004 година.  До април, 2013 г., 39 земји имаат пристапено кон Конвенцијата од Будимпешта (35 европски држави, Австралија, Доминиканска Република, Jaпонија и САД), 10 држави ја потпишаа (европски земји, Канада, Јужна Африка), а уште 8 држави се поканети да пристапат (Аргентина, Чиле, Коста Рика, Мексико, Mароко, Панама, Филипини, Сенегал). Во постапка се и барањата за пристапување и на други земји.  Конвенцијата од Будимпешта ја користат и многу други држави како насока за домашното законодавство.  Договорот е отворен за пристапување за сите држави кои се подготвени истиот да го вградат во домашното законодавство и да се вклучат во соработката.  Со Конвенцијата од државите се бара да го сторат следното:   * Да ги криминализираат дејствијата сторени против компјутерските системи (против правен пристап, противправно пресретнување, упад во податоци и упад во системот, итн.), и дејствијата што се прават преку компјутери (измама и фалсификување, детска порнографија и прекршувања на протоколи). Важно: договорот е технолошки неутрален и ги покрива однесувањата, а не технологијата или техниките (измама, а не фишинг, противправен пристап, а не хакирање, упад во системот, а не ускратување на услугите, итн.) * На органите на законот да им се обезбедат процесни алатки за зачувување на електронски докази (итно зачувување, претрес и заплена, итн.). Важно: овие мерки се однесуваат не само на компјутерскиот криминал туку и на секој друг вид криминал во кои има електронски докази на компјутерски систем * Да се ангажираат во делотворна меѓународна соработка со комбинација на итни и времени мерки, формална взаемна помош и 24/7 мрежата на лицата за контакт   Сите овие мерки – особено алатките на процесното право - треба да ги исполнуваат барањата во врска со човековите права и владеењето на правото. Затоа, Членот 15 (услови и заштитни мерки) е од особена важност.  Се на се, Конвенцијата од Будимпешта им овозможува на Владите да ги исполнат позитивните обврски за заштита на поединци од (компјутерски) криминал, а истовремено да ги почитуваат човековите права на поединците при преземањето мерки против компјутерскиот криминал.  Досегашните резултати се следни:   * Глобален процес на законодавни реформи * Зголемени мерки на казненото правосудство * Поголема доверба и соработка помеѓу страните * Глобален дофат, глобално влијание: 56 земји ратификувале, потпишале, се поканети за членство. Соработка со најмалку 50 други земји * Катализатор за градење капацитети * Поголема правна сигурност и доверба од приватниот сектор * Суштински елемент на нормите на однесување во компјутерскиот простор * Придонес кон човековите права и владеењето на правото во компјутерскиот простор * Ве штити вас и вашите права | | | | | |
| 51 | **Дел 5 - Некои нелегални *онлајн* активности**  Целта на овој дел е накратко да се даде опис на кои криминални активности што постојат на мрежите. | | | | | |
| 52 | *Фишинг* (ловење на лозинки) е техника што се користи за намамување на лица да испраќаат лични информации на други лица. Овие информации подоцна се користат за кражба или измама. Обично, сторителите на делото користат е-пораки да ја намамат жртвата, од која што добиваат лични податоци, вклучително и лозинки или други овластувања за пристап. Понекогаш, оваа техника се користи за пренасочување на корисниците кон злонамерни или лажни веб страници. | | | | | |
| 53 | *Спам* (небарана пошта) станува се поголем проблем. Се работи за несакани пораки што се испраќаат во милионски бројки. Лицата кои ги добиваат овие пораки не можат да го избегнат нивното примање. Понекогаш, тие пораки се испраќаат само за маркетиншки цели, но, честопати тие се вектори за *малвер* (злонамерен софтвер) со кои се заразуваат компјутерите.  Вообичаено, жртвата не го познава испраќачот, не бара да добива такви пораки, ниту пак дала овластување да и се испраќаат такви пораки. | | | | | |
| 54 | Терминот *малвер* е спој на два термина: „злонамерен" + „софтвер“. Се работи за софтвер изработен со цел да се оствари пристап до одреден компјутерски систем без согласност на сопственикот или корисникот, или со цел истиот да се оштети. Жртвата може без знаење да се зарази со малвер, преку е-пошта прилози или слики вметнати во пораките.  Ваквиот вид софтвер е обично штетен софтвер што се вметнува во компјутерот на жртвата без нејзина согласност со цел да извршува штетни функции или активности | | | | | |
| 55 | *Вирусите* се посебен вид на малвер. Вообичаено, вирусот е софтвер што може да се реплицира од една во друга датотека и да се смести во одреден систем – во тврдиот диск или во друг медиум за складирање на податоци. Вообичаено, вирусот се шири кога заразената датотека се копира или извршува. Се разбира, тоа се врши без согласност (ниту знаење) на корисникот/администраторот и целта е да се предизвика штета на компјутерскиот систем. | | | | | |
| 56 | *Црвчето* е многу слично на вирусот. Црвче е софтвер што исто како и вирусот може да се реплицира, да се инсталира во одреден систем и да ги користи ресурсите на тој систем. Се разликува од вирусот по тоа што се шири низ мрежата без да мора да се приклучи на каква било датотека. | | | | | |
| 57 | *Адвер* (софтвер за реклами)*е* исто така малвер. Се работи за софтвер што автоматски покажува или презема реклами, без согласност или интервенција на корисникот. Честопати се дистрибуира заедно со софтвер достапен за бесплатно преземање.  Некои видови адвер се поопасни од други, бидејќи го следат системот, како на пример интернет сајтови што ги посетува корисникот и неговите склоности | | | | | |
| 58 | *Спајвер* (софтвер за шпионажа) е најинтрузивниот вид на малвер. Се работи за софтвер што се инсталира на компјутерскиот систем без дозвола од корисникот со цел да следи и контролира како корисникот го користи системот. На тој начин спајверот собира информации за корисникот на тој систем, а потоа ги испраќа тие информации на трети страни. Негова конкретна задача е да се крие во компјутерот на жртвата и да ги пренесува информациите што ги собира до трети страни. | | | | | |
| 59 | *Тројанци* (тројански коњи) е име инспирирано од надалеку познатиот коњ што го изградил Одисеј, и го подарил на градот Троја за да ги отвори вратите на градот од внатре. Исто така, тоа е име на злонамерен софтвер што извршува непосакувани за корисникот функции, без негово знаење. Овој вид малвер може да уништува податоци, дезактивира безбедносен софтвер, овозможи пристап од далечина / задна врата ( неовластен влез во компјутер) или да презема и инсталира друг малвер.  Исто како и првобитниот Тројански коњ, овој софтвер има тајно да влезе во компјутерот и да овозможи пенетрација од надвор. | | | | | |
| 60 | *Ботнет* е акроним од *robot networks* (мрежи на роботи) и се користи за означување на мрежа на компромитирани компјутери (зомби), која е под контрола на одредено лице или организација, со цел да се користи за незаконски активности.  Ботнетот се гради така што сопственикот на ботнетот заразува други компјутери со малвер. Сите заразени компјутери се под контрола на софтвер што овозможува автоматизација на операциите во мрежата. Сопственикот на мрежата ги контролира активностите и може да издаде наредба за неактивирање, се додека не се јави потреба од тоа.  Ботнетот може да се состои од милиони „зомби“ компјутери кои добиваат инструкции да испраќаат спам или малвер или да вршат напад на инфраструктура. Ботнетите се користат за најразлични видови криминални активности, и затоа се нарекуваат „џебно ноже на компјутерскиот криминал“. | | | | | |
| 62 | **Дел 6 - Преглед** | | | | | |
| 63 | Што е компјутерски криминал и зошто претставува проблем.  Закани, трендови и алатки на компјутерскиот криминал и одговорот на овој феномен.  Реалностите опфатени со терминот компјутерски криминал, и концептите на кривичните дела од ваков вид согласно повеќето законодавства и меѓународни стандарди.  Потребата и предностите од усогласување на националните законодавства со меѓународните инструменти, особено Конвенцијата од Будимпешта. | | | | | |
|  | **Практични вежби (доколку се предвидени)**  За оваа сесија не се предвидени практични вежби, бидејќи нема гаранција дека степенот на технологијата и пристапот до интернет ќе овозможи одржување на вакви вежби во сите простории каде што се одржува обуката.  Во иднина, обучувачите би можеле да ја дополнат обуката со вклучување на вежби, доколку за тоа постојат соодветни услови. | | | | | |
|  | **Проверка на знаењето**  Не е предвидена конкретна проверка на знаењето,освен она што е претходно предвидено со обуката. Нема барања за официјално оценување. | | | | | |
| Сесија 1.1.3, 1.2.2 & 1.2.5 – Технологија | | | | | Времетраење: 330 минути |
| **Потребни ресурси:**   * Персонален компјутер или преносен компјутер со Windows 7 и со MS Office 2010 * проектор * Пристап до интернет (доколку постои) * PowerPoint презентација * Примероци на компјутерски хардвер (доколку постојат) * Видео клип (*Воини на интернет*) | | | | | |
| **Цел:**  Во оваа сесија се дадени информации за технологијата со која што ќе се среќаваат судиите и обвинителите во текот на нивната работа, и која што криминалците често ја користат за вршење кривични дела, а органите на законот за нивно откривање. Целта на сесијата е да им овозможи на учесниците да стекнат соодветно познавање на технологијата за да можат поделотворно да ја извршуваат својата работа.. | | | | | |
| **Задачи:**  На крајот на оваа сесија учесниците ќе можат да:   * Ги објаснат разните видови влијанија што технологијата ја има врз криминалот * Ги наведат составните делови на компјутерските системи * Разликуваат различни видови уреди за складирање на податоци * Ги одмерат последиците од експоненцијалното зголемување на капацитетите за складирање податоци во контекст на кривичното право * Идентификуваат различни компјутерски оперативни системи * Ги објаснат основите на функционирањето на мрежите * Ја објаснат функцијата на интернетот * Идентификуваат најмалку 5 главни интернет апликации * Објаснат како се развива интернетот, од неговите почетоци до денес. * Разликуваат различни интернет апликации * Идентификуваат како криминалците ги користат разните интернет апликации | | | | | |
| **Време**  **Траење** | | **Содржина:** | | | |
| 30 мин.  60 мин.  60 мин.  60 мин.  60 мин.  30 мин.  30 мин. | | Вовед и отворање (Агенда и задачи на сесијата)  Дел 1 – Како работат компјутерите  Дел 2 – Како работи интернетот  Дел 3 – Интернет услуги  Дел 4 – Други релевантни интернет апликации  Дел 5 – Интернет криминал  Дел 6 – Преглед | | | |
| **Слајд** | | **Содржина:** | | | |
|  | | **Вовед**  **Технологија за судии и обвинители**  Оваа сесија треба да обезбеди рамка според која обучувачите ќе изготвуваат материјали кои ќе се предаваат како дел од една поширока програма за обука. Таа не може да се покрие се, со оглед на тоа дека технологијата се развива со таква брзина што секоја техничка спецификација би била застарена во моментот на објавување. Судиите и обвинителите мора да имаат соодветното познавање за техничките аспекти на предметите на кои работат, и тоа е од суштинско значење за запазување на принципот на правичност на правосудниот систем. Во текот на оваа сесија ќе се направи преглед на релевантните технолошки аспекти и нивното значење во контекст на системот на кривично право. Подготвена е и PowerPoint презентација, што обучувачите можат да ја користат како ресурс.  Обезбеден е уште еден материјал. Тоа е видео клипот „Воини на мрежата“ кој ќе им овозможи на учесниците подобро и појасно да сфатат како функционира мрежата. Видеото може да се најде на www.warriorsofthe.net и е достапно на следните јазици: англиски, германски, француски, холандски, хебрејски, шведски, италијански, португалски, унгарски, чешки, шпански и украински.  Во оваа сесија се опфатени информации за технологијата со која ќе се среќаваат судиите и обвинителите во текот на нивната работа, а која што криминалците ја користат за вршење кривични дела, а органите на законот за нивно детектирање. | | | |
|  | | **PowerPoint**  Подготвена е PowerPoint презентација со белешки за обучувачот како дополнување, и како пример според кој обучувачот може да подготви сопствен материјал за покривање на зададените задачи. Да потсетиме дека обучувачот е одговорен за подготовката на наставните материјали, кои треба да се ажурирани и релевантни за слушателите. Обучувачот не треба да се потпира само врз материјалите што ги подготвил друг обучувач. | | | |
| 2 - 3 | | **Агенда**  На слајдовите се дадени деловите што ја сочинуваат оваа сесија. Обучувачот треба да ги помине, и да се задржи на некои специфични аспекти кои смета дека се важни за дадената група студенти. Обучувачот треба да објасни на кој начин ќе се презентира материјалот, и дека е предвидено време за интеракција и прашања. Треба да се нагласи дека обуката е конципирана како интерактивна, и дека подразбира постојана активност на учесниците. Обучувачот треба да појасни дали е предвидено оценување, како тоа ќе се одвива, и која е преодната оценка (во оваа пилот програма не се предвидува оценување). | | | |
| 4 | | **Цели на сесијата**  Од голема важност е учесниците да ги разберат задачите што се задаваат во оваа сесија. Тоа се “SMART” задачи, кои на учесниците треба детално да им се објаснат пред почетокот на сесијата со помош на информациите од слајдот. | | | |
| 5 - 54 | | Дел **1** – **Како функционираат компјутерите**  Кон крајот на сесијата, учесниците ќе треба да знаат да:   * Ги набројат составните делови на компјутерскиот систем * Идентификуваат различни видови уреди за складирање податоци * Ги одмерат последиците од експоненцијалното зголемување на капацитетите за складирање податоци во контекст на кривичното право * Идентификуваат различни компјутерски оперативни системи | | | |
| 5 | | Со цел судиите и обвинителите целосно да го сфатат влијанието на технологијата врз криминалот, потребно е тие да стекнат основно знаење за тоа како функционира таа технологијата . Особено во предметите со дигитална форензика, ваквото знаење ќе им овозможи подобро разбирање на контекстот, и поинформирано донесување одлуки. Во оваа сесија се дадени основни информации за компјутерите, нивните компоненти, складирањето податоци и значењето на можноста за складирање огромно количество податоци на поединечни уреди. И повторно, обучувачот треба да настојува сесијата да биде што повеќе интерактивна и преку презентираните информации да ги охрабри учесниците да сфатат како технологијата влијае врз нивната работата, како да се справуваат со огромно количество податоци, и како тие делотворно да се презентираат во правосудниот системот.  Доколку е можно, обучувачот треба да покаже примери на хардверот за кој се говори во оваа сесија, со цел учесниците да се запознаат и добијат можност сами со да работат со нив.  Постојат уште многу други компјутерски компоненти што не се разгледуваат во оваа сесија, а внесени се само оние кои се најзначајни за целите на курсот. При изработката на програмата за обука, се препорачува да се објаснат и компонентите што не се внесени, но тоа зависи од нивото на знаење на поединците во групата. На пример, се очекува дека повеќето учесници ќе знаат што е тастатура и глувче, и како тие се користат. Сепак, обучувачот не би требало да го прецени знаењето на учесниците. Елементите што би можеле да се додадат на овој список се: печатари, скенери, веб камери, модеми, звучници, компјутерска и видео телефонија и разни уреди за складирање податоци и мрежни поврзувања, како и надворешни порти како на пример *Firewire* и *USB*.  За подетални информации за компјутерски хардвер види [http://computer.howstuffworks.com/computer- hardware-channel.htm](http://computer.howstuffworks.com/computer-%20hardware-channel.htm), каде што има и фотографии преку кои овие концепти полесно ќе се разберат. Доколку тие да се употребат во програмата за обука, не заборавајте да побарате дозвола да ги користите овие информации, | | | |
| 6 | | Преку овој слајд се гледа дека и најголемите познавачи на технологијата не можеле да ги предвидат промените што таа ги носи. Учесниците веројатно не се единствени кои не го разбираат влијанието на технологијата врз нивната работа, а цитатите од овој слајд имаат и за цел да ги охрабрат да не се плашат од присуството на технологијата во правосудниот систем, туку напротив, да ја прифатат заедно со сите потребни заштитни мерки. | | | |
| 7 | | Како вовед во објаснувањето за компонентите на компјутерот, обучувачот треба да даде краток преглед на развојот на компјутерите, од нивните почетоци како самостојни уреди, развивањето во централни компјутерски терминали, а потоа и светот на мрежите. | | | |
| 8 | | **Компјутерски компоненти**  Обучувачот треба да објасни дека компјутерот се состои од многу компоненти и дека е потребно судиите и обвинителите да ги знаат имињата и функциите на овие компоненти, бидејќи ќе се повикуваат на нив во изјавите и доказите на сведоците.  Дадено е кусо објаснување на секој составен дел: | | | |
| 9 - 10 | | Матична плоча или главна плоча или системска плоча на компјутерот е централната електропроводна плоча на компјутерот. Сите други компоненти и надворешни уреди се приклучуваат на неа. Функцијата на матичната плоча е да пренесува информации помеѓу сите нив. Во матичната плоча се наоѓа oсновен влез-излез систем – BIOS , едноставен софтвер што се активира кога ќе се вклучи компјутерот. На неа се приклучуваат и сите други компоненти, на пример: меморија, централна процесирачка единица, графичка картичка, звучна картичка, тврд диск, дискетни единици и други надворешни порти и надворешни уреди.  Порти/канали за проширување – канали на задниот дел на компјутерот каде што можат да се приклучат звучни картички, видео картички, безжични адаптери и сл. | | | |
| 11 - 13 | | ***CMOS*** и ***BIOS*** се термини што честопати се користат наизменично; *BIOS* може да се сфати како софтвер, а *CMOS* како хардвер на кој работи *BIOS. CMOS* е кратенка од Комплементарен полупроводник од метален оксид. Се чита “симос“.  **CMOS** е хардвер што ги врши наједноставните функции и основни задачи за вклучување на компјутерот. *CMOS* на пример, води сметка за часовникот на компјутерот и овозможува интерфејс со другите делови на компјутерскиот хардвер, со што на *BIOS* му се овозможува да ја врши својата работа. Потребно му е многу малку напојување за да работи.  ***BIOS*** е кратенка од основен систем за влез излез, и се чита „бајос“. *BIOS* е интерфејс што му овозможува на корисникот да направи мали промени во матичната плоча на компјутерот, централната процесирачка единица, меморијата и други уреди. Стандардните BIOS подесувања обично се наместени како што треба. Едно од најчестите подесувања што се прават на *BIOS*, во форензична смисла, е да се измени редоследот по кој што компјутерот ги бара уредите за вклучување. Обично, форенсичките аналитичари користат софтвер од компакт диск (ЦД), и го менуваат BIOS за да компјутерот се вклучи од ЦД, а не од тврдиот диск, бидејќи самото вклучување од тврдиот диск доведува до промена на податоците. | | | |
| 14 | | Единицата на напојување со електрична енергија (***P****ower* ***S****upply* ***U****nit - PSU*) во компјутерот ги регулира и напојува со струја компонентите што се наоѓаат во куќиштето. Стандардното напојување со струја од 110V или 220V наизменична струја се преиначува во еднонасочна струја со волтажа соодветна за напојување на компонентите на компјутерот. Изворите за напојување имаат специфична моќност што се мери во Вати, а стандардниот извор за напојување треба да овозможи околу 350 Вати. Што е поголем бројот на компоненти на персоналниот компјутер толку е поголема потребата од поголемо напојување. | | | |
| 15 | | ***CPU*** е кратенка за централната процесирачка единица на компјутерскиот систем (ЦПЕ). Честопати се меша со куќиштето или шасијата на компјутерот. Но, ЦПЕ е внатрешна компонента на компјутерот и не може да се види од надвор. Првите ЦПЕ почнуваат да се користат во раните 1960-ти години. Со воведувањето на интегрираното коло во доцните 1970-ти години, стана можно да се произведуваат и помали ЦПЕ. На тој начин, големите, кабасти компјутери за чие што сместување биле потребни цели соби се трансформираат во пофлексибилни персонални или преносни уреди. ЦПЕ работи така што извршува серија на зачувани инструкции, познати како програма. Повеќето ЦПЕ ја користат архитектурата на Фон Нојман, што значи дека ЦПЕ мора да дојде најде, декодира, изврши, и повторно запише податоци со доста голема брзина. Лаички кажано, ЦПЕ е мозокот на компјутерот, т.е. се што прави компјутерот, тоа го прави со помош на ЦПЕ. | | | |
| 16 | | Меморија – компјутерската меморија технички претставува го означува складирањето на електронски податоци во каква било форма, иако најчесто се користи за времените форми на складирање до кој може брзо да се пристапи. Целиот процес би бил многу спор доколку ЦПЕ мора да бара податоци од тврдиот диск за секоја инструкција што треба да ја изврши; затоа, многу податоци времено се складираат во времена меморија, каде што може побрзо да се дојде до нив. Таа меморија е позната како меморија за директен/произволен пристап или РАМ меморија. ЦПЕ побарува податоци од РАМ меморијата, ги процесира и повторно ги запишува во РАМ. Ова се одвива милиони пати на секунда. При форензичкото фаќање на компјутерски податоци, важно е да се знае дека податоците од времената меморија нема да се зачуваат доколку компјутерот се исклучи од изворот на напојување, што е честа постапка при пребарувањето и заплената на компјутерски системи. Затоа сега, при пребарувањето на компјутери, органите на законот многу почесто се обидуваат да фатат податоци во РАМ, пред да го исклучат компјутерот од струја. Оваа постапка е позната како „форензичка обработка на живи податоци“ и се врши се почесто, со оглед на тоа дека обемот на податоци што може да се загуби ако тоа не се направи е многу поголем од обемот на податоци што до пред само неколку години можеше да се најде на еден тврд диск. | | | |
| 17 | | УСБ (Универзална сериска магистрала) – приклучоците за УСБ, што ги има на повеќето компјутери, овозможуваат едноставно приклучување на голем број уреди на компјутерот, како на пример, глувче, печатар, надворешни уреди за складирање и мобилни телефони. Тоа е моментно најчестиот начин за приклучување на надворешни уреди на компјутер. Порано постоеле други начини за поврзување, на пример паралелни или сериски порти, но тие се попроблематични со оглед на ограничениот број уреди што можеле да се поврзат во исто време, и бавниот пренос на податоци, за разлика од УСБ. Со УСБ е можно на компјутерот да му се приклучат до 127 уреди. Поради тоа што УСБ уредите се лесни за користење, тие денес најчесто се користат во дигитално-форензичките истраги. | | | |
| 18 - 20 | | Повеќето компјутери имаат барем еден тврд диск, а многу од нив имаат и повеќе. Поголемите компјутери, на пр. централните компјутери, обично имаат повеќе тврди дискови. Денес често се случува и други уреди, како на пример *CCTV* и уредите за пуштање музика да имаат тврд диск на кои се чува голема количина податоци. Овие дискови имаат тврди плочи на кои што се чуваат информациите, и податоците можат лесно да се бришат и презапишуваат, но структурата на дискот се зачувува, така што и податоците се одржуваат подолг временски период. Податоците се складираат на површината на плочата, во сектори и патеки. Патеките се концентрични кругови, а секторите се пресечен дел од нив. Податоците се складираат на тврдиот диск како фајлови/датотеки, и тие, едноставно кажано, претставуваат група бајтови. И програмите се фајлови/датотеки, и за да се користат треба да ги повика ЦПЕ. | | | |
| 21 | | ***SSD*** е единица за складирање во полупроводнички дискови, која понекогаш се нарекува и полу проводнички диск или електронски диск. Тоа е уред за чување податоци во тврда состојба, и пристапувањето е исто како и кај тврдиот диск. ***SSD*** се разликува од конвенционалните магнетни дискови, како што се тврдите дискови или дискетите кои се електро- механички уреди, и имаат дискови што се вртат и подвижни глави за читање/пишување. Наспроти тоа, ***SSD*** користи микро чипови кои ги задржуваат податоците во стабилни мемориски чипови и немаат подвижни делови. За разлика од електро-механичкиот тврд диск, електронските дискови се помалку подложни на физички удари, се потивки, побрзо се пристапува до нив, латентноста им е подобра, но и се поскапи по единица гигабајт. ***SSD*** уредите за складирање се нов предизвик за форензичарите, бидејќи податоците се складираат на сосема нов начин. | | | |
| 22 | | На ЦД/ДВД/Блуреј дисковите може да се зачува различна количина на податоци, и обично се користат за чување музика, видеа или компјутерски датотеки наменети за дистрибуција. Едно ДВД има еднаква големина како и ЦД-то, но задржува околу 7 пати повеќе податоци од него. Еден Блуреј диск пак, кој што може да се користи за складирање ХД содржина, може да прими 10 пати повеќе податоци од ДВД-то. Со други зборови, на нив може да се складираат повеќе податоци отколку што тоа беше можно на тврдите дискови до пред само неколку години.  Податоците на сите овие дискови поинаку се складираат отколку на тврд диск, и податоците што се чуваат на нив се постабилни од оние што се чуваат на тврд диск. | | | |
| 23 | | **Складирање податоци**  Во кривичните и граѓанските постапки се повеќе и се почесто се изнесуваат докази од компјутери или други дигитални уреди, како на пример, од мобилни телефони. Како што технологијата станува се поприсутна во општеството, така се повеќе ќе се употребуваат уреди кои содржат дигитални докази што можат да се користат во постапките. Веќе гледаме дека се испитуваат и домашните уреди за прибирање на вакви докази.  Според тоа, од голема важност е судиите и обвинителите да ги разберат прашањата што се поврзани со интегритетот и прифатливоста на дигиталните докази. Добра почетна точка за тоа е тие прво да спознаат како се чуваат податоци и како истражителите доаѓаат до нив.  Електронските или дигиталните податоци се чуваат на повеќе начини. Најмногу за таа цел се користи тврдиот диск на компјутерот, а тоа е воедно и најлесно за валидирање. Типичниот приод за зачувување и добивање дигитални докази започнува со испитување на уредите во статична состојба. Тоа значи дека компјутерот е исклучен и дека податоците не се во нестабилна состојба. Дигиталните форензичари се добро запознаети со барањата дадени во меѓународните и националните упатства за работење со ваков вид докази. Едно такво упатство е и „Заплена на е-докази“, подготвено со финансиска поддршка од ОИСИН програмата на Европската Комисија, кое може да се најде на: <http://www.e-evidence.info>. Во ова упатство се дадени основните принципи согласно кои работат повеќето органи на законот. Важно е судиите јасно да разберат како се складираат податоци, и како се доаѓа до доказите што се изнесуваат на суд. Има повеќе ресурси што лицата кои подготвуваат обуки можат да ги користат за прибирање информации за складирање на тврд диск, кои можат да се искористат во рамките на обуката. Еден таков пример може да се најде на <http://www.storagereview.com/hard_disk_drive_reference_guide>. Овде претежно се зборува за стабилно чување, на пример на магнетски медиуми, медиуми за оптичко складирање, флеш меморија и сл.  Се почесто се случува доказите да се земаат од нестабилни извори, на пример од РАМ или уреди како што се мобилните телефони, каде што податоците се понестабилни. Судиите треба да ја знаат разликите во однос на начинот на кој се прибираат ваквите податоци, и можните последици по интегритетот на доказите. Во врска со нестабилните податоци, најважно е да се знае дека ваквите податоци обично се губат кога уредот ќе се исклучи, а со тоа и можноста да се дојде го многу важни информации што можат да послужат како доказ. Техниките што се користат за прибирање на вакви информации треба да се во согласност со општите принципи за заштита и поврат на такви податоци. Исто така, нестабилни податоци најчесто се прибираат од вмрежени системи што не можат да се исклучат за да врз нив се изврши статична анализа. | | | |
| 24 | | **Меморија и складирање на податоци**  На овој слајд е даден приказ на термините што се користат за карактеризирање на податоците и нивната големина. Се работи за вовед во материја што понатаму ќе им биде потребна на учесниците за да го разберат делот каде што се обработуваат разни уреди за складирање и нивниот капацитет. | | | |
| 25 | | **Оперативни системи**  За да можат да работат, компјутерите и другите дигитални уреди мора да имаат оперативен систем. Оперативен систем е софтверска програма што му овозможува на хардверот да комуницира со софтверските програми. Без оперативен систем, компјутерот не може да работи. Има повеќе типови оперативни системи, во зависност од тоа за каков тип на компјутер или друг дигитален уред се работи.  Оперативни системи кои денес најчесто се користат се: Windows, Unix/Linux и Apple Mac. Постојат и други системи кои се користат кај други уреди како што се на пр. личните дигитални асистенти или мобилните телефони. Тие се обично помала верзија на големите системи, иако сега се почесто се развиваат и системи прилагодени за помали уреди.  Повеќето апликации за компјутери се пишуваат за конкретни оперативни системи, иако сега се почесто ги има за повеќе платформи.  Судиите и обвинителите траба да го знаат значењето на оперативните системи, и да знаат дека разни оперативни системи различно се однесуваат. Има многу извори каде што лицето што ја подготвува обуката може да добие информации за оперативните системи и задачите во врска со нив зададени со оваа сесија. Еден од нив е: <http://en.wikipedia.org/wiki/Operating_systems> | | | |
| 26 - 28 | | **Оперативни системи** – овие слајдови имаат за цел да ја објаснат целта на оперативните системи, да ги прикажат оперативните системи кои денеска најчесто се користат и статистичките податоци во однос на нивното користење. Обучувачите треба да имаат на ум дека овие податоци треба да се ажурираат, особено информациите на слајд 38, кој треба да се ажурира еднаш годишно. | | | |
| 29 | | **Дигитални уреди**  Сесијата посветена на дигиталните уреди има за цел да им овозможи на судиите и обвинители да ги идентификуваат разните видови уреди што можат да содржат докази. Ова е вовед во дискусијата за тоа колку податоци можат да се складираат на одредени уреди, и за предизвиците што количеството податоци ги носи во правосудниот систем. | | | |
| 30 - 38 | | Слајдовите во рамките на оваа сесија се многу опширни. Обучувачите треба сами да видат колку од нив ќе им бидат потребни за да ги постигнат задачите на сесијата. Целта на оваа сесија не се разликите помеѓу различните видови уреди, на пример мобилните телефони,палците или компјутерите, и предизвиците при пребарувањето, заплената и испитувањето на доказите од таквите уреди. Обучувачите треба да ги искористат оние примери со кои ќе се олесни совладувањето на зададените задачи.  Во оваа фаза од обуката, учесниците се веќе во голема мера запознаети со дел од техничките аспекти. Овие слајдови треба да им дадат една додатна перспектива што нема да им биде тешко да ја разберат, а воедно е и интересна.  Овде е важно да им се укаже на различната природа на уредите во кои што може да се складираат податоци, и каков предизвик е тоа за правосудниот систем. Обучувачите треба да размислат за примери на невообичаени уреди што биле клучен извор на докази во одредени кривични предмети. | | | |
| 39 | | **Малку поинакви компјутери**  Оваа кратка сесија се надоврзува на претходната, и служи за продолжување на дискусијата за дигиталните уреди. И повторно, обучувачот може сам да одлучи кои и колку од дадените слајдови ќе ги користи,а со цел да ја пренесе пораката дека доказите можат да се најдат на најразновидни уреди, и дека уредите на кои што ќе наидат не секогаш се тоа на што наликуваат.  Важно е во рамки на оваа сесија е да се предочи дека уредите на кои можат да се складираат илјадници страници документација што може да се користи како доказ се многу лесно достапни. | | | |
| 40 - 45 | | Овде е важно да се укаже на различната природа на уредите на кои може да се складираат податоци, и предизвиците за правосудниот систем во контекст. Обучувачите треба да размислат за примери на невообичаени уреди што биле клучен извор на докази во одредени кривични предмети. | | | |
| 46 - 54 | | **Колку податоци може да се чуваат на нив**  Ова е важна сесија, во рамки на која техничките информации за дигиталните уреди се преточуваат во реалност: колку информации можат да се чуваат на нив, и што тоа значи во однос на документацијата што може да произлезе од нив. Ова е вовед во дискусијата што ќе се води подоцна во врска со интегритетот и прифатливоста на дигиталните докази и нивните производи.  Фотографија дадена како пример има за цел да им појасни на учесниците колку податоци може да се чуваат на одредени уреди. Обучувачите можат и треба да дадат и други примери кои се релевантни за нивните земји.  Друга важна работа што треба да се објасни е дека овие уреди веќе не се скапи, и дека има различни уреди на кои може да се чуваат огромно количество податоци.  Обучувачите исто така треба да нагласат дека тоа може да биде предизвик за одлуките што ги донесуваат судиите и обвинителите, затоа што огромното количество податоци и печатен материјал може да го оневозможи ефективното работење. | | | |
| 55 - 81 | | **Дел 2 – Како работи интернетот**  На крајот на оваа сесија учесниците ќе можат да:   * Објаснат како се развива интернетот, од неговите почетоци до денес * Ја објаснат функцијата на интернетот * Разликуваат различни интернет апликации * Идентификуваат најмалку 5 главни интернет апликации * Идентификуваат како криминалците користат разни интернет апликации | | | |
| 55 | | Во оваа сесија се даваат основни информации за историјата, функционирањето и услугите што се достапни преку интернетот, како и информации што ќе им овозможат на учесниците да ги разликуваат и јасно да ги дефинираат компонентите на интернетот и како тој влијае врз системот на кривично право. Обучувачите треба да обезбедат практични примери со кои ќе се дополнат и дообјаснат техничките податоци што се дадени во оваа презентација. | | | |
| 56 - 57 | | Терминот ИНТЕРНЕТ настанал со поврзување на два збора *INTERconnected NETwork* (ИНТЕРконектирана МРЕЖА). Интернетот се користи за вршење многу кривични дела, како на пример: хакирање, ширење вируси и фишинг, но и за поконвенционални кривични дела, како што е измамата. За да судиите бидат во можност делотворно да работат на вакви предмети, потребно е тие да ги разберат основите на интернетот и неговите апликации, како што се светската мрежа и електронската пошта. Оваа презентација е вовед во темата и нуди образец за успешен модул за обука. | | | |
| 58 - 59 | | **Краток историјат на интернетот**  Историјата на интернетот започнува како ARPANET во 1960-ите години. Релевантноста на овој податок можеби не е веднаш очигледна, но фактот што интернетот никогаш не бил дизајниран за да биде безбеден дава објаснување за тоа зошто криминалците доста лесно можат да го злоупотребуваат овој систем. Првите физички врски биле воспоставени во 1969 година, со 4 универзитети како јазли. Првата порака по електронска пошта била испратена во 1972 година, а веќе наредната година бил создаден и новиот протокол за комуникација *TCP/IP*, кој денес е основата врз која што се одвива интернет комуникацијата. Развојот на интернетот каков што го знаеме денес не започнува спектакуларно, со оглед дека се работело за неповрзани мрежи со само неколку мрежни премини. Потоа, се развива паркетното префрлување на податоци и соодветниот протокол за работа, со кои се овозможува соединување на повеќе мрежи во една супер-рамка на мрежи.  На овој начин се овозможило се поголемо поврзување, прво кај поразвиените мрежите во западниот свет, а потоа и во другите делови на светот. Нееднаквиот на раст кај развиените земји и земјите во развој доведува и до дигитален јаз, што постои до ден денес.  Потоа следи комерцијализација на интернетот и формирањето на приватни испорачувач и/провајдери на интернет услуги (*Internet Service Providers*) во 1980-ите години. Со тоа се популаризира пристапот, особено во текот на 1990-ите години. Интернетот врши огромно влијание врз трговијата и културата. Сега, преку електронската пошта, сајтовите на социјалните мрежи, форумите за дискусија и светската мрежа можна е инстант комуникација. Интернетот продолжува да расте, поттикнат од трговијата, огромното количество *онлајн* информации и знаење. Започнува времето на новатa мрежа - Веб 2.0. | | | |
| 60 | | Обучувачот треба на учесниците да им обезбеди доволно информации за да тие ги разберат основите на работењето на мрежа и неговите ограничувања. Учесниците треба да ги знаат разликите помеѓу локалните мрежи и пошироките мрежи што покриваат поголема површина. На овие слајдови се дадени основните информации во врска со тоа. Обучувачите треба да изнајдат соодветни примери, и да ги поттикнат учесниците на дискусија во врска со различните видови мрежи и развојот на интернетот. Во оваа фаза треба да се даде објаснување на некои термини кои што често се среќаваат на пример порти и проток (*bandwidth*). Учесниците треба да се поттикнат да ги споделат сопствените искуства, на пример за пристапот до интернет што го имаат дома или на работа. | | | |
| 61 | | **Локална мрежа - ЛАН мрежа (Local Area Network (LAN)) –** е компјутерска мрежа која покрива мала географска површина, како дом, канцеларија или група на згради, на пример училиште. Карактеристиките на локалните мрежи се побрза стапка на пренос на податоци, помал географски опфат, како и фактот дека овие мрежи не бараат изнајмување на телекомуникациска линија..  **Регионална мрежа – (Wide Area Network (WAN))** – е компјутерска мрежа која покрива широка област (на пример, било која мрежа чии комуникациски врски ги преминуваат границите на градовите, регионите или државите), или едноставно кажано тоа е мрежа која користи рутери и јавни комуникациски врски.  Споредете ги овие мрежи со персоналните мрежи -personal area networks (PANs), обласна мрежа -campus area networks (CANs), или општинска мрежа - metropolitan area networks (MANs), кои вообичаено се ограничени на една соба, зграда, област или конкретна општинска територија (на пример еден град). Пример за најголема и најпозната регионална мрежа-**WAN е** ИНТЕРНЕТОТ. | | | |
| **62** | | **Порти -** претставува крајната точка или „канал“ за мрежна комуникација. Бројот со кој е означената портата овозможува различните апликации на истиот компјутер да ги користат мрежните ресурси без да си попречуваат меѓусебно. Портите се „виртуелни“- тие НЕ се приклучокот во кој се вклучувате!  **Проток-Bandwidth** - претставува обем на информациите кои може да се пренесат преку телефонска линија, кабловска линија, сателитска врска, итн. Колку што е поголем протокот, толку е побрза вашата конекција и со тоа вашето работење на интернет се доближува до преземање на податоците веднаш во дадениот момент, како да гледате ТВ емисија. | | | |
| 63 | | **Контролорот за мрежниот интерфејс - Network Interface Controller (NIC)** е електронска плоча или картичка која се инсталира на компјутерот со кој на компјутерот му се овозможува да се поврзе со мрежата.  **Контрола на пристап на медиум (MAC адреса) - (Media Access Control (MAC))** е квази-единствен идентификатор кој на најголем дел од мрежните адаптери, односно картички за мрежен интерфејс (NIC) им го доделува производителот за идентификација и при тоа им доделува единствена вредност.  **Мрежен разводник (Network Hub)** – или поврзувач е уред за поврзување на повеќе преплетени парови на етернет уреди со оптички кабли, со што функционираат како единствен мрежен сегмент. Разводникот работи на физичкиот слој (слој 1) од OSI моделот (референтен модел за отворено поврзување на системи) и често истовремено со овој термин се користи и терминот „слој 1 преклопник“ (‘layer 1 switch’). Уредот така претставува форма на повеќе-портен повторувач. Мрежните разводници исто така се одговорни за праќање сигнал за заплетување до сите негови порти доколку открие судир. | | | |
| 64 | | **Мрежен преклопник (Network Switch) -**  е уред за компјутерски мрежи кој е сличен на разводникот. Преклопниците главно се користат за да поврзат групи на мрежни уреди. За разлика од разводниците, преклопниците користат податоци кои веќе се чуваат во базите на податоците за да запомнат која (Контрола на пристап на медиум-MAC)MAC адреса се користи за која порта на преклопникот. Така можат да ги испраќаат целните групи на податоци. Во минатото било побрзо да се користат Слој 2 техниките, кога во контекст на асоцијативна меморија (content addressable memory (CAM) може да се видат само MAC адресите. Со појавата на трислојната асоцијативна меморија (TCAM), стана подеднакво брзо да се најде Интернет протокол адресата или МАС адресата.  **Рутер - насочувач (Router) –** е уред кој ја определува следната точка во мрежата од која групата на податоци треба да се прати кон нејзината одредница. Тој мора да биде поврзан со барем две мрежи. Тој е интелигентен и работи според табели на насочување. Иако е лоциран на капијата на мрежата (gateway), тој не мора да биде капијата на мрежата за излез кон интернет. Терминот „трислоен преклопник“ често се користи истовремено со терминот рутер или насочувач, но преклопникот е општ термин без строга техничка дефиниција.  **Сервер - опслужувач (Server) –** е компјутер или уред кој обезбедува информации или услуги за други компјутери на мрежата. Доколку го има соодветниот софтвер, секој компјутер поврзан на мрежата може да се конфигурира како сервер. Во најголем дел од случаите, тоа е наменски моќен компјутер определен да биде „секогаш достапен“. Еден компјутер може да дава повеќе услуги- на пример да функционира како веб сервер, сервер за електронска пошта, сервер за печатење, итн. Во една деловна средина се чини дека е логично различни услуги да се обезбедат преку различни компјутери - сервери поради безбедност и за да се минимизира влијанието на било каква грешка. | | | |
| 65 - 66 | | **Основите на интернетот**  Интернетот може да се замисли како инфраструктура во која истовремено можат да работат повеќе апликации. Ако еден дел од интернетот престане да функционира или се уништи, комуникацијата се уште може да продолжи. Интернетот нема сопственик – тој не е во сопственост ниту на една влада, корпорација или влада. Во голема мера тој е само-регулиран. Се користи иста технологија за поврзување.  Повеќето модерни мрежи на податоци, како што е интернетот, се дефинираат како „мрежи кои не се поврзани “ или „пакетни комутатори“. Сообраќајот се дели на мали пакети кои сами си го наоѓаат патот од испраќачот до примачот. Сите не одат по ист пат, а повторно се соединуваат кога ќе пристигнат на крајната дестинација. | | | |
| 67 - 68 | | Обучувачите треба јасно да ги објаснат разните апликации што постојат на интернет, со јасни примери за тоа што тие значат. Треба да се даде пример за секоја апликација, додатно на оние дадени на овој слајд.  Има многу интернет протоколи, но најважен е Интернет протоколот (IP). Секој компјутер што е поврзан на интернет МОРА да го користи. ИП адресата e вашиот „телефонски интернет број“и без ИП адреса не можете да користите интернет. Различни апликации и услуги користат различни протоколи за комуницирање на мрежа. Еве некои од нив : HTTP (HyperText Transfer Protocol) или протокол за пренос на хипертекст , SMTP (Simple Mail Transfer Protocol) или протокол за пренос на едноставна пошта; FTP (File Transfer Protocol) или протокол за пренос на датотеки; NNTP (Network News Transfer Protocol) или– Протокол за пренос на вести од мрежата. | | | |
| 69 - 70 | | Повеќето луѓе се поврзуваат со интернет преку испорачувачи на интернет услуги т.е. интернет сервис провајдери (ISP). Тоа се комерцијални организации што издаваат простор. Тие чуваат записи. Но, колку долго? Прашањата поврзани со правната заштита на податоците на национално и меѓународно ниво, како и прашањата поврзани со приватноста влијаат на тоа колку долго еден испорачувач на интернет услуги може да чува податоци. Ова, се разбира, влијае врз можноста органите на законот да обезбедат докази од овие извори. Поврзувањето најчесто се врши на следните начини: со телефонскоизбирање (Dial-up), широкопојасно поврзување(Broadband/ADSL), ISDN, кабелска ТВ, безжично *hotspot* поврзување и преку сателит.  Треба да се дадат информации како се остварува врска со интернет, а учесниците треба да се поттикнат да ги споделат сопствените искуства. Треба да се објасни дека испорачувачите на услуги чуваат свои записи, но дека законодавството поврзано со заштита на податоците ограничува колку долго можат да го прават тоа.  Треба да се објасни улогата на испорачувачите на интернет услуги, да се објасни нивниот правен статус и број. Ова е добра можност да се разговара за значењето на испорачувачите на интернет услуги за остварување пристап до податоци или вршење законско пресретнување/следење.  Едноставно кажано, испорачувачите на интернет услуги го изнајмуваат нивниот пристап до интернетот, на поединци и на организации.  Сите провајдери чуваат одредени информации за своите корисници. Колку и какви информации се чуваат зависи од провајдерот, а колку– дали саати или денови, зависи од потребите.  Од овие податоци може да се дознае:   * Име, адреса и други информации што се користат за пријавување * Датум на пријавување и како лицето се пријавило * Конкретна адреса за е-пошта или имиња што ги употребува корисникот * Име што се користи на интернет * Финансиски информации, како кредитни картички кои се користат за претплата до провајдерот. * Можно е да се добијат и одредени софтвер податоци за корисникот * Најважно од се, можат да се добијат информации за онлајн активностите на корисникот: на кој датуми, во кое време и колку долго корисникот бил на интернет   Времето е особено важно (за временските зони ќе се разговара подоцна во оваа сесија). Треба да се напомене дека е можно да се користат и неточни податоци за отворање сметка.  Може ли провајдерот да следи сомнителен интернет сообраќај? Да, може, но за тоа е потребно специјална опрема за евидентирање и следење, а потребни се и човечки ресурси, а сето тоа чини. Исто така, треба да се има предвид и овластувањето потребно за вршење вакви активности. Во секој случај, потребно е да се контактира со провајдерот уште во раната фаза на истрагата.  Превод на адресата на мрежата (Network Address Translation) – е техника со која изворот и/или ИП адресата на одредиштето се презапишува кога поминува низ заштитниот ѕид или рутерот. Најчесто се користи кога повеќе хоста на приватна мрежа остваруваат пристап до интернет преку една ИП адреса.  Се препорачува во секоја обука да се воведе подетално објаснување за адресните шеми, а особено адресите од ИПв4, кои се состојат од 32 бита, групирани во 4 октети, одвоени со точки и претставени во децимален формат . Минимална декадна вредност на еден октет е 0, а максимална 255, т.е. има 256 можни комбинации . Одредени броеви вредности се резервирани. Треба детално да се објасни како се формираат ИП адресите, а тоа најлесно може да се направи со визуелна презентација на бинарниот броен систем. Презентацијата исто така треба да ја објасни разликата меѓу статични и динамични ИП адреси и влијанието што тоа може да го има врз истрагата. Треба да се објаснат промените со ИПв6 и потребата за менување на верзијата кога ќе почне да снемува ИП адреси. | | | |
| 71 - 72 | | Значајна карактеристика на интернетот е тоа што се користи ширум светот. На овие два слајда, на два различни начини се прикажани информации во врска со пенетрацијата на различните јазици што се користат на интернет, и промените настанати во релативно краток временски период. Како и кај сите други информации кои се менуваат со текот на времето, обучувачот треба да обезбеди најнови податоци од потврдени извори. | | | |
| 73 | | **Интернет – Како работи?**  Во текот на оваа сесија, на учесниците им се овозможува да го осознаат начинот на кој податоците се пренесуваат преку интернет. Тоа се основни информации кои одговараат за овој вид обука. | | | |
| 74 | | Во случај на ИП, податочните блокови можат да бидат со различна големина. Тие не мора да одат по ист пат за да сигнат од изворот до целта. Компјутерот што ги прима овие пакети повторно ги подредува кога тие ќе стигнат на целта, и доколку недостасува некој пакет, повторно повикува на негов пренос.  Предноста е во тоа што мрежата е заеднички ресурс што може динамички да се алоцира, во зависност од потребите. Лошата страна е што тешко се гарантира квалитетот на услугата, бидејќи нема посветена врска. Ова е проблем на кој се работи, а веќе има и интернет телефонија која се нуди одличен квалитет. | | | |
| 75 - 76 | | Овие две илустрации му овозможуваат на обучувачот на полесен начин да објасни како се одвива сообраќајот на интернет. | | | |
| 77 | | Одличен ресурс каде што се објаснува како работи интернетот е филмот „Воини на мрежата“. Ова е совршена алатка за запознавање со интернетот која им овозможува на новите корисници визуелно да осознаат како функционира мрежата. Филмот трае 12 минути и го опишува патувањето на еден ИП пакет низ мрежните рутери, заштитните ѕидови, и трансатлантски кабли. Достапен е и може бесплатно да се преземе за некомерцијална употреба од www.warriorsofthe.net и моментно (од јануари 2012) го има на следните јазици: англиски, германски, шпански, холандски, шведски, француски, италијански, португалски, дански, норвешки, унгарски и чешки. Уште еден корисен извор кој го објаснува нивото на пенетрација и ширењето на интернетот по земји и региони може да се најде на http://www.internetworldstats.com/ . Во текот на обуката, се препорачува да се внесат и одредени статистички информации со цел да им овозможи на учесниците да го согледаат влијанието и значењето на интернетот во нивната земја. | | | |
| 78 | | Значајно е учесниците да се информираат за ИП адресите и за ограничувањата на IPv4. Ова ќе им помогне во подоцнежните дискусии за динамични и статични ИП адреси. Оваа едноставна информација е вовед во идното поглавје, во кое се расправа за иднината на интернетот. | | | |
| 79 | | Повеќето интернет провајдери имаат помалку ИП адреси отколку корисници, што значи дека тие работат на принципот дека не сите корисници ќе се поврзат истовремено. Провајдерите доделуваат динамични ИП адреси, кои може да се преработат.  Бидејќи постои голема веројатност во текот на денот различни луѓе да користат иста ИП адреса, при вршењето проверка на осомничени лица провајдерот мора да внимава на времето и датумот (временска зона).  Интернет сервис провајдерите и статични ИП адреси (кои секако се предуслов за имање веб страница), но по повисока цена. | | | |
| 80 до 81 | | Иднината на интернетот постојано носи промени. Воведувањето на IPv6 ќе внесе многу промени во нашите животи, а исто така и во системот на кривичното право. Обучувачот ќе треба да објасни како со IPv6 секој поединечен уред ќе има сопствена ИП адреса, и како тоа ќе влијае врз начинот на кој ќе се спроведуваат истрагите в иднина.  Треба да се дадат примери за тоа како се менува интернетот и како овие промени влијаат врз начинот на кој се спроведуваат и раководат истрагите. Примерите треба да се релевантни за учесниците, а на слајдот се посочуваат протокот, бизнисот и безжичниот интернет. | | | |
| 83 -111 | | Дел **3 – Интернет услуги** | | | |
| 83 | | Оваа сесија подетално се задржува на услугите достапни на интернет, особено, светската мрежа (World Wide Web) и електронската пошта. | | | |
| 84 | | Пред детално да се разгледаат услугите на интернетот, добро е да се види до која мера државите денес зависат од овие услуги. Обучувачите треба да направат преглед на клучната инфраструктура во земјата, за да им овозможат на учесниците да сфатат како, за кратко време, интернетот станува се позначаен за безбедноста на оваа национална инфраструктура. | | | |
| 85 | | **Светка мрежа (World Wide Web - WWW)**  Светската мрежа - World Wide Web (WWW) - прв пат се појавува во 1991 година, со хипертекст маркирачкиот јазик - HTML. HTML е изум на Сер Тим Бернерс-Ли и претставува платформа за комбинирање зборови, слики и звуци на веб страниците. Стандардите за мрежата ги утврдува Конзорциумот за светската мрежа (W3C). Со следниот цитат во извесна мера се објаснува и името на овој конзорциум**: „**W3C го гледа светот како место каде што сите документи се поврзани со линкови. Се нарекува мрежа, затоа што наликува на пајакова мрежа“ (Тим Бернерс-Ли, Роберт Кајо (*WorldWide Web*, септември, 1992 година) | | | |
| 86 - 87 | | Пристапот до WWW вообичаено се постигнува преку веб- пребарувач – софтверска програма која служи за лоцирање и прикажување на веб страници. Заклучно со јануари 2012 година, најчесто користени пребарувачи се: Mozilla Firefox, Google Chrome, Internet Explorer, Safari и Opera. Задача на обучувачите е дадената статистика да ја ажурираат во дадени временски интервали. | | | |
| 88 - 89 | | Протоколот за пренос на хипертекст (Hyper-Text Transfer Protocol (HTTP) е заеднички јазик што веб пребарувачите и веб серверите го користат за комуницирање на интернет.  ИакоWWW пребарувачите поддржуваат повеќе протоколи на пр. FTP, NNTP, SMTP, и слично, HTTP е протоколот што најчесто се користи во комбинација со веб пребарувачите. HTTP претставува едноставен Протокол на барање/одговор (RR protocol) преку Протоколот за контрола на преносот - TCP (Transmission Control Protocol).  Многумина имаат погрешна претстава и мислат дека WWW е всушност интернет, а тоа најверојатно се должи на фактот што WWW е апликацијата што луѓето најчесто ја користат. Затоа и криминалците најчесто ја злоупотребуваат.  При изработка на материјалите за обука, треба да се обмислат примери за криминални активности на WWW, релевантни за јурисдикацијата каде што се врши обуката. | | | |
| 90 | | **Имиња на домени и ИП адреси**  Во овој дел на учесниците им се даваат основни информации за ИП адресите и што тие претставуваат, без детално да се објаснува врската помеѓу ИП адресите и доменските имиња. Претпоставката е дека техничките детали во врска со тоа ги надминува рамките на оваа обука. Важно е обучувачот да го објасни овој дел на наједноставен можен начин. Презентираниот материјал се обидува да го идентификува најдобриот начин да се стори токму тоа. | | | |
| 91 - 93 | | Во овој дел, има три главни точки што треба да се пренесат:   1. Да се објасни што е униформен локатор на ресурси (URL - Uniform resource locator) и каква е неговата поставеност; 2. Да се објасни распределувањето на статични ИП адреси– статичните ИП адреси се постојани и се секогаш онлајн.   Динамичните ИП адреси се доделуваат секојпат кога корисникот е онлајн, но овие ИП адреси можат да се прераспределат откако корисникот ќе се одјави.  Од тие причини е многу важно да се знае во кое време е остварен пристапот на интернет.   1. Да се објасни односот помеѓу ИП адресите и URL. Имињата на домените и ИП можат да се заменуваат едни со други. Ако се знае ИП адресата може да се внесе на адресната линија и да се оствари врска со истиот сајт.   Она што вообичаено се случува во практика е следно: се внесува име да домен што е полесно за користење, на пример [www.open.gov.uk](http://www.open.gov.uk), а интернет сервисите го преведуваат тоа за вас и ве носат на точниот сајт.  Со интернет протокол адреса, името на доменот се преиначува во единствен број од 32 бита, и вообичаено се запишува во серија од четири броја од 8 бита, запишани во децимали и одвоени со точки. На пример, во бројот 212.140.189.10, четирите броеви мора да се помеѓу 0 и 255 (т.е. имаат по 256 комбинации). Во овој пример, очигледно е дека последниот број треба да биде 010, но, договорено е тој да може да се скрати на 10. | | | |
| 94 | | **Траги**  Кога се работи за компјутерски криминал, од особена важност се трагите кои истражителите можат да ги остават кога го користат интернетот за вршење истрага. Ова е релевантно не само за истражителите, туку и за обвинителот кој ја покренува истрагата. Важно е и за судиите кој одлучуваат за прифатливоста на доказите. Во овој во дел на обуката на учесниците траба да им се укаже на можните ризици кога истрагата се врши онлајн. | | | |
| 95 - 98 | | Информациите дадени на слајдовите посочуваат какви информации можат да останат како трага, вклучително и од истражителите кои посетуваат веб страници. Тоа треба да се поврзе со потребата истражителите да го заштитуваат нивниот идентитет во вакви ситуации. Исто така, треба да се укаже дека во дадени јурисдикации постојат законски услови кои треба да се исполнат за да се преземат вакви истражни дејствија | | | |
| 101 - 104 | | **Електронска пошта**  Електронска пошта или *емеил* е метод за размена на дигитални пораки. Корисникот добива впечаток дека е-поштата оди директно од уредот на испраќачот до тој на примачот; но вообичаено, секоја порака минува низ најмалку четири компјутери во текот на својот животен век.   * 1. Пораката се составува на компјутерот на корисникот, па се испраќа до сервер за излезна пошта со протокол за пренос на едноставни пораки (*SMTP*) на интернет провајдерот (*ISP*)   2. ISP ја препраќа оваа порака до SMTP серверот за пошта на примачот (SMTP – SMTP)   3. Серверот за пошта на примачот го пронаоѓа серверот за влезна пошта на примачот - POP3 (поштенски протокол) и ја доставува пораката до „поштенското сандаче“ на примачот.   4. Примачот се пријавува на сметката и пораката стигнува во влезното сандаче на примачот, а при тоа таа се брише од серверот за пошта   *\* Сервер за пошта/Поштенски сервер – компјутер посветен на работење со пошта* | | | |
| 105 | | Има повеќе видови е-пошта:  **E-пошта -** традиционална *Outlook* пошта , која се испраќа со SMTP , се прима преку POP3 и откако ќе се преземе, останува на уредот  Е-пошта преку мрежа (*Web-based mail*) - POP3 пошта – на пр. со користење на Outlook Express – вообичаено, по пријавувањето се презема сета нова пошта во влезното сандаче за пошта и таа останува на вашиот уред.  IMAP пошта (интернет протокол за пристап до пораки) –„вистинска“ веб-пошта – се гледа преку вашиот уред, но престојува на оддалечен сервер – може да се организира по веб-фајлови и сл., но се гледа само кога сте онлајн. | | | |
| 106 - 109 | | **Заглавија на Е-пошта**  Кога се објаснува е-поштата, најлесно е да се спореди со писмо. Е-писмата имаат заглавие (плик), и содржина (самото писмо) со прилози. Заглавието на пораката е од најголем интерес за истражителите, бидејќи содржи информации за испраќачот, примачот, ИП адресата, серверите за пошта, време итн. Овие информации се користат за следење на трагите на испраќачот на пораката, во случај кога тоа не е веднаш очигледно, на пример кога се работи за барање на откуп испратено со е-пошта. Целосното и проширеното заглавие е од клучно значење кога се следи изворот на пораката, и важно е судиите да знаат да ја воочат разликата меѓу заглавието што се гледа кога ќе се испрати писмото и проширеното заглавие што ги содржи сите релевантни информации. Е-поштата е апликација со која што судиите најчесто се соочуваат, и затоа обучувачите треба во материјалите да ги внесуваат најновите информации за различните видови е-пошта, како од нив на правилен начин се добиваат докази, било преку самите пораки или преку интернет провајдерот низ кој што минуваат пораките. Дополнителни информации за тоа како функционира е-поштата, кои можат да бидат корисни како ресурс за обучувачите можат да се најдат на http://www.learnthenet.com/english/html/20how.htm. | | | |
| 112 - 159 | | **Дел 4 – Други релевантни интернет апликации**  Во овој дел од обуката учесниците се запознаваат со интернет апликациите кои не беа опфатени во претходните делови. Ова е потребно бидејќи учесниците ќе се среќаваат со нив во текот на вообичаените работни активности. Овие информации ќе придонесат кон остварувањето на поставените задачи на обуката. Степенот на предвидените детали одговара на потребниот степен на наставата. Се препорачува обучувачите да не одат во детали, бидејќи е предвидено оваа материја да се покрие со напредната обука чија што изработка е во тек. | | | |
| 113 - 114 | | **Компјутерско работење во облак - клауд комјутинг**  Клауд комјутинг е маркетиншки термин што се користи за технологиите што испорачуваат компјутерски услуги, софтвер, пристап до податоци и нивно складирање без крајниот корисник да ја знае физичката локација и конфигурацијата на системот што ја дава таа услуга. Паралела на овој концепт може да се направи со електричната мрежа: крајните корисници користат енергија без да имаат потреба да знаат какви елементи или инфраструктура е потребна за обезбедување на услугата. Клауд компјутинг претставува нов модел на дополнување, користење и испорачување на ИТ услуги врз основа на интернет протоколи, кои вообичаено се динамични и честопати виртуелни ресурси. Тоа е нус производ и последица на лесниот пристап до оддалечени компјутерски сајтови што ги има на интернетот. Може да биде во форма на веб алатки или апликации до кои што крајниот корисник може да пристапи преку веб пребарувач, исто како да се програми инсталирани на нивните компјутери. Клауд компјутинг провајдери испорачуваат апликации преку интернет и пристапот е преку веб пребарувач и апликации за статични и мобилни уреди, а софтверот и податоците се чуваат на сервер на далечна локација. Во одредени случаи, постарите апликации се испорачуваат преку технологија на делење ист екран, а компјутерските ресурси се на оддалечена локација во одреден центар за податоци. Во други случаи, цели бизнис апликации се кодираат со *Web0* технологија, како AJX. Во основата на клауд компјутингот лежи еден поширок концепт на здружување на инфраструктура и заеднички сервиси. Ваквиот тип на центар за податоци им овозможува на фирмите побрзо да ги активираат нивните апликации, и полесно да ги одржуваат. Со ова ИТ системот полесно ги приспособува ИТ ресурсите (сервери, складирање и работење на мрежа) за да одговори на променливите и непредвидливи деловни потреби. Поголемиот дел од инфраструктурата на компјутерското работење во облак состои од услуги што се испорачуваат преку заеднички дата центри и единствена точка за пристап за компјутерските потреби на корисниците. Понекогаш тоа се прави со комерцијални понуди за услугите што се нудат, но малите компании ретко преговараат за конкретни услови. Големото влијание на клауд компјутинг врз бизнисот ја натера Сојузната американска влада да гледа на клаудот како средство за реорганизација на својата ИТ структура и за намалување на ИТ буџетите. (Извор: [www.wikipedia.com](http://www.wikipedia.com))  Прашањата поврзани со идентификација и прибирање податоци од облак, како и правните импликации од тие дејствија ќе се разгледуваат во текот на обуката. | | | |
| 115 - 116 | | Обучувачот им укажува на учесниците за се посеприсутното онлајн складирање, и како пример ги наведува пребарувањата на Гугл и нивното постојано зголемување, со што го демонстрира големиот интерес за ваков вид складирање. Обучувачот треба ја ги објасни различните видови онлајн складирање, и да ја посочи разликата помеѓу бесплатните услуги и услугите што се достапни со претплата. Треба да се јасно да се предочи дека криминалците може да користат токму ваков вид на складирање. | | | |
| 117 - 118 | | На учесниците треба да им се посочат и другите начини на кои што криминалците ги користат интернет услугите. Еден таков начин е користењето на „мртво поштенско сандаче“. Овој начин на комуникација кој носи многу мал ризик да биде откриен може лесно да се објасни. | | | |
| 119 - 120 | | **Систем Peer to Peer (P2P)**  Со години **P2P** услугите овозможуваат трансфер на нелегални датотеки, како и на датотеки заштитени со правата на интелектуална сопственост. P2P станува се популарен кај криминални групи кои се бават со ваков вид активности. Првата генерација P2P архитектура работеше врз принципот на користење централен сервер на кој се приклучуваат клиенти за да преземат фајлови. Со тоа се олеснуваше идентификацијата на лицата кои нудат вакви нелегални услуги, нивното лоцирање и затварање. Во втората генерација на P2P, методите на поврзување на клиентите се различи од списоците на достапни фајлови, за да се олесни нивното пребарување. Сега тие делуваат како супер јазли кои идентификуваат каде можат да се најдат фајловите.  Судиите ќе треба да обрнат особено внимание на P2P активностите, бидејќи тие можат да бидат релевантни во многу кривични и граѓански предмети. Подлабоко познавање не е потребно. Обучувачите можат да се послужат со следниот сајт: http://ezinearticles.com/?How-Peer-to-Peer-(P2P)-Works&id=60126 со цел да обезбедат најнови информации. | | | |
| 121 - 122 | | **Групи за вести**  Терминот група за вести можеби не е најправилен опис, бидејќи станува збор за хостирање дискусии. Групите за вести технички се разликуваат, но функционираат на сличен начин како и форумите за дискусија на светската мрежа (*World Wide Web*). Овие групи за вести ги хостираат повеќе организации кои се согласуваат редовно да ги синхронизираат нивните информации меѓу себе. На тој начин, на корисниците им се овозможува да постираат пораки на еден сервер, и тие да бидат видени од поголем аудиториум. | | | |
| 123 - 124 | | **Протокол за пренос на датотеки** **(FTP - File Transfer Protocol)**  *FTP* е моќен протокол кои овозможува пренос на датотеки од еден во друг компјутер. Функционира на база клиент/сервер. Кај клиентот се инсталира *FTP* програм со кој му се овозможува да комуницира со одреден сервер, а со цел да оствари присилат до услугите и информациите на тој сервер. Кога клиентот сака да пренесе датотека во целниот систем, се создава *TCP* (протокол за контрола на преносот) конекција. Се дозволува пренос на корисничкото име и лозинката, и корисникот може да ги специфицира датотеките и потребните дејствија. Откако ќе добие дозвола за пренос на датотека, се создава друга *TCP* конекција за пренос на податоците. Зошто е потребно судиите да знаат за постоењето на *FTP* услугите? Одговорот е дека тие можат да се сретнат со предмети каде што криминалците разменуваат датотеки на овој начин, или пак каде што *FTP* се користи како метод за пренос со други протоколи како на пример ИРЦ (разговор преку интернет) | | | |
| 125 - 126 | | **Разговор преку интернет** (IRC)  Разговорите преку интернет (IRC) e телеконференциски систем, малку застарен, но криминалците се уште го користат за комуникација и размена на датотеки. Работи на принцип на серија поврзани сервери преку кои се споделуваат пораки постирани на „канали“, т.е. виртуелни сали за состаноци за текстуални пораки. Има теми за дискусија и корисниците на IRC можат да се поврзат со еден или повеќе канали во кое било време, и да се вклучат во дискусија со луѓе со исти интереси. IRC не е најлесен за користење, и најчесто го користат поискусни лица и евентуално постари корисници. Криминалците го користат овој протокол, и следствено, судиите и обвинителите треба да имаат основно познавање за неговото функционирање. | | | |
| 127 - 132 | | **Инстант пораки** (IM) **и социјални мрежи**  Во последно време, инстант пораките и социјалните мрежи го преземаат приматот како начесто користена алатка за комуникација. Има многу добро познати примери преку кои се остварува моментно и лесно поврзување со други корисници низ целиот свет. Главната карактеристика на сите овие сајтови е можноста да се креира личен профил , да се споделуваат лични информации и да се запознаваат нови луѓе. Исто така, може да се споделуваат фотографии, музика и видеа. Обемот на лични информации што лицата ги постираат може да ги направи мета за криминалците, како на пример оние кои се бават со кражба на идентитетот и наведување деца. Дополнителни информации кои можат да помогнат во изработка на материјалите за обука можат да се најдат на: http://communication.howstuffworks.com/how-social-networks- work.htm .  Инстант пораките се еден вид директен разговор во реално време на двајца или повеќе поединци преку заеднички клиенти. Овој вид разговор претпоставува контакт помеѓу две лица што се познаваат, за разлика од други видови разговори што овозможуваат комуникација помеѓу непознати лица. И криминалците ги користат инстант пораките како начин за комуникација.  Обучувачот може да обезбеди дополнителни информации во вид на статистички податоци за зголемениот број корисници на социјалните мрежи. Дадени се примери за растот на одредени сајтови и нивното глобално влијание.  Обучувачот треба да обезбеди примери за видот на информации што им е достапен на истражителите. Во презентацијата се дадени неколку корисни примери. Сепак, обучувачот треба да се обиде да обезбеди примери кои се релевантни за географската локација од каде што потекнуваат учесниците. | | | |
| 133 - 136 | | **Онлајн игри**  Онлајн игри се игри што се играат на некаков вид компјутерска мрежа. Тоа скоро секогаш подразбира интернет или слична технологија. Игрите секогаш користеле најсовремена технологија: модеми пред интернетот, статични терминали пред модеми. Експанзијата на онлајн игри е одраз на севкупната експанзија на компјутерските мрежи, кои од мали локални мрежи прераснаа во интернет, и на се поголемиот пристап до интернет. Онлајн игрите имаат широк дијапазон - едноставни игри базирани на текст до игри со сложени графички и виртуелни светови во кои истовремено се среќаваат повеќе играчи. Многу онлајн игри имаат свои онлајн заедници, со што онлајн игрите се еден вид социјална активност, а не само игри наменети за само еден играч.  Обучувачот треба да презентира примери за криминал во кој се вклучени игрите. Ваквите случаи се почесто се среќаваат, и затоа би било корисно да се разгледаат правните последици во повеќе земји. | | | |
| 137 - 146 | | **Анонимност на интернет и следливост**  Анонимноста на интернет е значајна тема што треба да се покрие во почетната обука. Судиите и обвинителите редовно ќе се среќаваат со овие термини. Треба да се дадат пример за анонимните прокси сервиси и да се објасни како тие функционираат. Исто така треба да се објасни разликата помеѓу анонимен и транспарентен пренос. Слајдовите дадени во презентацијата може да им помогнат на обучувачите при подготовката на сопствени материјали. Обучувачот треба да приложи примери и за анонимни веб и е-пошта сервиси. | | | |
| 147 - 159 | | **Дел 5 – Интернет криминал и кривични дела на интернет**  Во последниот дел од оваа сесија, обучувачот треба да ги идентификува начините на кои веќе објаснетата технологија се користи за извршување на кривични дела. Единствена земја на светот што прибира податоци за тужбите за интернет криминалот се САД . Статистиката од Центарот за тужби за интернет криминал дава делумен увид во сериозноста на овој проблем. Обучувачите можат да ги искористат овие податоци, внимавајќи тие да се соодветно ажурирани. | | | |
|  | | **Инвестициски шеми**  Интернетот се користи за барање финансиска поддршка за високо-технолошки шеми, како на пр. виртуелни трговски центри или нови испорачувачи на услуги.  **Шеми со кредитни картички**  Интернетот се користи за купување скапи производи со незаконски добиени податоци од кредитни картички.  **Деловни можности /Шеми за работа од дома**  Интернетот се користи за рекламирање на деловни можности при што жртвите треба однапред да платат за информации  **Измами 419**  Западно африкански измами. Сменет е само начинот на испорака – денес се испраќа по е-пошта а не по традиционалната пошта или преку факс. Западно африкански измами. Сменет е само начинот на испорака – денес се испраќа по е-пошта а не по традиционалната пошта или преку факс.  **Интернет банкарство**  Едноставно се копира веб-страница на одредена банка, малку се менува веб-адресата, се нудат линкови до легитимни банкарски услуги и еден или два линка до инвестиции кои ветуваат висок приход. Учеството во овие неверојатни можности за инвестирање се обезбедува преку префрлање големи суми пари однапред.  **Повик за доброволни прилози при непогоди**  Во рок од еден саат од цунамито на Далечниот исток, на мрежата се појавија веб страници со апел за помош за жртвите. Многу, (ако не и сите) беа лажни.  **Хeрбална Виагра**  На „потрошувачите“онлајн им се продаваат алтернативни медицински третмани преку *спам* пошта. Повеќето од нив немаат никакви корисни ефекти (ако воопшто и се испорачаат), а некои се и опасни.  **Руски невести**  Сајтови на кои се нудат контакти со убави жени од источна Европа и евтини посети во руските држави  **Добивки на лотарија**  Барања за исплата заради подигнување на лотариски добивки или нудење помош за да се оствари добивка (честопати од странски лотарии)  **Фишинг *(Phishing)***  E-писма кои наводно ги испраќа добро познат извор (банка или интернет испорачувач на услуги) со барање за потврда на лични податоци  Обучувачот треба да побара да побара релевантни случи од регионот каде се одржува обуката и да ги презентира како примери. На крајот на сесијата, обучувачот треба да ги охрабри учесниците да со споделат сопственото знаење и искуство поврзано со криминалот на интернет. | | | |
|  | | **Практични вежби (доколку се предвидени)** За оваа сесија не се предвидени практични вежби бидејќи не постои гаранција дека технолошките услови и пристапот до интернет ќе овозможи одвивање на вакви вежби на сите места каде што се одржува обуката.  Обучувачите може да размислуваат и за дополнување на обуката со додавање вежби, доколку обуката се врши во средина каде што тоа ќе биде можно. | | | |
|  | | **Проверка на знаењето**  Освен горенаведеното, не е предвидена друга проверка на знаењето. Не се предвидува ниту формално оценување. | | | |
| 160 - 162 | | **Дел 6 – Преглед / Резиме** | | | |
|  | | Обучувачот треба да направи преглед и да го провери стекнатото знаење во врска со наведените точки, за да осигури дека учесниците успешно совладале целите на сесија, и знаат да:   * Објаснат како технологијата влијае врз криминалот * Ги наведат составните делови на компјутерските системи * Објаснат како се складираат податоци во компјутерските системи * Идентификуваат различни компјутерски оперативни системи * Ги објаснат основите на функционирањето на мрежите * Ја објаснат функцијата на интернетот * Идентификуваат најмалку 5 главни интернет апликации * Објаснат како се развива интернетот, од неговите почетоци до денес * Разликуваат различни интернет апликации * Идентификуваат како криминалците ги користат разните интернет апликации   Тоа може да се постигне преку групна дискусија, прашања до учесниците, квиз или на друг прифатен начин.  Целта на оваа е да даде одредени насоки за видот и степенот на познавање на технологијата што судиите и обвинителите треба да го имаат за успешно извршување на нивните улоги. Не претендира дека дава целосна анализа на прашањата, и каде тоа е соодветно, може да се дополни со додатни информации.  Се препорачува изготвуваните на обуката за обезбедат материјал што е ажуриран, и ги опфаќа најновите технолошки прашања и како тие влијаат врз криминалното однесување, влијанието врз правните, процесните и доказните правила во јурисдикацијата каде што се одржува обуката. Промените во технологијата, како на пример складирањето податоци во полуспроводници и Веб 2.0. Тоа се значајни прашања што треба да се вклучат во програмите за обука, со оглед на нивното зачестено присуство..  Како и сите други програми, обуките наменети за судии и обвинители имаат јасни СМАРТ цели и да бидат: конкретни, мерливи, постигливи, релевантни и временски ограничени. Тоа е значајно, за да можат да се исполнат зададените задачи. Треба да се избегнуваат задачи кои бараат од учесниците да „знаат“ или „разберат“, бидејќи тие не ги исполнуваат критериумите. На пример, како нешто може да се измери дека некој нешто „знае“ за одредена тема? Подобро е да се користат термини како „наброј“, „наведи“ или „идентификувај“, кои се мерливи. Упатство за поставување на СМАРТ цели може да се најде на: [www.sheffield.ac.uk/.../Guide%20to%20setting%20Задачи.doc](http://www.sheffield.ac.uk/.../Guide%20to%20setting%20objectives.doc)  Случаите од практиката се добри за консолидирање на знаењето и се соодветни за овој вид на обука, бидејќи повеќе одговараат за учењето кај возрасните отколку чисто дидактичките предавања.  Клучната улога на обучувачот е да обезбеди дека се постигнува целта на сесијата и конкретните задачи. Во ова поглавје се дадени информации што можат да помогнат во тој процес.. | | | |
| **Други можни ресурси**  Во прилог следува список на публикации издадени од организации/држави што можат да им бидат од корист на обучувачите кои подготвуваат материјали за обука поврзана со електронски докази. | | | | | |
| **Организација** | | | **Земја на потекло** | **Вид документација** | |
| Меѓународна организација за стандардизација (ISO) и Меѓународна електротехничка комисија Commission (IEC) | | | Меѓународно | ISO/IEC 17025:2005 општи услови на компетентност за тестирање и калибрирање во лаборатории (18.10 класа на електронски докази, 01 одржување на податоци, .02 анализа на податоци)  ISO/IEC CD 27037 информатичка технологија – безбедносни техники – упатства за идентификација, собирање, здобивање и одржување на дигитални докази  ISO/IEC 9797-2:2011 информатичка технологија – безбедносни техники – Кодови за автентикација на пораки (MACs) -- Дел 2: механизми за посветена хеш-функција | |
| Европска мрежа на институтите за форензични науки (ENFSI) | | | EК | EA-5/03 Упатства за спроведување на ISO/IEC 17020 при истраги на местото на настанот | |
| Здружение на полициски комесари (ACPO)  PCeU  Полициски сили на Велс  E-криминал Велс | | | Англија, Велс и Северна Ирска  Велс | Прирачник за добро рабење со електронски докази од компјутер.  Прирачник за лица што први реагираат: упатства за истражители кои први интервенираат на инциденти поврзани со компјутери. | |
| ACPO | | | Англија, Велс и Северна Ирска | Прирачник со совети и добри практики: за раководители на одделенија за високо-технолошки/компјутерски криминал. | |
| ACPO | | | Англија, Велс и Северна Ирска | Прирачник за раководители: Прирачник со совети и добри практики за лица кои раководат со истрагите при е- | |
| Британски институт за стандарди Institution (BSI) | | | Обединето Кралство | ASTM E1732 – 11 Стандардна терминологија во форензичките науки Forensic Science  ASTM E1492 – 11 Стандардни практики за прием, документирање, чување и вчитување докази во форензична лабораторија | |
| Служба за акредитација на Обединетото Кралство (UKAS) | | | ОK | Публикации поврзани со акредитација на органи за сертификација | |
| Регулатор за форензични науки (FSR) | | | ОK (МВР) | Кодекс на практики и Кодекс за форензични научници и практичари во системот на кривично право  Записници од Групацијата за дигитална форензика | |
| Институт за инженерство и технологија (IET) | | | Меѓународно (IET ги опфаќа и институтите за електрично инженерство (IEE) И институциите на здруженија на инженери (IIE) | Развивање стандарди кај нови и постојни технолошки области. | |
| Европска групација за образование и обука за компјутерски криминал (ECTEG) | | | EC (Eвропол) | Записници од состаноци на ECTEG | |
| Британска компјутерска заедница, Групација на форензични специјалисти за компјутерски криминал | | | ОK | Документирани политики | |
| Оддел за правда на САД | | | САД | Форензично испитување на дигитални докази: Упатства за органите за спроведување на законот | |
| ФБИ /SWGDE | | | САД | Дигитални докази: стандарди и принципи | |
| Оддел за трговија на САД | | | САД | Упатства за форензика кај мобилни телефони | |
| Меѓународна организација за компјутерски докази | | | Меѓународно | Упатства за дигитални докази | |
| Совет на Европа | | | СЕ | Правни и процесни предуслови за земјите што сакаат да ја ратификуваат Конвенцијата за борба против компјутерски криминал | |
| Интерпол | | | Меѓународно | Прирачник за компјутерски криминал | |
| Вештини за правда | | | ОK | Национални професионални стандарди за борба против е-криминалот- стандарди за знаење и вештини потребни за работење со дигитални докази, за дигитална форензика и истраги на компјутерски криминал. | |
| Тајна служба на САД (Оддел за домашна безбедност) | | | САД | Најдобри практики за заплена на електронски докази  v.3A Џебен прирачник за лица што први интервенираат | |
| Европска Комисија | | | ЕК | Заплена на “e-докази” Проект Оисин 2002/OIS/014 | |
| Национален институт за правда (NIJ)  (National Institute of Standards in Technology NIST) | | | САД | Истрага на место на настан на електронски криминал. Упатства за лица што први интервенираат (второ издание) | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Сесија 1.3.1 – Дневен преглед | | | | | **Времетраење: 30 минути** | |
| **Потребни ресурси:**   * Преносен компјутер или ПК со Windows 7 и Office 2010 * Проектор * PowerPoint презентација | | | | | | |
| **Цел:**  Целта на оваа сесија е да се направи преглед на активностите од претходниот ден, да се добијат повратни информации од учесниците и да се провери дали се исполнети целите на сесијата | | | | | | |
| **Задачи:**  На крајот на сесијата, учесниците ќе можат да:   * Го идентификуваат материјалот од претходниот ден што го имаат совладано * Го идентификуваат материјалот што треба да го повторат за да го доведат знаењето до потребното ниво | | | | | | |
| **Вовед**  Оваа сесија треба да им овозможи на учесниците да проверат дали го разбрале материјалот од претходниот ден и да видат дали се во можност да ги исполнат задачите за дадените сесии. Исто така, оваа сесија му дава можност на обучувачот да го провери степенот на знаење на учесниците и да ги идентификува деловите каде што наставниот материјал може да се подобри. | | | | | | |
| **Слајд бр.** | **Содржина:** | | | | | |
| **1 - 12** | **PowerPoint** (или друг вид презентација)  Слајдовите од оваа презентација се дадени за да му помогнат на обучувачот и на учесниците за поминување на активностите од претходниот ден. Обучувачот треба да ги резимира тие активности, користејќи ги агендите и задачите како репер. | | | | | |
|  | **Практични вежби (доколку се предвидени)**  За оваа сесија не се подготвени практични вежби. | | | | | |
|  | **Проверка на знаењето**  Обучувачот треба да го провери знаењето преку поставување прашања што ќе ги опфатат сите аспекти на сесијата. | | | | | |
|  | **Преглед / Резиме**  Оваа цела сесија е посветена на резимирање на активностите од претходните денови. | | | | | |
| Сесија 1.2.3 Компјутерскиот криминал како кривично дело – Домашно законодавство | | | | | **Времетраење: 90 минути** | |
| **Потребни ресурси:**   * Преносен компјутер или персонален компјутер со Windows 7 и Office 2010 * Проектор * PowerPoint презентација | | | | | | |
| **Цел:**  Целта на оваа сесија е да се воведат учесниците во националните регулативи за компјутерски криминал, видовите на кривични дела што се опишуваат и релевантните и применливи меѓународни правни рамки. | | | | | | |
| **Задачи:**  На крајот на оваа сесија, учесниците ќе бидат во можност да:   * Ја идентификуваат националната регулатива за компјутерски криминал * Ги идентификуваат видовите кривични прекршоци опишани согласно националното законодавство * Идентификуваат некои специфичности во националната регулатива за компјутерски криминал, во контекст на меѓународната правна рамка | | | | | | |
| **Вовед**  Целите на оваа сесија е на судиите и обвинителите да им ги даде сите потребни информации и историјат за да тие можат делотворно да ги применуваат правните одредби од домашното законодавство при гонењето и судењето на предмети поврзани со компјутерски криминал. На крајот на оваа сесија, учесниците ќе бидат во можност да ги идентификуваат правните одредби во домашното законодавство што се однесуваат на:   * Престапи против доверливоста, интегритетот и достапноста на компјутерските системи * Престапи направени со компјутерски податоци и системи * Престапи поврзани со содржина, и сл.   Оваа сесија е подготвена за да со пример им покаже на учесниците како Конвенцијата од Будимпешта е инкорпорирана во домашното законодавство на една земја, поточно Португалија. Обучувачите ќе треба за ги заменат информациите од Португалија со соодветни законодавни информации од нивната земја. | | | | | | |
| **Слајд бр.** | | **Содржина:** | | | | |
| **1 - 66** | | *PowerPoint* (или друг вид презентација)  Слајдовите дадени за оваа сесија се само пример за тоа што може да се подготви во рамки на локалните обуки.  Во идеални услови, оваа сесија посветена на материјалното национално законодавство треба да ги наведе потпишаните или ратификуваните меѓународни правни инструменти, и како тие се пренесени во домашното законодавство.  Исто така, треба да се даде опис на кривичните дела согласно националното законодавство, и на крај, доколку тоа е случај, опис на какви било специфичности на националното материјалното право. | | | | |
| **2** | | **Агенда**  Оваа сесија има четири дела:  Дел 1 се задржува на кривичното материјално право од Конвенцијата од Будимпешта за борба против компјутерскиот криминал.  Дел 2 се задржува на националното кривично материјално право  Дел 3 се задржува на случаи од практиката.  Дел 4 претставува преглед на сите делови | | | | |
| **3** | | Обучувачот треба да ги покрие следните точки:   * Одредбите на материјалното кривично право и клучните фактори што се користат за опис на кривичните дела врз основа Конвенцијата од Будимпешта * Одредбите на материјалното кривично право и клучните фактори што се користат за опис на кривичните дела врз основа на постојното национално законодавство. * Потребата и предностите од усогласување на националното законодавство и меѓународните инструменти особено Конвенцијата од Будимпешта. | | | | |
| **4** | | * Релевантните одредби од материјалното право врз основа на дискусиите за случаите од практиката што се презентирани овде | | | | |
| **5 - 6** | | **Дел 1 - Конвенцијата од Будимпешта за борба против компјутерскиот криминал –кривично материјално право**  Како прв меѓународен договор за компјутерски криминал, Конвенцијата од Будимпешта има за цел да ја овозможи и развива меѓународна соработка во кривичните истраги.  Примарната цел е усогласување на материјалното право кај Страните со што ќе се дозволи соработката. За таа цел, Конвенцијата од Будимпешта ги дефинира   * Престапите против доверливоста, интегритетот и достапноста на компјутерските системи и податоци * Престапи сторени со компјутери. | | | | |
| **7** | | Овој дел се однесува на една од најважните категории компјутерски криминал: престапите против доверливоста, интегритетот и достапноста на компјутерските податоци и системи. Тоа е компјутерски криминал во потесна смисла на зборот. | | | | |
| **8 - 9** | | Кривичното дело нелегален пристап го прават лица кои противправно пристапуваат до еден компјутерски систем во целина или до еден негов дел. Согласно Член 2 од Конвенцијата од Будимпешта, ова дејствие мора да е намерно извршено.  Честопати се нарекува упад во компјутерски систем или хакирање и е еден вид на компјутерски криминал што најчесто се сретнува. Но, постојат и други дејствија кои можат да се класифицираат како нелегален пристап –всушност терминот *хакирање* вообичаено се користи за да се опише дејствието на противправно пристапување до компјутерски систем, со користење на технологија. Но нелегален пристап покрива и каков било неовластен упад во компјутерски систем , без оглед на технологијата што се користи, па дури и да не се користи технологија. Тоа, на пример, би биле противправно стекнати лозинки од страна на сторителот. Интересот што се заштитува е доверливоста на компјутерскиот систем и податоци. | | | | |
| **10 - 11** | | Согласно Член 3 на Конвенцијата од Будимпешта, недозволеното пресретнување е исто така престап сторен со намера. Го вршат лица кои противправно пресретнуваат компјутерски податоци кои не се од јавен карактер, од, до и внатре во еден компјутерски систем.  Оваа одредба го заштитува интегритетот на преносот на податоци кои не се од јавен карактер, така што го криминализира нивното неовластено пресретнување.  Преносот на податоци до еден компјутерски систем, од системот или внатре во истиот систем е денес најрелевантна појава на мрежите.  Технички, пресретнувањето на комуникација може да е многу лесно ако мрежата и комуникацијата не се соодветно заштитени. Со пресретнување на комуникацијата може, на пример, да се открие кои веб страници ги посетило некое лице, или е-поштата што тоа лице ја испратило или примило.  Следствено, кривичното дело недозволено пресретнување има за цел да ја одбрани ранливоста на комуникациската технологија, заштитувајќи ја комуникацијата која не е од јавен карактер. | | | | |
| 12 - 13 | | Лицата кои со умисла и противправно предизвикуваат оштетување, бришење, влошување, изменување или прикривање на компјутерски податоци вршат кривично дело упад во податоци, согласно Член 4 на Конвенцијата од Будимпешта.  Делото упадот на податоци го заштитува интегритетот на податоците од неовластен упад. Сопственикот на податоците има право истите да ги држи онакви какви што се, исто како и кој било сопственик на каква било стварна сопственост има право неа да ја заштити од упадот на други. Во некои јуриздикции, регуларната и класичната штета исто така покрива и упад во податоци. Во други јуриздикции, пак, има потреба посебно да се опише штетата на компјутерски податоци, или упадот во податоци.  Ова кривично дело произлегува од постоењето на се повеќето релевантни податоци (компјутерски податоци) во современиот живот. Компјутерските податоци се многу ранливи и многу лесно можат да се уништат или манипулираат. Со ова правило се заштитува нивниот интегритет и достапност.  Еден од најчестите примери на упад во податоци е резултат на дејството на вирусите што противправно сами се инсталираат на компјутерот на жртвата, и можат, да пример, да бришат податоци. | | | | |
| 14 - 15 | | Упад во системот означува попречување на функционирањето на одреден компјутерски систем - сериозно попречување. Членот 5 на Конвенцијата од Будимпешта не покрива не-сериозно попречување. Тоа може да биде резултат на внесување, пренесување, оштетување, бришење, влошување, изменување или прикривање на компјутерски податоци, ако тоа се прави со умисла и против правно. Со ваквиот став, општо земено, се изземаат безбедносните тестови кои ги вршат администратори на мрежите. Овој престап покрива широк спектар на дела, кои можат да го попречуваат регуларното и исправното функционирање на мрежата. Всушност, Конвенцијата од Будимпешта ја признава важноста на комуникациските системи и на компјутерската технологија во секојдневниот живот – достапноста на овие системи е од суштинска важност за регуларното функционирање на јавните, економските и општествените активности. Но, овој вид на криминал не покрива само упади од голем размер – на пример, напади за ускратување на услуги. Дури и малите дејствија кои вклучуваат само еден компјутер може да биде упад во систем – тоа е случајот на бомбардирање со пошта (*mail bombing),*  на една таргетирана адреса за електронска пошта. Всушност, кривичното дело упад во системот настанува секогаш кога сторителот таргетира одреден компјутерски систем со барања што ја надминува можноста на системот да одговори.  Со криминализација на ова дело се заштитува пристапот до комуникациските мрежи, овозможувајќи заштита и за системските оператори и крајните корисници. | | | | |
| 16 - 19 | | Еден од најсложените престапи опишани во Конвенцијата од Будимпешта е кривичното дело злоупотреба на уред– Член 6.  Како и другите кривични дела, дејствијата на сторителот мора да се сторени со умисла и противправно. Покрива широк спектар на активности, сите поврзани со уреди што можат да се злоупотребат.  Ова е многу „ново“ кривично дело, и не е вклучено во Препораката од 1989 година. Тоа е и многу иновативно – фактите наведени таму претходно не биле признати како кривично дело во многу јуриздикции.  Во основа, се забранува производство, продажба и набавка заради употреба, увоз, дистрибуција, или на друг начин да се направи достапен уред, вклучувајќи компјутерска програма, изготвена или адаптирана првенствено заради извршување на кое било од суштинските кривични дела наведени во Конвенцијата.  Во иста мера, се криминализира и продажбата на компјутерски лозинки, кодови за пристап или слични податоци со кои целината или дел од компјутерскиот систем се оспособува за пристап.  Со оваа одредба, Конвенцијата ја признава потребата од криминализација на се поисплатливиот и економски важен „второстепен пазар“на “опрема што овозможува криминал”: Хакерите онлајн ги продаваат нивните алатки, приборите за „направи сам“вирус се широко распространети онлајн, и големо продажба на лозинки украдени со Тројанци или со други уреди. Тоа значи дека хакирањето на компјутерски систем не е веќе привилегија на обучените програмери. Секој „обичен “ криминалец може лесно да ги набави потребните алатки, или украдени лозинки. Честопати, продавачот на криминал нуди и „услуги на корисниците„ и му помага на клиентот да го намести компјутерот за извршување на кривично дело.  Еден од најдебатираните делови на Член 6 е точката 1. б, со кои (се уште со умисла и противправно), се инкриминира и поседувањето на *уред* со умисла да се користи за целите на извршување на кој било од престапите утврдени во Членовите 2 до 5 на Конвенцијата (недозволен пристап, недозволено пресретнување, упад во податоци и упад во систем).  Оваа решение е слично на она што во повеќе јуриздикции се нарекува „подготвителни дејствија“, што во овој случај се веќе криминализирани сами по себе. | | | | |
| 20 | | Делата поврзани со компјутер се кривични дела кои се вршат со компјутерски систем. Овие дела се познати/конвенционални кривични дела што се вршат со нови модалитети, но и дела што можат да се извршат само во дигитална средина, и не можат да се случат надвор од виртуелниот свет. | | | | |
| 21 | | Делото фалсификување поврзано со компјутер, опишан во Член 7 на Конвенцијата од Будимпешта е посебен модалитет на фалсификување. Во повеќето земји фалсификувањето е стар/традиционален кривично дело. Но вообичаено, станува збор за конкретни предмети, и понекогаш тоа не може да се користи за криминализирање на компјутерското фалсификување или фалсификување на компјутерски податоци. Тоа е и причината за воведувањето на Член 7 во Конвенцијата .  Со овој член, Конвенцијата има за цел да воведе престап аналоген на традиционалното фалсификување на документи (опипливи документи). Но во овој случај, предмет на кривичното дело се компјутерските податоци. Ова кривично дело го вршат лица кои внесуваат, менуваат, бришат или прикриваат компјутерски податоци, кое нешто резултира со добивање неавтентични (лажни) податоци, со намера тие во правниот промет да се сметаат или да се користат како веродостојни.  Се разбира, и ова кривично дело подразбира дејствие извршено со умисла и против правно. | | | | |
| 22 | | Согласно Член 8 на Конвенцијата од Будимпешта, кривичното дело измама поврзана со компјутер, догматски гледано, е дело што многу малку се разликува од традиционалното дело измама . Но, во основа, се работи за нов модалитет, сам за себе, кое може да се изврши само во дигитална средина.  Повеќето национални закони ја криминализираат традиционалната измама, но, општо земено, тоа не може да се користи за ситуации поврзани со компјутер. Измамата подразбира лага или намерно направена грешка. Но, во повеќето случаи на компјутерска измама нема директна интервенција на одредено лице, туку таа настанува со манипулирањето на компјутерскиот систем. Затоа во описот на кривичното дел компјутерска измама, учеството на лице како сторител се заменува со манипулација на податоци со цел противправно стекнување на економска корист. На овој начин, не е потребно да постои лажење на друго лице како елемент за измама. | | | | |
| **23** | | Кривичните дела поврзани со содржински податоци се дела што сега многу полесно се вршат со користење на компјутер или мрежа. Овие дела можат да се вршат и со други средства, но компјутерите и мрежите многу го олеснуваат нивното извршување. | | | | |
| 24 - 26 | | Член 9 од Конвенцијата од Будимпешта ни го открива внесувањето на една голема новина во овој Договор: се криминализираат делата на детска порнографија извршена преку компјутерски систем.  Трговијата со детска порнографија драстично се зголемува со проширувањето на интернетот. Комуникациските и информатичките мрежи нудат многу предности и можности за лица кои бараат ваков вид на содржина. Исто така, корисниците што онлајн пристапуваат до материјали со злоупотреба да деца на интернет можат да останат анонимни.  Еден аспект од кривичното дело детска порнографија мора особено да се продискутира бидејќи тоа опширно се разгледува во текстот на Конвенцијата: казнувањето на поседувањето на материјали со детска порнографија. Член 9, 1 како кривичен престап го наведува самото поседување на ваков вид материјал во компјутерскиот систем, вклучително и набавувањето на такви слики само за сопствена употреба. Овој е пристап што најчесто го прифаќаат и другите меѓународни форуми што работат на оваа проблематика.  Еднакво спорна е криминализацијата на „псевдо-слики“. Членовите на Конвенцијата не покриваат само ситуации на фотографирање на сексуален акт со вистинско дете; се криминализира и лажни прикази на деца – на пример, слики на деца што се целосно генерирани на компјутер (на пример сексуален акт со возрасно лице, каде што ликот на лицето се заменува со детски лик), или слики на возрасни лица (што навистина личат возрасно) кои се преправаат (се однесуваат или се облечени )како деца.  Криминализацијата на самото поседување на материјал со детска порнографија многу ги олеснува кривичните истраги на оваа тема, со оглед дека согласно оваа одредба кое било лице што поседува овој вид на материјал може да биде гонето, и не треба да се докажува конкретна намера за тоа како се користат сликите (на пример за продажба), ниту пак учеството во нивното производство. Исто така, тоа значи дека осомничените педофили можат да се казнуваат без какви било докази дека тие делувале поради нивните нагони кон деца. И, се разбира, на овој начин полицијата и судовите можат да ги истражуваат и да ги осудат добавувачите на детска порнографија (со самото поседување на ваков материјал) со или без докази дека дошло до трговија/размена на ваквите информации.  Во тој поглед, важно е исто така да се разгледа и правните можности кои постојат во ЕУ. Веќе години наназад, со Одлуката на Советот од 29 мај, 200 година, ЕУ одлучи да го криминализира самото поседува на материјали со детска порнографија. Од понов датум, во Директивата на Европскиот парламент од 2011 година (Directive 2011/92/EU) и на Европскиот Совет од 13 декември, 2011, за борба против сексуална злоупотреба на деца и детска порнографија се вели дека земјите членки на Европската унија треба, меѓу другите нелегални активности, да го криминализира и стекнувањето или поседувањето на детска порнографија (Член 5, 2). Но, истиот документ им остава на земјите членки да одлучат дали инкриминирањето ќе се однесува и на случаи каде порнографскиот материјал се користи само за приватни потреби (доколку за изготвувањето на таквиот материјал не е користен порнографски материјал и доколку не вклучува ризик од дистрибуција на истиот).  Опцијата што ја дава Европската унија е целосно во согласност со Член 9 на Конвенцијата од Будимпешта со кој што се инкриминира производството, нудењето или на друг начин овозможувањето достапност, дистрибуцијата или преносот, набавката и самото поседување на детска порнографија на компјутерски систем или на медиум за складирање податоци. Но, за вклучувањето на „набавката“ или „поседувањето“ можно е Страните на Конвенцијата да изразат резервираност.  Оваа опција беше потврдена и со Конвенцијата за заштита на децата (CETS 201), на Советот на Европа, што беше отворена на потпишување во 2007 година. Целта на овој договор е да се усогласат одредбите на кривичното право кај Страните, со цел заштита на децата од сексуална експлоатација. Согласно Член 20, треба да се криминализира, меѓу другото, и “*набавката на детска порнографија за сопствени потреби или за друго лице*“ *и* „поседувањето детска порнографија” . | | | | |
| 27 - 28 | | Конвенцијата од Будимпешта не содржи одредби конкретно за делата поврзани со авторските права. Тие се споменуваат во Член 10 на Конвенцијата, но не е даден нов концепт за регулирање на оваа проблематика. Во Конвенцијата само се нагласуваат претходните правила за авторските права: тоа што важи во реалниот свет мора исто така да се почитува и во реалноста онлајн. Повредата на авторските права онлајн, или повреда сторена преку компјутерски систем, мора да се казнува како да е сторена во реалниот свет . Од тие причини, Конвенцијата се повикува на постојните меѓународни договори за оваа проблематика (Парискиот договор од 24.јули, 1971 г., Бернската конвенција и .договорите на Светската организација за интелектуална сопственост – WIPO. | | | | |
| 29 | | Постојат уште две прашања во врска со материјалното казнено право што треба се разгледаат: казнувањето на дејствијата помагање и поттикнување, и кривичната одговорност на правни лица. Членот 11 на Конвенцијата од Будимпешта го опишува дејството на помагање и поттикнување што секоја Страна на Конвенцијата мора да ги вгради со домашното законодавство. Но се уважува дека интернет криминалот обично е активност на „повеќе страни“ при што честопати нема јасни разграничување на придонесот на страните, со што може се отежни гонењето. | | | | |
| 30 | | И на крај, Членот 12 на Конвенцијата бара од сите Страни да ги криминализираат дејствата на правните лица. Ова е значајно. Во ЕУ, криминализацијата на дејствијата на правните лица е исто така важно и доста контроверзно прашање, па затоа е вклучено во рамките на Советот на Европа.  Ставот и на ЕУ и на Советот на Европа е дека треба да постои некаква (кривична или не) одговорност за компаниите и други правни лица за кривичните дела што ги вршат нивни претставници, кои дејствуваат во нивно и ги застапуваат нивните интереси. Додатно на тоа, во Конвенцијата се наведува дека одговорност треба да постои и во случај на невршење надзор или контрола на правниот застапник на компанијата или на друго правно лице врз физичко лице под нивна надлежност  Во некои земји во Европа се претпочита одговорноста на правните лица да се регулира преку граѓанските, а не кривични, постапки. | | | | |
| **32** | | **Дел 2- Национално материјалното кривично право** | | | | |
| **33 - 43** | | Во овој дел обучувачите треба да постават слајдови со правните одредби на сила во земјата каде што се одржува обуката. | | | | |
| 44 | | Дел 3– Случаи од практиката | | | | |
| 45 | | **Случај од практиката 1**  **Факти / Сценарио**  Боби е полицаец. Една вечер, тој е на должност и гледа еден Мерцедес паркиран пред неговата куќа. Не ја препознава колата, но се сомнева дека возилото му припаѓа на шефот на неговата жена. Телефонира во полициската станица и ја прашува Мери, компјутерскиот оператор, да му каже кој е сопственик на Мерцедесот, велејќи дека возилото штотуку поминало на црвено светло. Мери потврдува дека возилото е навистина на шефот на неговата сопруга.  *Дали Боби извршил кривично дело?*  **Прашања**  *Дали Боби остварил пристап до компјутерски систем?*  *Дали тој пристап е противправен?*  **Точки за дискусија**  Мери остварила пристап до компјутерот, не Боби. Таа е овластена да пристапува до податоци на компјутерот. Таа нема вина. Дејствувајќи преку невино лице, Боби го предизвикува пристапот до податоци. Тој ја излажал Мери (пример за општествено инженерство). Дали, согласно законот, тоа претставува остварување пристап?  И Боби и Мери имаат право да остваруваат пристап во полицискиот компјутер, но според стриктни правила за легитимно пребарување поврзано со полициски активности. Дали пристапот што ги надминува овластувањата претставува кривично дело?  Што ако Боби оди во полициска станица и гледа преку рамото на Мери, (сурфање преку рамо) додека таа врши легитимно пребарување за сопственикот на Мерцедесот?  Со „сурфањето преку рамо“ Боби остварува пристап до компјутерските податоци. Може да се постави прашањето за неговата „намера“, и тоа дека тој не го злоупотребил компјутерскиот систем за да пристапи до податоците, но тој сепак остварува противправен пристап. (иако тоа е многу тешко за докажување)  Овој случај од практиката има за цел да ги поттикне учесниците да размислуваат за прашањето на овластување (противправен пристап).  Од учесниците може исто така да се побара да размислат за сценарио во кое Боби оди во полициската станица и ја наоѓа информацијата за сопственикот на Мерцедесот во картотека. Дали овие информации се исти како информациите на компјутерот? Поентата е дека не се заштитуваат самите податоци (иако и тие можат да бидат заштитени согласно законодавството за заштита на податоци, при што однесувањето на Боби може исто така може да се смета за престап), туку медиумот на кој што се чуваат податоците.  Полициските компјутерски системи содржат огромно количество лични информации за поединци, вклучително и доста чувствителни информации. Пристапот до такви податоци треба да им се дозволи само на лица кои имаат легитимен интерес. Во Обединетото Кралство, полициските службеници и компјутерските оператори во полицијата честопати се фаќаат како пристапуваат до полициските системи за сопствени потреби, за да дојдат до информации што се од интерес за новинарите, или пак, кога се работи за корумпиран службеник, за откривање какви информации се чуваат за одредено лице, или дали одредено лице или група се под активна истрага. | | | | |
| 46 | | **Случај од практиката2**  **Факти / сценарио**  Група криминалци го тераат лицето за обезбедување на една банка да го постави уредот *запишувач* зад неколку терминали во банката. Уредот ги забележува типските што ги отчукува корисникот, и на тој начин ги открива лозинките и другите информации што му овозможуваат на некое лице со пристап до терминалот да се пријави/логира на корисничките сметки на банкарските работници.  Додатна функција на *запишувачот* е што може да ги снима телефонските разговори што корисникот на терминалот ги прави на Скајп.  Криминалците исто така поставиле бубачка на масата, со која се снимаат сите телефонски повици што ги прави и добива корисникот на терминалот.  *Дали е тоа противправно пресретнување?*  **Прашања**  *Дали има пресретнување?*  *Дали тоа пресретнување е направено со технички средства?*  *Дали има пренос на податоци на или од компјутерски систем?*  **Точки за дискусија**  Запишувачот е технички уред што фаќа податоци пренесени од терминалот. Тоа е пресретнување, и очигледно е дека е против правно.  А телефонските разговори со Скајп? Според ова сценарио, се чини дека податоците одат по иста линија како и другите податоци од компјутерот, но што ако корисникот имал самостоен Скајп телефон? Дали таквиот телефон е компјутерски систем? Според Конвенцијата, „компјутерски систем“ е каков било уред или група на меѓу-поврзани или сродни уреди, каде што еден или повеќе уреди, согласно одредена програма, вршат автоматско процесирање на податоци. „Компјутерски податоци“ се какви било записи на факти, информации или концепти во формат соодветен за процесирање во *компјутерски систем,* вклучително со соодветна програма со која што еден компјутерски систем може да изврши одредена функција.  Користењето на бубачката е малку посложена ситуација. Дали е тоа „пресретнување“? Судовите во Обединетото Кралство се на став дека за да постои пресретнување мора да постои некакво интерферирање или извлекување на сигнал додека истиот се пренесува на мрежата. Во овој случај снимањето се врши независно од преносот, иако информациите што се добиваат на овој начин се исти со оние што би се добиле доколку уред бил поставен на „линија“/онлајн  Што се случува доколку самата Компанија го постави запишувачот на системот, за да се осигури дека вработените лица не го користат интернетот за несоодветни цели.  Повеќето телекомуникациски системи патуваат и по јавни и по приватни мрежи. Во моментот кога одредена комуникација го напушта вашиот имот, таа оди од приватен во јавен систем. Контролорот на приватниот систем има право на пристап до комуникацијата во тој систем. Така, вие би можеле да ги следите разговорите на вашата домашна телефонска линија, но само доколку техничкиот уред што ќе го користите за таа цел е приклучен на приватниот дел на системот.  Ова сценарио има за цел да ги наведе учесниците да размислуваат на елементите на пресретнувањето – дека пресретнување на компјутерски податоци настанува при нивниот пренос, со помош на технички средства и противправно.  Учесниците треба јасно да сфатат дека оваа одредба има за цел да ја заштити содржината на комуникациите, а не информациите поврзани со адресата/адресирањето на пораката или цената на услугата. | | | | |
| 47 | | **Случај од практиката 3**  **Факти / сценарио**  Една криминална банда комуницира преку систем за е-пошта на мрежа. Пристапот е преку интернет и може да се оствари од кое било место на светот. Наместо да си испраќаат пораки што полицијата може да ги пресретне или кои можат ги инкриминираат доколку се откријат на нивните компјутери, тие користат систем на „мртво писмо“. Тие ја пишуваат пораката како нацрт порака и не ја испраќаат. Другите членови на групата ја имаат лозинката со која што можат да влезат во таа е-пошта сметка, да ја прочитаат и да одговорат на пораката.  Дали евентуалниот пристап на полицијата во ова сандаче за нацрт е-пошта претставува пресретнување?  **Прашања**  *Дали пораката се уште се пренесува?*  **Точки за дискусија**  Во повеќето држави, потребно е полицијата да утврди висок степен на сомневање пред да добие овластување за пресретнување на содржината на одредена комуникација. Стекнување докази без соодветно овластување може да резултира со прекин на процесот, или со неприфаќање на доказите.  Компјутерите и интернетот нудат можности за повеќе видови на комуникација, на пример е-пошта, инстант пораки, твитер и сл. Пораките честопати стојат неотворени пред примачот за кого што тие се наменети да ги прочита. Дали може да се каже дека пораката што не е отворена е се уште на пат т.е. се уште се пренесува? Не постои начин за да се утврди дали примачот за кого таа е наменета ја прочитал нацрт пораката. Дали законот треба да обезбеди иста заштита за лицата кои намерно ги избегнуваат регуларните начини за испраќање е-пошта, како и за лицата кои е-поштата ја користат како што треба?  Ова е доста чест начин за комуникација помеѓу криминалците. Дали барањето пристап до вакви пораки е пресретнување или не зависи од домашното законодавство и/или мислењето на домашните судови. Но, корисно е учесниците да знаат дека доколку вакви информации се бараат преку Взаемна правна помош, земјата што се замолува може тоа да го смета за пресретнување, или во најмала рака, бидејќи се работи за пристап до содржината на комуникацијата, да биде потребно да се утврди повисок степен на сомневање пред да може да се добие соодветно судско овластување за таа намена. | | | | |
| 48 | | **Случај од практиката 4**  **Факти/Сценарио**  Полицаецот Боби го зема телефонот на жена му, ја погодува лозинката и слуша зачувана гласовна порака што таа се уште не ја слушнала.  *Дали е тоа пресретнување?*  **Прашања**  Дали гласовната порака се уште се пренесува?  Дали имаме случај на пресретнување на компјутерски податоци?  **Точки за дискусија**  Се додека пораката не стигне до одредиштето, веројатно е дека нејзиното пренесување е се уште во тек, и покрај тоа што таа се чува во системот. Пораката веројатно дигитално се чува на серверот на телефонската компанија, па така Боби пристапил до компјутерски податок. Дали е телефонот компјутер? Веројатно да, со оглед дека автоматски процесира податоци. Полициските службеници што вршат пребарување на телефони треба тоа да го имаат предвид, за бидат сигурни дека ги имаат потребните овластувања за пристапување до такви пораки. Ситуацијата би била поинаква доколку примачот ја слушнал пораката и решил да ја зачува.  Прашањата што се покренуваат со ова сценарио се слични на претходното. Сценариото има за цел да појасни една ситуација која често може да се сретне, а која се однесува и на полициските службеници кои што, при извршувањето на налог за пребарување, запленуваат компјутер што содржи и отворена и неотворена пошта. Исто така, илустрира дека повредата на Член 3 се однесува на сите видови на пренос на електронски податоци, било тоа да е преку телефон, факс, е-пошта или пренос на датотеки. | | | | |
| **49** | | **Случај од практиката 5**  **Факти/Сценарио**  Боби се интересира за НЛО и мисли дека руската влада заробила летало на вонземјани што слетало некаде во Сибир во почетокот на 20-иот век. Тој оди на еден руски сајт за регрутација на војници, кој пак дава врска/линк со сајт на руското воено воздухопловство. За овој сајт е потребна лозинка, но со помош на алатка за откривање на лозинки, тој успева да влезе. Поминува одредено време во истражување на системот и копира одреден број датотеки. Тој исто така се обидува да ги избрише сите датотеки кои содржат запис за неговите активности, за да не може да биде идентификуван. Потоа, ја менува почетната страница на сајтот, и наместо ознаките на Руското воено воздухопловство поставува слика на НЛО*.*  *Дали Боби има направено престап?*  **Прашања**  Дали неовластениот пристап сам по се себе претставува упад во податоци или систем?  Дали бришењето на записите за неовластен пристап е престап?  Дали треба да постои сериозно попречување на функционирањето на компјутерот за да постои кривична одговорност?  **Точки за дискусија**  Целта на овие одредби е да се заштитат компјутерските податоци и компјутерските програми од нанесувањето штета со умисла, слично како и материјалниот имот.  Боби не бил овластен да влезе во сајтот на военото воздухопловство, кој бил заштитен со лозинка. Затоа, пристапот на овој сајт претставува противправен пристап.  Боби избришал податоци, датотеки за евиденција и ознаки на руското воздухопловство. И покрај тоа што тој го предизвикал создавањето на овие датотеки, тие не се негови. Системот е конфигуриран да забележува активности од таков вид. Военото воздухопловство секако ќе сака да знае кој пристапува до нивниот систем.  Со менувањето на првичната страница, тој избришал и додал податоци во системот. И покрај тоа што тие најверојатно не предизвикале губење на важни информации, тоа претставува срам за руското воено воздухопловство. Но уште поважно од тоа, се поставува прашањето дали кој било системски администратор би можел да има доверба во интегритетот на податоците по ваков незаконски упад, и покрај тврдењата на Боби дека во системот влегол само за да најде информации и дека ги избришал датотеките или други податоци кои не се важни.  Дали во дадените околности е направен престап е прашање што ќе се толкува на локално ниво. Можно е да нема утврден праг за сериозност. Но, како и да е, системскиот администратор најверојатно ќе се чувствува обврзан да го симне сајтот за да ги утврди последиците од ваквиот упад, особено ако сајтот содржи доверливи или чувствителни податоци, или пак податоци што се користат за операции ж, кои доколку не се извршат правилно, би ја загрозиле пошироката јавност, на пример системот управување на нуклеарна централа.  Во случај системот во кој што влегол Боби да се користи за управување на нуклеарна централа, дали повредите од Член 4 и 5 се соодветни за да ја одразат сериозноста на ваквиот упад што е рамен на напад на клучна инфраструктура од национално значење? | | | | |
| 50 | | **Случај од практиката 6**  **Факти / сценарио**  Секој ден, автоматизирана програма за *спам* испраќа е-писма до илјадници корисници низ целиот свет. Доколку лицето ја отвори пораката, на апаратот на корисникот се даунлоудира софтвер. Софтверот не влијае врз работата на компјутерите, не презема податоци од компјутерот, не брише податоци и не предизвикува краткорочни или какви било други штети. Но, компјутерот станува „зомби“, т.е. дел од „мрежата на заразени компјутери“ (*ботнет*), што „контролорот на заразената мрежа“ може да ја користи за преземање на разни видови активности.  *Дали лицето одговорно за испраќањето на спам пораките извршил повреда на Член 4 или 5?*  **Прашања**  Дали се работи за случај на неовластен пристап до апаратот на корисникот?  Дали на апаратот на корисникот дошло до изменување на податоци­?  Дали е направена штета на апаратот на корисникот?  **Точки за дискусија**  И покрај тоа што не направил штета, софтверот предизвикал измени на податоците на компјутерот на корисникот. Оваа промена не е овластена, со оглед на тоа дека до корисникот не е испратено предупредување или барање за одобрување за ваквите измени на неговиот компјутер. Дали само по себе, испраќањето *спам* пошта е нелегално, или пак само непријатно? Дали тоа станува нелегално доколку предизвикува негативен ефект?  Што се случува доколку спам поштата имала и прилог и покана до примачот да го отвори прилогот со пораката „ова ќе ви се допадне?  Може да се аргументира дека со самиот избор што го направил примачот, тој изразил согласност да даунлоудира/преземе податоци на неговиот компјутер. Но, реално гледано, ваквата согласност не е дадена со знаење, иако може да се аргументира дека оние што решаваат да отворат прилози од непознати испраќачи тоа го прават на сопствен ризик.  Дали прави некаква разлика тоа што на корисникот му е сеедно дали неговиот компјутер станал дел од „ботнет“ или не  Патувајќи по интернетот, ние посетуваме сајтови и преземаме податоци без соодветно да размислуваме за природата на материјалите што влегуваат во нашите компјутери, верувајќи им на имињата на сајтовите, на имињата на датотеките или на резултатите добиени со пребарувачот да ги донесат правите одлуки за нас. Кликнувањето на малата сликичка за да ја видиме слика во целосна големина укажува дека сме свесни кои и какви податоци бараме да добиеме и дека сме целосно информирани за природата на податоците и сме согласни со тоа. Но, доколку кликнеме на малата сликичка на моторно возило, а сликата во целосна големина е авион, тогаш не може да се каже дека сме дале согласност да ги добиеме тие податоци.  Одлуката да се отвори еден линк за одреден вебсајт ќе предизвика преземање на многу податоци. Доколку сајтот е легитимен, тогаш голем дел од тие податоци се во врска со содржина на веб сајтот, иако еден одреден дел може да содржи реклами поставени од трети страни. И повторно, сме донеле информирана одлука и сме дале преќутна согласност да ја примиме рекламата, бидејќи знаеме дека тоа често се случува на интернет. Честа практика во интернет индустријата е да се даунлоудираат податоци на интернет пребарувачот на корисникот и тоа се т.е. „колачиња“ ..  Колачињата вршат повеќе функции, меѓу кои е и водењето евиденција за тоа што корисникот пребарувал на мрежата. Доколку на корисникот му се дава опција да го оневозможи колачето на пребарувачот, дали самото постоење на таква опција е доволно за да се смета дека корисникот дал согласност за даунлоудирање на такви податоци. | | | | |
| 51 | | **Случај од практиката 7**  **Факти / сценарио**  Боби е поранешен полицаец отпуштен од работа поради неовластено користење на полицискиот компјутерски систем. Тој решава да и се одмазди на полицијата. Користи програма за е-пошта што му овозможува да испрати 70,000 e-писма на час до секторот каде што работел. Го менува заглавието на е-писмото, за да изгледа дека е пратена од полицискиот началник, и на тој начин успева да го измами полицискиот сервер за е-пошта дека се работи за легитимен извор. Полицискиот сервер нема капацитет да прифати толкав обем на сообраќај, и паѓа.  *Дали е ова претставува упад во системот?*  **Прашања**  Испраќањето е-пошта подразбира пристап или барање пристап до *компјутерски систем, т.е. серверот за е-пошта*. До која мера сопственикот на ваков сервер овластува таков пристап?  Дали самото имање на адреса за е-пошта не значи дека ги поканувате другите да ви испратат е-писмо?  **Точки за дискусија**  Се работи за право. Боби пристапил/влегол до системот и предизвикал негово паѓање со тоа што испратил податоци. Со креирање адреса за е- писмо достапна до јавноста, сопственикот на адресата имплицитно дава согласност за примање на пораки. Боби може да каже дека полицијата се согласила да го прими секој поединечен е-меил, и дека не е негова вина тоа што системот немал капацитет да прими толку многу пораки. Но дали е тоа согласност? Сопственикот на куќа дава имплицитна согласност поштарот да ги става во сандачето писмата испратени до сопственикот. Исто така, постои и имплицитна согласност за примање на „шут – пошта“, на пример флаери за испорака на пица. Но, сопственикот не се согласува да добива толку многу флаери за пица за да не може да ја отвори вратата.  Може ли исто така да се каже дека со менување на информациите за испраќачот на е-меилот, пристапот до серверот за е-меил е остварен со измама? За такви „лажни“ е-меили не е дадена согласност.  И покрај тоа што сценариото се однесува на е-пошта, принципот исто така важи и за оние кои сакаат да предизвикаат паѓање на веб сајт преку напад на ускратување на услуги, при што сајтот не е во можност да го прифати сообраќајот насочен кон него. Поврзувањето со вебсајт подразбира размена на податоци помеѓу компјутерот на корисниците и веб сајтот. Слично како и во случајот со е-пошта пораки, прашањето што се поставува е во врска со имплицираната согласност за поврзување со сајтот. | | | | |
| 52 | | **Случај од практиката 8**  **Факти/Сценарио**  Боби и испраќа е-меил на сопругата, со која што тој не е во добри односи, на работа. Го менува заглавието така за да се стекне впечаток дека меилот го испратила некоја нејзина пријателка. Е-меилот содржи програма наречена „пристап до сите области“, што му овозможува на Боби да преземе контрола врз компјутерот на сопругата. Пред Боби да има шанси тоа да го стори, системскиот администратор го детектира присуството на програмата, и го исклучува системот за да направи проценка на степенот на упадот.  *Дали Боби направил престап според Член 5?*  **Прашања**  Дали Боби врши блокирање на податоци што се чуваат во системот?  Дали Боби го попречил функционирањето на компјутерскиот систем?  Дали таквото блокирање на податоци или попречување на функционирањето на системот е направено против правно?  **Точки за дискусија**  Реакцијата на администраторот на системот на е-меилот на Боби значи дека на корисниците на системот им е ускратена услугата. Следствено, пристапот до податоци што се чуваат на системот е блокиран, без оглед на тоа дека се работи за рестрикција на пристапот е од времен карактер. За овој вид престап не е потребно податоците да бидат долгорочно недостапни.  Веќе се разговараше за степенот до кој што сопственикот на е-меил адресата дава согласност за примање на податоци од други.  Член 5 се однесува на компјутерски системи, т.е. на еден или повеќе поврзани компјутери. Дали единичен компјутер поврзан со интернет и дел од систем?  Поголема е веројатноста дека компјутерот на жена му на Боби на работа е дел од систем. Најверојатно, таа е дел од некоја локална мрежа (LAN ) или поширока мрежа (WAN ) или интернет. Дали Боби го попречил функционирањето на системот ?  Боби може да каже дека тој не е одговорен за ускратувањето на услугите и дека тој немал намера да предизвика таков настан. Напротив, тој сакал системот да продолжи да работи, за да може да открие што прави жена му. Честопати, нападите за ускратување на услугите не се доволни за да еден сајт биде симнат офлајн. Но провајдерите го симнуваат сајтот за да ги минимизираат влијанијата од нападот врз системот и да ги минимизираат непријатностите за другите корисници.  Во ова сценарио, се чини дека Боби ја нема потребната намера/умисла согласно Член 5, но тоа секако не значи дека ја избегнува кривичната одговорност.  Ова е пример за Тројански вирус, кој криминалците многу често го користат за да остварат пристап до компјутерите на други лица. | | | | |
| 53 | | **Случај од практиката 9**  **Факти / сценарио**  Една онлајн интернет ‘хакерактивистичка‘ група која се противи на користењето животни за тестирање на козметика извршува напад наречен: „дистрибуирано ускратување на услуги“ ( DDOS) против веб страниците на козметичките компании и списанија за убавина. Преку нивната веб страница, групата дистрибуира софтвер кои го нарекуваат „Супер-пиштол“ (‘Supergun’), со помош на кој што можат да ги координираат нападите на веб страниците, и да го максимизираат сообраќајот упатен до одредена страница во одредено време. Овој софтвер првобитно бил развиен од системските администратори за тестирање на безбедноста на нивните системи. Но, и покрај тоа што софтверот се уште функционира на ист начин, корисничкиот интерфејс е сега многу полесен за користење и го носи логото на групата.  *Дали е престап да се направи програмата Супер -пиштол достапна за преземање (даунлоудирање)?*  *Дале е престап да ја имаш програмата Супер-пиштол?*  **Прашања**  Дали фактот што супер-пиштолот може да се користи и за легитимни цели значи дека не може да се покрене судска истрага?  Дали тоа што Супер-пиштолот е достапен за преземање е еднакво на дистрибуција?  **Точки за дискусија**  Делата поврзани со овој член се; неовластен пристап, нелегално пресретнување, упад во податоци и систем.  Првобитно софтверот имал двојна намена, т.е. имал и легитимна функција, Дали сега, со модификација на корисничкиот интерфејс , самото поседувањето на овој софтвер може да се смета за престап?  Во претходниот случај од практиката, софтверот „пристапот до сите делови“ кој Боби го искористи за да влезе во компјутерот на неговата жена има и легитимна употреба. Програмите како оваа им овозможуваат на корисниците да влезат во своите компјутери од далечина.  Дали тоа што Боби поседувал софтвер за разоткривање на лозинки преставува престап? Дали тоа е прашање на умисла? Која легитимна причина имал Боби да поседува таков софтвер? Дали има докази со кои може да се докаже дека тој го употребил овој софтвер за да направи престап?  Ова кривично дело нема за цел да се употребува за криминализација на легитимните софтвер провајдери и корисници. Во случај како што е овој, каде што има лоша намера, тоа не проблем. Но, лицата кои се бават со компјутерски криминал честопати се бават и со легитимни интернет активности; може да се и професионалци кои користат и развиваат таков софтвер, а кои, кога ќе им се пружи можност, се подготвени да го постават/користат за нелегални активности? Што е пак со сопствениците на продавниците за вакви програми?. Како можат тие да знаат кои се намерите на купувачот на одреден вид на хардвер или софтвер? Дали опфатот на ова дело е недоволно дефиниран | | | | |
| 54 | | **Случај од практиката 10**  **Факти / сценарио**  Испорачувач на софтвер произведува шифриран софтвер. Софтверот ја дели содржината на тврдиот диск на две зафатнини. За пристап до двете е потребна лозинка. Но само едната зафатнина е видлива за обичниот корисник, додека скриената зафатнина не може да се детектира со форензички софтвер што постои во моментот.  Производителот тврди дека овој софтвер е корисен за сите лица кои може да се најдат под притисок да ја откријат нивната лозинка. Податоците на скриената зафатнина се безбедни, дури и ако тие ја откријат лозинката за видливата.  **Прашања**  Дали изработката, производството и дистрибуцијата или поседувањето ваков софтвер претставува кривично дело?  **Точки за дискусија**  Постојано сме предупредувани дека треба да ги обезбедиме податоците што ги чуваме. Јасно е дека една ваква програма би била корисна за лица кои се инволвирани во криминал, а особено лица кои стравуваат дека содржините во нивниот компјутер може да ги инкриминира. Тие не ја користат оваа програма за извршување на кривично дело, туку за прикривање докази.  Лицата кои што се бават со компјутерски криминал може да користат други и програми или системи за да избегнат откривање - вклучително и програмот за анонимност, со кои е можно да се сурфа на интернет без откривање на вистинската ИП адреса, или програмот „елиминатор на докази“ со кој може да се избрише содржината на тврдиот диск. | | | | |
| **55** | | **Случај од практиката11**  **Факти / сценарио**  Ник работи за ИТ одделот на една голема компанија која има сопствен интранет. Компанијата не им дозволува на вработените да ги користат компјутерите и интернет конекцијата на компанијата за купување онлајн. Во слободното време, Ник почнува да работи на софтвер што ќе и овозможи на компанијата да ги разоткрие вработените кои вршат плаќања онлајн. Програмата треба да ги запишува овие информации за да тие можат подоцна да се искористат како доказ при дисциплинската постапка. Но, Ник не е доволно вешт тоа да го направи сам, и затоа *онлајн* стапува во контакт со Јупитер. Заедно, тие развиваат софтвер што, откако ќе се преземе на компјутерот на корисникот, се активира кога корисникот почнува да пополнува онлајн образец, како оние што се користат за онлајн плаќања, и ги запишува податоците што ги внесува корисникот. Компанијата на Ник е многу задоволна, а Јупитер почнува да го развива софтверот со Тројанска програма.  *Дали Ник направил кривичен престап*  *Дали компанијата направила кривичен престап ?*  *Дали Јупитер направил кривичен престап?*  **Прашања**  Дали уредот е изработен или прилагоден за извршување на одредени кривични дела?  **Точки за дискусија**  Лицата кои се бават со компјутерски криминал можат да пристапат до многу алатки што им овозможуваат на извршат престап, или им помагаат тоа да го сторат. Можно е да се купи код со кои може да се изгради сопствен „бот“,може да се купи „ботнет“ или пристапот до ботнет што ќе му овозможи на корисникот да врши разни видови кривични дела, како на пример „фишинг“ .  Јупитер ќе ја користи оваа програма за да дојде до финансиски информации за лицата, кои може да ги користи тој самиот или други лица. Компанијата мисли дека Ник го изготвил овој софтвер во текот на работното време. Ник е невин; тој не сакајќи му помогнал на Јупитер да направи моќна алатка за вршење криминал. Ниту Ник, ниту компанијата ја немаат потребната кривична намера/умисла. Дали работите би биле поинаку поставени доколку Јупитер започне да ја нуди програмата за продажба на други компании кои сакаат да следат што нивните вработени прават на интернет. Дали може Јупитер да рече дека софтверот има легитимна цел, и покај неспорната привлечност за криминалците? | | | | |
| 56 | | **Случај од практиката 12**  **Факти / сценарио**  Стефан користи комерцијален фотографски софтвер за изработка на реалистичен банкарски налог на неговиот домашен компјутер. Го носи налогот во банка, која го прифаќа, и префрла пари на сметката на Стефан.  *Каков престап прави Стефан?*  **Прашања**  Дали изработката на фалсификуван банкарски налог е дело на фалсификување поврзано со компјутер?  Дали ова дело се смета за сторено само откако банкарскиот службеник ќе го прифати како вистински?  **Точки за дискусија**  За изготвувањето банкарски налог е потребно во компјутерот да се внесат неточни податоци т.е. дека е изготвен налог за исплата на Стефан. Но, дали е ова е сторено противправно или Стефан има право да изготви ваков документ на сопствениот компјутер. Стефан можеби имал намера да го искористи овој налог за да ја измами банката, но од одредени причини, никогаш не стигнал да го отпечати налогот. Дали постоењето на овој документ во хартиена верзија би променило нешто во однос на одговорноста на Стефан?  Ова дело нема толку за цел да ги санкционира сценарија од овој вид, иако може да е од корист доколку националните закони не го криминализираат изготвувањето на фалсификувани банкарски налози. Ваквите дела е подобро е подобро да се разгледуваат од гледна точка на второстепена одговорност, т.е. обид.  Ова дело има за цел да ги санкционира лицата кои го користат компјутерот како механизам за извршување на кривично дело, така што банкарскиот службеник, со добра волја ги внесува податоците што му ги дал Стефан , сметајќи ги за автентични. | | | | |
| 53 | | **Случај од практиката 13**  **Факти / сценарио**  Стефан отсекогаш им се фалел на пријателите дека како тинејџер бил одличен спортист. Неговите пријатели не му веруваат. Тој успева да влезе во базата на податоци на еден негов стар пријател и ги преиначува записите така што тие го прикажуваат него како капитен на училишниот тим по атлетика, со многу освоени медали  *Дали овој престап е фалсификување?*  *Дали ова е дело е фалсификување поврзано со компјутер?*  **Прашања**  Изменетите податоци нема да произведат правни последици  **Точки за дискусија**  Стефан ги изменил податоците и внел неавтентични (лажни) податоци. Јасно е дека пристапот и направените измени се преземени противправно.  Настрана се друго што Стефан можеби направил како дело, мала е веројатноста дека извршил фалсификување поврзано со компјутер, со оглед на тоа дека овие податоци нема да произведат правни последици.  Делото фалсификување поврзано со компјутер не се бави со финансиска или друга корист; овој вид дела спаѓаат под делото измама поврзана со компјутер. Овој член има за цел да ја осигури безбедноста и сигурноста на електронските податоци што може да произведе последици во правните односи. Терминот „за правни цели“ се однесува на трансакции и документи кои се релевантни од правна гледна точка. | | | | |
| 58 | | **Случај од практиката 14**  **Факти / сценарио**  Откако ја изгуби работата во полиција и се разведе, Боби бара алтернативни начин како да заработи за алиментацијата на поранешната сопруга. Отсекогаш се интересирал за работење со акции и купува 1000 акции во *Flanders Mining Inc ,* компанија со ексклузивно право да врши ископување на ураниум . Акциите ги купува за 1 евро по акција. Боби е исто така член на еден интернет форум, каде што другите членови, исто како и Боби, се интересираат за берзата. Боби постира порака во која што вели дека еден пријател во белгиската Влада му рекол дека во Белгија се откриени значителни резерви на ураниум. По оваа објава, цена на акциите на *Flanders Mining* вртоглаво расте, и до крајот на неделата една акција вреди 1000 евра. Боби тогаш ги продава своите акции.  *Дали Боби направил престап?*  **Прашања**  Дали пораката на Боби е невистинита?  Доколку пораката е невистинита, дали таа како резултат доведува до економски загуби за други лица?  Дали Боби стекнал економска корист?  **Точки за дискусија**  Ако пораката што Боби ја постирал е невистинита, тогаш е можно тој да има извршено кривично дело. Внел лажни податоци во компјутерот, и се стекнал со економска корист со растењето на цената на акциите.  Дали причинско-последичната врска помеѓу вносот на податоци и последиците од тоа е премногу лабава?  Дали Боби на некој му предизвикал загуби? Има аргументи за тоа, со оглед дека акциите се неправилно вреднувани, и ако тоа е така, тогаш нивната вредност несомнено ќе падне. Но, треба да се има предвид дека берзите се многу непредвидливи. Зар вредноста на една акција не е цената што некое лице е подготвено да ја плати за неа во одреден момент. Дали тука некој навистина е измамен? Зар не се класините и пораките од ваков вид широко распространети на интернет? Дали некој воопшто би поверувал на ваков пост, или нема да може да види дека се работи за неопитен обид за манипулирање на цената на акциите? Дали ова значи дека на интернет не смее да се лаже? | | | | |
| 59 | | **Случај од практиката 15**  **Факти / сценарио**  Стефан оди со кола до банка. Во кола увидува дека нема ситни пари. Наместо пари, во автоматот за паркинг, става некаков жетон , а автоматот му издава билет  *Дали Стефан направил престап?*  **Прашања**  Дали автоматот за паркинг е компјутер?  Дали прави разлика тоа што автоматот директно издава билети и во целата ситуација нема измамено лице?  Каков е статусот на билетот за паркинг?  **Точки за дискусија**  Автоматот за паркинг е компјутер. Во него се обработуваат податоци во и се пресметуваат парите во однос на тарифата за паркинг, врз основа на што се издава билет за соодветно време. Стефан внел неавтентични податоци, жетон наместо соодветната мента. Во Член 7 не се предвидува дека внесените податоци треба да се обработени од човек.  Билетот за паркинг е фалсификат. Податоците користени за неговото издавања се лажни, и целта е контролорот на паркингот да мисли дека станува збор за автентичен билет, за да не му напише казна на Стефан. | | | | |
| 60 | | **Случај од практиката 16**  **Факти / сценарио**  Откако е уапсен, полицијата увидува дека Стефан поседува многу податоци од кредитни картички на голем број трети лица.  *Дали поседувањето на овие податоци е кривично дело?*  **Прашања**  Каков статус имаат компјутерските датотеки? Дали во правна смисла тие се „ствари“, и покрај тоа што, во основа, тие се само низа на бинарни кодови?  **Точки за дискусија**  Во Обединетото Кралство, поседувањето на нешта што се користат за измама се смета за материјално кривично дело. Се разбира, потребно е да се докаже потребната умисла, но тешко е да се аргументираат легитимни причини за поседување на вакви податоци.  Сосема е можно тоа да се смета за подготвително дејствие. | | | | |
| 61 | | **Случај од практиката 17**  **Факти / сценарио**  Адам е член на една ексклузивна онлајн група која разменува фотографии со сексуално злоупотреба на деца. Адам е исто така член на P2P групата за споделување на датотеки. Тој ги става ваквите фотографии од онлајн групата во заедничките P2P датотеки, со што тие стануваат достапни и за другите членови на таа мрежа.  *Каков престап направил Адам?*  **Прашања**  Дефиниција на производство, набавка и дистрибуција.  Адам преземал датотеки со слики од интернет. Дали преземањето може да се изедначи со производството на ваква слика? Преземањето, и особено складирањето на слики не компјутер не е како гледањето телевизија. Дејствието на преземање создава нешто ново -- компјутерска датотека, така што гледањето на овие слики на интернет значи и создавање на нови слики. Овој концепт може да им биде од корист на обвинителите.  П2П мрежите за споделување на датотеки им дозволува на членовите да пристапат до датотеки кои се заеднички и за другите со другите членови на мрежата. Со самото ставање на сликите во датотека за споделување, Адам нив ги прави достапни за дистрибуција. | | | | |
| 62 | | **Случај од практиката 18**  **Факти / сценарио**  Бил е уапсен на аеродром при враќањето од Камбоџа. Во неговиот преносен компјутер има многу слики од сексуален акт помеѓу него и деца што изгледаат како да потекнуваат југо источна Азија.  *Дали може против Бил да се покрене судска истрага за овие слики?*  **Прашања**  Јурисдикција  Избор помеѓу материјално кривично дело, поседување на слики и производство на слики.  **Точки за дискусија**  Околу производството на сликите, може да има проблеми во врска со јурисдикцијата, со оглед дека наликува дека се направени во странство.  Поседувањето не би требало да биде проблем.  Која би била позицијата доколку сликите биле пронајдени на неалоциран простор?  За да постои поседување, мора да постои и знаење и контрола. Бил можеби знаел, а можеби и не знаел дека до сликите кои биле избришани се уште може да се дојде преку тврдиот диск. Но тоа тој сам не може да го направи доколку нема технички средства и стручност за тоа. Но, останува работа на обвинителот (а зависи и од јурисдикцијата) дали ќе тој ќе се гони за производство на сликите или за поседувањето на овие слики во минатото.  Која би била позицијата доколку на сликите имало голи деца на три до седум годишна возраст кои си играат на плажа, а Бил даде објаснување дека е натуралист (нудист), но дека сепак гледањето на сликите му претставува сексуално задоволство?  Дали ваквите слики се нелегални или е прашање кое се решава на локално ниво. Во Обединетото Кралство е потребно сликите да имаат сексуален елемент, а мотивацијата на фотографот би се сметала за нерелевантна.  *Кој решава дали некоја слика е нелегална? Дали описот на делото е доволно јасен?* | | | | |
| 63 | | **Случај од практиката 19**  **Факти / сценарио**  WWW.Iuvfishin.com е веб сајт посветен на риболов. Сајтот е хостиран на сервери лоцирани во САД. Сопствениците на сајтот откриваат дека сајтот бил хакиран и дека на него се поставени и вметнати илјадници слики со злоупотреба на деца. Тоа е направено на начин што не овозможуваа овие слики да се видливи за обичните корисници на сајтот. Сајтот има запис на ИП адресите на лицата кои пристапиле кон овие фотографии.  ИП адресата што му се препишува на Џон и е дадена на полицијата во вашата земја. Тие ја бараат адресата на Џон и го запленуваат компјутерот на Џон во кој има илјадници фотографии со злоупотреба на деца. Од интернет историјата и податоците во овие датотеки, јасно е дека повеќето од овие фотографии се симнати од интернет.  *Кое кривично дело го направил Џон?*  **Прашања**  Како може да се докаже дека Џон е одговорен за сликите?  Ефектот врз осомничените за педофилија.  **Точки за дискусија**  Овој метод на прикривање слики не е редок. Но би било опасно да се бара налог само врз основа на ИП адресите, без да се знае како таа ИП адреса се логирала на тој сајт. До тоа можело да дојде сосема случајно, по препорака на друг сајт, и можено е дека лицата не ги отворил сликите откако виделе за што станува збор. Секако, можно е да го попетелиле и неколку пати, и да отвориле повеќе слики.  Ова може да се искористи за дискусија околу предострожнота што е потребно да се има пред да се обвини одредено лице за педофилија. Кај лицата обвинето за овие кривични дела има висока стапка на самоубиства. Како и кај сите предмети на компјутерски криминал, и мора да се утврди дека осомниченото лице се наоѓало на тастатурата во одредено време. ИП адресата може да се користи од повеќе лица на истата адреса, или пак безжичната мрежа може да биде киднапирана. Обвинувањата од овој вид можат да имаат страшни последици кај невините лица. | | | | |
| 64 | | **Случај од практиката 20**  **Факти / сценарио**  Американската полиција демонтира еден сајт што хостира сајтови што нудат фотографии на злоупотреба деца за месечна претплата. Американските власти ги фаќаат податоците на оние кои платиле за пристап, вклучително и нивните ИП адреси, број на кредитни картички, е-пошта адреси, адреса до која се врши исплата и лозинка. Еден од корисниците е Освалд. По добивањето на соодветен налог, се пребарува неговиот компјутер. Не е најдено ништо инкриминирачко, бидејќи Освалд користел програма што се вика „Елиминатор на докази“.  *Дали Освалд направил престап?*  **Прашања**  Дали Освалд сторил материјално кривично дело или дело со второстепена одговорност?  Дали овде има прашања поврзани со јурисдикција?  Дали прави разлика тоа што американскиот сајт бил целосно автоматизиран?  Што треба да се каже во врска со користењето на програмата Елиминатор на докази?  **Точки за дискусија**  Освалд не поседува ниту една од сликите и не може да се докаже дека тој кога и да пристапил на вебсајт за да гледа такви слики, иако може да се докаже дека тој ја платил претплатата да може тоа да го прави. Но, Освалд платил пари за да наговори друго лице, сопственикот на сајтот во САД, на дистрибуција или да овозможи дистрибуирање на слики со злоупотреба деца. Дали тоа претставува престап?  Фактот што американскиот сајт е целосно автоматизиран значи дека нема живо суштество што е вклучено во процесирањето на информациите од кредитните картички. Но, без оглед на тоа, процесот го создало и администрирало лице кое од тоа има финансиска корист.  Користењето на програма за бришење на докази не е само по себе нелегално. Освен ако Освалд не ја активирал програмата во текот на полициската истрага, веројатноста дека тој направил престап поврзан со спроведувањето на правдата не е многу голема. Но, доколку Освалд се гони, тогаш судот може да го смета користењето на таква програма за отежнувачка околност. | | | | |
|  | | Практични вежби (доколку се предвидени)  За оваа сесија не се подготвени практични вежби. | | | | |
|  | | Проверка на знаењето  Обучувачот треба да го провери знаењето преку поставување соодветни прашања поврзани со секој од аспектите разработени во оваа сесија | | | | |
| **65 - 66** | | Преглед / Резиме  Обучувачот треба да направи резиме / го тестира знаењето за следните теми:   * Одредбите од материјалното кривично право и некои клучни фактори што се користат за опишување на кривичните дела во Конвенцијата од Будимпешта. * Одредбите од материјалното кривично право и некои клучни фактори што се користат за опишување на кривичните дела во * национално законодавство. * Потребата и предноста од усогласување на националното законодавство со меѓународните инструменти, особено Конвенцијата од Будимпешта. * Релевантните одредби од материјалното право поврзани со дискусиите за случаите од практиката. | | | | |
| Сесија 1.2.4 Домашно процесно право | | | | | | **Времетраење: 90 Минути** |
| **Потребни ресурси**   * Преносен компјутер или ПЦ со Windows 7 и Office 2010 * Проектор * PowerPoint Презентација | | | | | | |
| **Цел:**  Целта на оваа сесија е учесниците во секоја земја да се запознаат со истражните мерки што ги овозможува националното законодавство и регулатива за електронски докази. | | | | | | |
| **Задачи:**  На крајот на оваа сесија, учесниците ќе бидат во можност да:   * Ја идентификуваат националната регулатива за електронски докази * Ги идентификуваат истражните мерки што се дозволени согласно националното законодавство, и вредноста и условите за собирање и зачувување на електронски докази * Идентификуваат некои специфичности во домашните постапки во врска со електронските докази, а во контекст на меѓународната правна рамка | | | | | | |
| **Вовед**  Оваа сесија е подготвена за да на учесниците им предочи пример како Конвенцијата од Будимпешта е вградена во националното законодавство на една земја, во дадениот случај, Португалија. Обучувачите треба да ги заменат информациите за Португалија со соодветни информации за законодавството во секога од земјите што се опфатени со обуката. | | | | | | |
| **Слајд бр.** | | | **Содржина:** | | | |
| **1 - 29** | | | *PowerPoint* (или друг вид презентација)  Содржината на овие слајдови се пример за информациите што треба/може да се покријат со локалните обуки.  Во идеални услови, сесијата за електронски докази треба да ги спомене меѓународните правни инструменти што ги потпишала или ратификувала земјата, и како тие се транспонирани во домашното законодавство.  Исто така, треба да се наведат сите видови истражни мерки што се дозволени согласно домашното законодавство, како и да се објасни важноста и условите за прибирање и зачувување електронски докази.  На крај, доколку тоа е соодветно, треба да се образложат некои специфичности на домашните постапки, доколку тие постојат. | | | |
| **2** | | | **Агенда**  Оваа презентација има три дела:  Дел 1 ги покрива процесните одредби на Конвенцијата од Будимпешта;  Дел 2 ги покрива процесните одредби согласно националното законодавство;  Дел 3 е резиме на двата погоре наведени дела. | | | |
| **3** | | | На крајот на оваа сесија учесниците ќе можат да ги објаснат процесните одредби во Конвенцијата од Будимпешта и да ги објаснат процесните одредби што постојат во домашното законодавство. | | | |
| **5** | | | **Дел 1 – Процесни одредби во Конвенцијата од Будимпешта**  Еден од најважните аспекти на Конвенцијата што мора да се нагласи е процесната димензија. | | | |
| **6** | | | Член 14 на Конвенцијата од Будимпешта и дава многу широк опсег. Согласно овој член, Конвенцијата се применува, и тоа е очигледно, во случаи кога кривичното дело што се истражува е престап наведен во Конвенцијата .  Но, исто така се даваат и две многу далекосежни можности:  Процесни одредби што се користат при истрага на кое било кривично дело, доколку е извршено со компјутерски систем;  Правилата исто така се однесуваат на собирањето на електронски докази во врска со кое било кривично дело. Тоа значи дека секое кривично дело може да се најде под процесните одедби на Конвенцијата за борба против компјутерскиот криминал. | | | |
| **7 - 10** | | | Во Член 16 и 17 се обработува итното зачувување на компјутерски податоци и итното зачувување и откривање на компјутерски податоци. И двете одредби се многу иновативни и значајни.  Традиционалните докази остануваат на местото на настанот подолго време, за разлика од дигиталните податоци - електронските докази – кои се многу нестабилни и многу брзо исчезнуваат.  Следствено, во Член 16 се воведува “итно зачувување” како итна времена мерка за зачувување на докази и за овозможување доволно време за добивање судски налог за заплена или откривање на овие податоци. Оваа мерка се однесува и на податоци од сообраќај и на содржината на податоците.  Комуникацијата на интернет може да се одвива и преку повеќе провајдери, не само еден. Важно е органите на законот да бидат во можност да им наложат на провајдерите кои учествуваат во одредена комуникацијата да ги зачуваат бараните податоци. Затоа, согласно Член 17, на сервис провајдерот може да му се наложи да обелодени доволно преносни податоци за да може да се утврди патот на комуникацијата.  Членовите 16 и 17 се однесуваат на конкретни податоци во конкретни истраги. Не треба да се меша со регулативата за задржување на податоци, со која што на провајдерите им наложува одредено време да ги чуваат сите податоци за сообраќај, во случај тие да им се потребни на органите на законот. Конвенцијата од Будимпешта нема одредба за задржување на податоци. | | | |
| **11 - 13** | | | Одредбата во Член 18 е исто така многу интересна. Секоја страна мора да усвои законодавни мерки со кои на органите на законот им се дава можност за издавање „налог за испорачување“. Органите на законот можат да издадат судски налог за граѓани и интернет сервис провајдери, со кој им се наложува тие на соодветните власти да им предадат податоци складирани во одреден компјутерски систем во нивна надлежност или да достават податоци за претплатници.  Согласно Конвенцијата , во налогот за производство мора да се специфицира природата и обемот на податоците што се бараат: јасно се вели дека мора однапред да се утврди кои податоци се потребни за истрагата; според тоа, се забранува *ловење на информации.* Целта на ова законско ограничување е да се спречи злоупотребата на овие нови истражни овластувања од страна на органите на законот. Во реалниот свет, претресот или заплената се однесува само на стварни предмети или документи кои се во врска со случајот што се истражува. Во дигиталниот свет, овозможувањето целосна дозвола за пристап до сите информации што се наоѓаат на даден хардвер би значело пристап до разни видови информации што се чуваат на тој компјутер, кои честопати не се поврзани со кривичното дело што се истражува и може да инволвира и трети страни (на пример во случај на комуникација преку е-пошта)  Член 16 е првиот чекор за зачувување на податоци. Член 18 е вториот чекор, и се однесува на откривање на зачуваните податоци на соодветните власти. | | | |
| 14 - 19 | | | Претресот и заплената се објаснети во Член 19 на Конвенцијата од Будимпешта.  Повеќето национални процесни одредби содржат општи прописи за вршење претрес и заплена, но не сите имаат и конкретни правила во врска со претрес и заплена на компјутери. Многу јуриздикции можат сосема добро да функционираат само со традиционални претреси и заплени. Но, реалниот свет ни кажува дека дигиталните истраги носат нови предизвици, претходно непознати, како меѓуповрзаноста на компјутерските системи.  Соочувајќи се со овие нови предизвици, Конвенцијата од Будимпешта предвидува конкретни правила за претреси и заплени во дигиталниот свет.  На пример, има конкретно правило во Член 19.2, кое се однесува на хипотетично проширување на претрес, во случаи кога при претресот на одреден компјутерски систем, истражителите утврдат дека треба да се изврши претрес и на друг компјутерски систем. Согласно Конвенцијата, во случај кога овластениот орган законски добие дозвола за пристап до одреден компјутерски систем или некој негов дел, и кога во текот на инспекцијата на овој систем органот заклучи дека има разумни основи да се смета дека бараните податоците се чуваат на друг компјутерски систем во таа јурисдикција, тој може „по итна постапка“ да го прошири претресот и на другиот систем.  Конкретно во врска со претресот, има одредени специфичности кои треба да се нагласат, бидејќи се карактеристични за новата дигитална средина, а тоа се разните можности за физичка заплена на компјутерски систем.  Повеќето законодавства имаат конкретни прописи за претрес во физичкиот свет, но не сите имаат посебна регулатива за новите и поефикасни начини за заплена на компјутерски податоци.  Во врска со тоа, Конвенцијата од Будимпешта поставува услов државите потписнички да усвојат законодавство со кое што при законската заплена на компјутерски податоци се овозможува:   * Физичка заплена на компјутерски систем, * Копирање на компјутерски податоци и задржување на копијата (што е значајно во случаи кога податоците се чуваат на поголем сервер чие е што физичко преместување е невозможно и во кога физичката заплена премногу интерферира со правата на други лица кои имаат право на пристап до тој уред – како на голем сервер на одредена компанија. * Одржување на интегритетот на релевантните зачувани компјутерски податоци, и * Ги направат овие податоци недостапни или истите ги отстранат од компјутерскиот систем што се истражува.   Оваа последна одредба е релевантна во случаи кога физичката заплена е невозможна, а пристапот до овие податоци од трето лице би предизвикало вистинска штета.  Со исклучок на заплената на податоци во оригинална форма, сите овие процесни мерки се однесуваат конкретно на дигиталната средина. | | | |
| 20 | | | Понекогаш, истражителот има потреба од понови податоци од оние зачувани на компјутерскиот систем. Собирањето на преносни податоци во *реално време*  дава можност за вршење истрага „во живо “, и оваа можност се разработува во Член 20 на Конвенцијата од Будимпешта. За вакви интрузивни мерки е потребно соодветно законодавство со што органите на законот се овластуваат да прибираат или евидентираат, со технички средства, податоци во *реално време,*  а потребни се и овластувања со кои органот може да му наложи на провајдерите да собираат или евидентираат преносни податоци за нивните корисници во реално време.  Овој вид истражна алатка може да биде многу важна, како на пример за утврдување на изворот на одредена комуникација, а со цел идентификување на сторителот во реално време. | | | |
| 21 | | | На крај, но не и најмалку важен е Членот 21 каде што се објаснува пресретнувањето на содржински податоци. Додатно на податоците за сообраќај, понекогаш органите на законот име потребно да ја знаат и содржината на комуникацијата помеѓу лицата осомничени за криминал. Некои земји веќе имаат одредби за следење на телефонска комуникација, но не сите дозволуваат пресретнување која не се одвива преку телефон. на комуникација им  Тоа е причината за Член 21, со кој што на истражителите им се овозможува да престретнуваат и евидентираат податочна комуникација.  Ова е моќна истражна алатка, но истовремено, пресретнувањето на комуникации е и многу интрузивна мерка и согласно Конвенцијата, се дозволува само во случаи на тешки кривични дела утврдени со националното законодавство. | | | |
| 23 | | | **Дел 2 – Процесни одредби согласно националното законодавство** | | | |
| 24 - 31 | | | Во овој Дел, обучувачите треба да ја внесат соодветната правна регулатива на земјата каде што се одржува обуката. | | | |
|  | | | Практични вежби (доколку се предвидени)  За оваа сесија не се подготвени практични вежби | | | |
|  | | | **Проверка на знаењето**  Обучувачот треба да го провери знаењето со поставување на релевантни прашања за сите аспекти на оваа сесија. | | | |
| 33 - 34 | | | Преглед / Резиме  Обучувачот треба на направи преглед/провери знаењето на учесниците за следните точки:   * националната регулатива за електронски докази * Меѓународната рамка, доколку постои * Видовите истражни мерки дозволени согласно националното законодавство, и значењето и условите за собирање и зачувување на електронски докази * Специфичности во домашните постапки во врска со електронските докази, а во контекст на меѓународната правна рамка | | | |
| Сесија 1.3.1 Дневен преглед | | | | | | **Времетраење: 30 Минути** |
| **Потребни ресурси**   * Преносен компјутер или персонален компјутер со *Windows 7* *и Office 2010* * Проектор * PowerPoint Презентација | | | | | | |
| **Цел:**  Целта на оваа сесија е да се направи преглед на активностите од претходниот ден, да се добијат повратни информации од учесниците и да се провери дали задачите зададени со сесијата се исполнети | | | | | | |
| **Задачи:**  На крајот на оваа сесија, учесниците ќе бидат во можност да:   * Ги идентификуваат активностите од претходниот ден што им се јасни * Ги идентификуваат деловите што треба да ги повторат за да го доведат нивното знаење на соодветно ниво | | | | | | |
| **Вовед**  Оваа сесија е подготвена за да им овозможи на учесниците да проверат дали ги разбрале предавањата од претходните денови, и да видат дали ги исполнуваат задачите зададени со поединечните сесии. Исто така, оваа сесија му овозможува на обучувачот  да го провери степенот на знаење на учесниците и да ги идентификува деловите каде што наставниот материјал може да се подобри. | | | | | | |
| **Слајд бр.** | | | | **Содржина:** | | |
| **1 - 12** | | | | **PowerPoint** (или друг вид презентација)  Овие слајдови треба да му помогнат на обучувачот и на учесниците да ги резимираат активностите од претходните денови За таа цел, обучувачот треба да ги искористи Агендите и Задачите за сесиите. | | |
|  | | | | Практични вежби (доколку се предвидени)  За оваа сесија не се предвидени практични вежби | | |
|  | | | | Проверка на знаењето  Обучувачот треба да го провери знаењето со поставување на релевантни прашања за сите аспекти на сесијата. | | |
|  | | | | Преглед / Резиме  Оваа цела сесија е наменета за резимирање на активностите од претходните денови, и затоа нема потреба од посебен преглед. | | |
| Сесија 1.3.2 и 1.3.3 Електронски докази | | | | | | **Времетраење: 120 & 90 Минути** |
| **Потребни ресурси**   * Преносен компјутер или ПЦ со Windows 7 и Office 2010 * Проектор * Пристап од интернет (доколку е достапен) * PowerPoint Презентација * Примери од хардвер (доколку се достапни) * Копија од упатствата за е-докази финансирани од EC OISIN | | | | | | |
| **Цел:**  Целта на оваа сесија е на судиите и обвинителите да им пренесе информации во врска со електронските докази, како на пример видовите електронски докази на кои што можат да наидат, како тие се добиваат, како се работи со нив во текот на истрагата, и како се презентираат на кривични судења. Дадени се и додатни информации во врска со предизвиците за добивање на такви докази од други јуриздикции. | | | | | | |
| **Задачи:**  На крајот на оваа сесија, учесниците ќе бидат во можност да:   * Дискутираат за повеќето видови електронски докази * Ги објаснат принципите на најдобрата практика поврзана со заплената и работењето со електронските докази * Ги идентификуваат предизвиците поврзани со „статичните податоци“, „живите податоци“ и интернет изворите на електронски докази * Ги идентификуваат предизвиците при добивањето докази од друга јруиздикција * Дискутираат за прашањето на прифатливост на електронските докази во судските постапки, во однос на веродостојноста, точноста и целовитоста | | | | | | |
| **Време траење** | | | **Содржина:** | | | |
| 30 минути  30 минути  60 минути  60 минути  30 минути | | | Вовед и отворање (Агенда и задачи на сесијата)  Дел 1 – Што се електронски докази  Дел 2 – Постапки и Добри практики  Дел 3 – Правни прашања  Преглед /Резиме | | | |
| **Вовед**  Оваа сесија има за цел на обучувачите да им даде една рамка за зготвување материјали за обуката која се предвидува како дел од една поширока програма. Тоа не може да биде сеопфатно, со оглед на тоа дека технологија брзо се менува и кој било детални технички спецификации што би се дале би биле веќе застарени при самото издавање на документот. Судиите и обвинителите мора да имаат задоволително познавање на техничките аспекти на предметите на кои што работат, и тоа е од суштинско значење за правично функционирање на судскиот систем. Оваа сесија дава преглед на аспектите на технологијата кои се релевантни за системот на кривичното право. На обучувачите како ресурс им се нуди *PowerPoint* Презентација, и можат да ја користат доколку сметаат дека тоа е соодветно.  Во оваа сесија се дадени информации за технологијата со која што ќе се соочуваат судиите и обвинителите во текот на нивната работа, која што криминалците ја користат за извршување кривични дела, а органите на законот за нивно откривање.  Оваа сесија како извор на материјали го користи документот „Заплена на е-докази“. Овој документ е изработен со финансиска поддршка од OISIN програмата на Европската комисија со референтен број 2002/OIS/014[[3]](#footnote-3). Документот е изготвен пред неколку години, и следствено, некои негови делови се веќе застарени. Во одредени релевантни делови, информациите се ажурирани и се вклучени во оваа обука. Документот е изготвен пред се за органите на законот: но принципите и постапките важат и за другите инстанци во системот на кривичното право. Овој документ може да се применува во сите случаи предмети каде што се предвидува заплена на електронски докази.  При толкувањето на мерките предложени во овој документ, секоја земја членка треба да ги има предвид националните документи и прописи. Исто така, секоја земја членка треба да додаде контакт информации за стручните одделенија во нивната земја.  Секоја организација или агенција што сака да ги примени препорачаните процедури, треба да ја одреди одговорноста за поединечните чекори/дејствија согласно внатрешната структура. | | | | | | |
| **Слајд бр.** | | | **Содржина:** | | | |
| 1 | | | ***PowerPoint*** (или друг вид презентација) | | | |
| **2** | | | **Агенда**  На овој слајд се дадени деловите од кои се состои сесијата, и обучувачот треба да ги помине, задржувајќи се на конкретни аспекти кои се важни за одредена група учесници. Обучувачот треба да објасни како ќе се предава материјалот, и дека е предвидено време за дискусија и прашања. Обучувачот треба да нагласи дека обуката треба да биде интерактивна, и дека низ целиот нејзин тек учесниците треба да придонесуваат со своето активно учество. Обучувачот треба да објасни дали се предвидува и оценување, и како тоа ќе се врши, вклучително и тоа дали ќе има преодна оценка и која е таа (за оваа пилот програма не се предвидува оценување). | | | |
| **3** | | | Важно е учесниците да ги разберат задачите на одредена лекција. Задачите треба да се “SMART” и тие треба детално да им се објаснат на учесниците пред почетокот на сесијата, користејќи ги информациите дадени на слајдот. | | | |
| **6** | | | **Дел 1– Што се електронски докази** | | | |
|  | | | **Видови и извори на електронски докази**  **Примери**  Обучувачот треба да започне со дискусија, така што ќе побара од учесниците да идентификуваат видови електронски докази со кои што тие се запознаети и ќе ги поттикне да споделат што тие знаат во врска со темата. Обучувачот треба да ги запише примерите што ги даваат учесниците на табла, а потоа да го дополни списокот со видови на докази кои учесниците не ги навеле. На списокот треба да се наведат и видовите докази, на пр. статични податоци, живи податоци, меморија, интернет, и изворите на докази, како што се оние во делот на обуката каде што се обработува технологијата. | | | |
| **8** | | | **Дефиниција**  Дефиницијата на доказ обично се дава во националното законодавство.  Со оглед дека во овој случај се работи за меѓународна обука, дадена е една општа дефиниција од речникот за правни термини Блек. Обучувачите треба да ја вметнат дефиницијата за докази што се применува во земјата каде што се одржува обуката.  „Доказ“ е каков било доказен материјал што страните во спорот го изнесуваат на суд преку сведоци, документи, предмети, материјали и слично, со цел да го убедат судот или поротата во исправноста на нивните тврдења“. Електронските информации обично се прифаќаат како доказ во судската постапка. | | | |
| **9 - 10** | | | Не постои меѓународно прифатена дефиниција за електронски доказ. Но, сите земји имаат регулатива во која се дадени принципите кои, на еден или друг начин, се однесуваат на *електронските докази.*  Еден корисен пример на „дефиниција“:  Информации или податоци важни за истрагата што се чуваат на или пренесуваат со електронски уред.  [www.nij.gov/topics/forensics/evidence/digital/digital-glossary.htm](http://www.nij.gov/topics/forensics/evidence/digital/digital-glossary.htm)  Уште еднаш, обучувачот има одговорност да ја внесе дефиницијата за докази што се користи во земјата каде што се одржува обуката, доколку таква постои.  Во борбата против современите форми на криминал потребна е поддршката на стручни и специјализирани службени лица кои ќе ги анализираат и правилно ќе ги толкуваат доказите во текот на истрагата и во фазите на судскиот процес. | | | |
| **12** | | | **Извори и видови на електронски докази**  Не е потребно да се врши навраќање на сите видови и извори на докази  идентификувани во делот на оваа обука поврзан со технологијата. Обучувачот само треба уште еднаш да го помине списокот сочинет на почетокот на оваа сесија.  Во изворите спаѓаат сите електронски уреди. Во оваа фаза, обучувачот може ќе сака да го истакне значењето на разни електронските докази од различни уреди и улогата што тие ја одиграле во дадени предмети.  Видовите на докази што ќе се опфатат се следни:   * Статични податоци * Живи податоци * Интернет податоци | | | |
| **13** | | | **Карактеристики на електронските докази**  Има многу карактеристики што создаваат додатни предизвици во однос на прифатливоста на електронските докази наспроти конвенционалните докази. Во повеќето случаи, со електронските докази се работи како и со традиционалните докази. Но, за судиите и обвинителите е од клучно значење да ги разберат прашањата што произлегуваат од електронската природа на овој вид докази и соодветно да одговорат на нив.  Од примерите што се дадени во оваа обука може да се види дека повеќето прашања се однесуваат како на електронските така и на конвенционалните докази. Но, има и некои разлики, и треба да се нагласат во оваа нејзина фаза.  Прашањата се следни:   * **Нестабилност** * Може лесно да се изменат * Може да не се долготрајни * **Природа** * Може да се јави потреба од специјализирани вештини за увид во нив * Може да се јави потреба од нивно стручно толкување * Може да се јави потреба од употреба на сила за добивање и пристапување кон нив, или пак нивното користење да биде ограничено * **Локација** * Може да се нераскинливо поврзани со не-доказен материјал * Може да се надвор од дадената јурисдикција * **Обем** * Идентификување на доказен материјал * Идентификување на неискористен материјал | | | |
| 14 | | | **Прашања поврзани со докази**  Карактеристиките на електронските докази доведуваат до одредени проблеми што треба да се истакнат. Обучувачот треба преку примери да ги објасни следните проблеми:   * Докази од втора рака * Деловни архиви/записи * Автоматизирани процеси * Испреплетени докази * Обем на доказите * Стручни докази * **Чувствителност.** Одредени дигитални податоци што ги обработуваат компјутерските системи се многу чувствителни, и лесно можат да се избришат или изменат. Овој аспект не се однесува само за оценувањето на доказите, туку и за процесот на нивно прибирање. Податоците што се чуваат само во РАМ системска меморија обично се губат при исклучување на системот доколку не се преземат посебни технички мерки што ќе го спречат тоа. Со оглед на тоа дека информациите што се чуваат во системската меморија можат да бидат од големо значење за истрагата, техниките за прибирање на ваков вид докази може да се разликува од процесите за прибирање на конвенционални докази. * **Подложна на измени.** Дигиталните податоци се подложни на измени. Еден од најосновните начела на компјутерската форензика и потребата да се одржи интегритетот на дигиталните докази. За да се избегне сомнежот дека доказите се манипулирани, од суштинско значење е да се обезбеди целосна документација на процесот и примената на методите за одржување на интегритетот. Затоа, компјутерските вешти лица одат кон тоа да ги заменуваат истражните процеси што водат до промени кај датотеките на компјутерот на осомниченото лице со други пософистицирани процеси * **Децентрализирано чување.** Широкопојасното поврзување и серверите за далечинско чување влијаат врз начинот на кои се чуваат информациите. Во минатото, во потребата по компјутерски податоци истражителите се фокусирале на местото каде што живее/работи осомниченото лице. Сега, мора да се има предвид дека дигиталните информации може физички да се чуваат и надвор од земјата и дека осомниченото лице може до нив да пристапи само од далечина доколку тоа е потребно. * **Брз технички развој.** Техничкиот развој продолжува да се одвива со брзо темпо. Има голем број новини што носат нови предизвици за форензичките испитувања. Овие новини наметнуваат потреба од континуирана обука за лицата кои учествуваат во прибирањето докази, и постојано осовременување на форензичката опрема. Новите верзии на оперативните системи и други софтверски производи може да генерираат поинакви податоци што можат да бидат релевантни за истрагата. Ист е случајот и со хардверот. Во минатото, податоците се чуваа на дискети, но денес истражителите мораат да водат сметка за тоа дека релевантни информации може да се чуваат и на MP3 плеери или саати со УСБ уред за чување податоци. | | | |
| 18 - 19 | | | **Дел 2– Процедури и добри практики** | | | |
|  | | | Овој дел од обуката во голема мера се потпира врз упатството за е-докази. Дадени се многу детали кои можат да му помогнат на обучувачот да ја подготви лекцијата. Тие се детално разработени во упатствата за обучувачот и резимирани како точки во соодветните слајдови. Обучувачот треба да размисли за тоа колку детално треба навлезе во темата во зависност од тоа што смета дека им е потребно на учесниците за да успешно ги совладуваат зададените задачите.  Упатството може да се користи во сите случаи каде што треба да се изврши заплена на електронски докази.  При толкувањето на мерките предложени во овој документ, секоја земја членка треба да ги има предвид националните документи и прописи. Исто така, секоја земја членка треба да додаде контакт информации за стручните одделенија во нивната земја.  Секоја организација или агенција што сака да ги примени препорачаните процедури, треба да ја одреди одговорноста за поединечните чекори/дејствија согласно внатрешната структура. | | | |
| **20** | | | **Општи начела**  Кога се работи со електронски докази, многу е важно да се следат следните општи начела:   * Сведочење на лице место, * Интегритет на податоците, * Ревизорска трага, * Стручна поддршка, * Обука на службените лица, и * Законитост и почитување на принципите   Овие начела се објаснуваат подолу | | | |
| **21** | | | 1. **Сведочење на лице место**   **Начело 1: *лице никогаш не треба да оди сам на местото на настанот***  Ваков вид активности треба да се вршат со најмалку две службени лица. На тој начин се заштитуваат самите лица, а и се фаќаат повеќе детали од местото на настанот. Службените лица треба да ги планираат и координираат нивните активности. Можните проблеми полесно се решаваат „кога размислуваат две глави“. | | | |
| **22** | | | 1. **Интегритет на податоците**   **Начело:** *Со ниту едно преземено дејствие не смее да се менува електронскиот уред или медиум, кој подоцна ќе се користи во суд.*  При постапување со електронските уреди и податоци, истите не смеат да се менуваат, ниту нивниот софтвер, ниту нивниот хардвер. Надлежното лице е одговорно за интегритетот на материјалот кој е собран од местото на настанот и од него почнува синџирот на процесот на постапување со доказите | | | |
| **23** | | | 1. **Ревизорска трагa**   **Начело:** *мора да се остави ревизорска трага или друг вид евиденција за сите дејствија преземени при постапувањето со електронските докази. Следејќи ја ревизорската трага независна трета страна би требало да го постигне истиот резултат.*  Од суштинска важност е точно да се евидентираат сите дејствија за да ѝ се овозможи на трета страна да направи реконструкција на дејствијата на лицето кое прво интервенирало на местото на настанот за да се обезбеди доказната вредност пред судот. Сите дејствија во однос на запленувањето, пристапот, чувањето или преносот на електронските докази мора да бидат целосно документирани, зачувани и достапни за контрола. | | | |
| **24** | | | 1. **Стручна поддршка**   **Начело:** *Доколку се претпоставува дека во текот на одредена операција ќе се најдат електронски докази, надлежното лице треба навреме да ги извести специјализираните стручни лица/надворешни соработници.*  Во истраги каде што има претрес и заплена на електронски докази може да биде неопходно да се консултираат надворешни специјализирани стручни лица. Сите надворешни експерти треба да бидат запознаени со начелата дадени во овој Прирачник или во други релевантни документи. Специјализираното стручно лице треба да го поседува следново:   * Неопходната специјалистичка експертиза и искуство на ова поле * Неопходни познавања за вршење истраги и познавања од областа на правото * Неопходни познавања за предметот на истрагата * Соодветни комуникациски вештини (и за писмени и за усни образложенија) | | | |
| **25** | | | 1. **Соодветна обука**   **Начело:** *Лицата кои први интервенираат на местото на настанот мораат да бидат соодветно обучени за да можат да го извршат претресот и да ги запленат електронските докази, доколку на местото на настанот не може да биде присутно специјализирано стручно лице.*  Во исклучителни околности кога е неопходно лицето кое прво интервенира на местото на настанот да собере електронски докази и/или да пристапи кон оригинални податоци кои се на електронски уред или дигитален уред за чување податоци, тоа лице кора да биде обучено тоа да го стори соодветно и да ја објасни релевантноста и импликациите на неговите дејствија. | | | |
| **26** | | | 1. **Законитост и почитување на начелата**   **Начело**: Лицето и органот надлежен за случајот се одговорни да обезбедат дека се почитуваат законот, општите форензички и процедурални правила и погоре наведените начела. Ова се однесува на поседувањето и пристапот кон електронските докази.  При толкувањето на мерките предложени со овој документ, секоја земја членка треба да ги земе предвид сопствените законски акти и прописи.  Еден од најважните меѓународни правни документи, Конвенцијата за компјутерски криминал на Советот на Европа, е отворена за потпишување за државите членки, за други држави кои учествувале во нејзината подготовка, и како и за пристапување на други држави | | | |
| **28** | | | **Видови заплена**  Има повеќе опции за запленување на електронски докази и тие се важен дел од обука. Сите тие носат различни карактеристики, ризици и резултати. Обучувачот треба да обрне внимание детално да ги објасни сите, за да учесниците можат да го разберат влијание што тоа го има врз нивната улога на судии и обвинители. Информациите што следат се во прилог на тоа на обучувачите да им помогнат да изготват соодветен материјал за тоа цел  Постојат четири општи видови заплена на е-докази:   1. Заплена со конфискација на електронската опрема и медиумите за чување на податоци; 2. Заплена со копирање на сета содржина на меморијата (пресликување или огледало); 3. Заплена со конфискација на медиумот за чување на резервната копија 4. Заплена со селективно копирање на податоци: и 5. Заплена на докази од интернет   Овие видови заплени се дискутираат во деловите што следат. Треба да се има во вид дека е сосема можно да се комбинираат повеќе видови заплена во рамките на една постапка за заплена. На пример, може да се јави потреба од конфискација на електронската опрема, но и на уредот за чување на резервната копија. | | | |
| **29** | | | 1. **Заплена на електронски опрена и медиуми за чување на податоци**   Овој вид на заплена може да соодветствува во услови кога:   * Нема многу опрема што треба да се конфискува, на пример поединечен компјутер или мала (пр. од станот на осомниченото лице); * Не постои ризик од големи финансиски или други загуби што би се предизвикале со прекинот на работа/недостапноста на конфискуваната опрема * Конфискацијата е апсолутно потребна поради природата на кривичното дело; * Има потреба од запирање на активностите што ги поддржува опремата што треба да се конфискува   Предностите на овој вид заплена се следни:   * Вообичаено може да се врши без стручна поддршка на местото на настанот; * Времетраењето на процедурата за заплена е кратко; * Електронските докази се земаат под контрола * Електронските докази може да се анализираат во контролирана средина.   Недостатоците на овој вид заплена се следни:   * Ризик од оштетување на опремата * Ризик од наштетување на лица кон не се поврзани со кривичното дело кое се истражува; и * Ризик од интерферирање во активности кои не се поврзани со кривичното дело што се истражува  1. **Заплена со копирање на сета содржина на меморијата**   Oвој вид заплена, што понекогаш се нарекува пресликување или огледало, се користи посебна опрема за да се направи потполно идентичен дупликат на содржината на меморијата на електронската опрема (или уред за дигитално складирање) на надворешен уред за складирање.  Овој вид заплена е соодветна кога:   * Има многу опрема што треба да се земе предвид (на пример мало или средно претпријатие); * Постои ризик од големи финансиски или други загуби што ќе се предизвикаат со неработењето/недостапноста на опремата (на пример ИТ системот да е од суштинска важност за трето лице) и * Конфискацијата не се смета за потребна имајќи ја предвид природата на кривичното дело.   Предностите на овој вид заплена се следни:   * Мал ризик од оштетување на опремата; * Мал ризик од нанесување штета на лица кои не се поврзани со кривичното дело што се истражува; * Мал ризик од интерферирање во активности кои не се поврзани со кривичното дело што се истражува; * Електронските докази може да се анализираат во контролирана средина   Недостатоците на овој вид заплена се следни:   * Има потреба од посебна опрема на местото на настанот; * Вообичаено има потреба од стручна поддршка; * Постои ризик од пренебрегнување на дел од доказите; * Процедурата за заплена бара многу време; и * Опремата за која што станува збор не се става под контрола.  1. **Заплена со конфискација на медиумот за чување на резервната копија**   Овој вид заплена може да е соодветна во услови слични на оние кога се врши заплена со копирање на целата содржина на меморијата, особено ако станува број за многу голема опрема и податоци (на пример големи мрежи, централни компјутери и сл.)  Предностите се слични како кај заплената со пресликување објаснета во Дел 2 (скоро и да не постои ризик од штета или штетни дејствија). Додатна предност е тоа што:   * Нема потреба од посебна опрема на местото на настанот; и * Нема потреба од долготрајни операции за пресликување на местото на настанот   Недостатоците на овој вид заплена се:   * Вообичаено има потреба од стручна поддршка на местото на настанот; * Вообичаено е потребна поддршката на локалниот администратор на системот; * Постои ризик од пренебрегнување на дел од доказите (затоа што целовитоста на резервната копија на податоците не може да се утврди однапред); и * Опремата во прашање не се става под контрола  1. **Заплена со селективно копирање на податоци**   Овој вид заплена треба да се користи само во исклучителни околности кога не е можно да се примени ниту една од претходно наведените видови заплена. Во вакви случаи се копираат само одредени податоци (најрелевантните) кои се анализираат подоцна. На местото на настанот е задолжително присуството на стручната поддршка.  Предностите и недостатоците се слични како и во случајот на заплена со конфискација на медиумот за чување на резервната копија. Додатен недостаток е тоа што не е возможно да се направи какво била анализа на историјата на компјутерот. Со тоа се ограничува и истражната вредност на овој вид заплена. Додатно, заштитата на доказната вредност на информациите добиени на овој начин бара големо внимание.   1. **Заплена на докази од интернет**   Заплената на докази од интернет е од суштинско значење во многу видови истрага, и потребни се специјализирано знаење, вештини и ресурси за да таа делотворно се изврши. Во рамките на оваа обука нема да навлегува во деталите на овој начин на прибирање податоци, освен што ќе нагласи дека и во овој случај треба да се применуваат општите начела дадени погоре. Има повеќе видови на прибирање податоци од интернет, и општо земено тие можат да се поделат на 1. Прибирање податоци од отворени извори на податоци, и 2. Прибирање со притаени средства. Во врска со тоа има многу правни и процедурални прашања, но тие нема да се елаборираат. Тоа е предвидено да се направи во модули што се дел од напредните обуки. | | | |
| **30 - 40** | | | **Постапка за заплена на е-докази**  Како што се напомена во Воведот, овој документ се бави со постапката за заплена на електронски докази што вклучува претрес, препознавање прибирање и документирање на заплена на е-докази. Постапката се состои од неколку фази, што детално се опишуваат подолу:   1. Подготовки за заплена (Дел 1), 2. Обезбедување на местото на настанот (Дел2 **.**), 3. Документирање на местото на настанот (Дел 3), 4. Собирање на докази (Дел 4), и 5. Пакување, транспорт и чување (Дел 5)   При изготвувањето на постапките објаснети подолу, предвид се земени клучните начела за претрес во ИТ средина препорачани од Советот на Европа.   1. **Подготовка за заплена**   Во текот на предистражната постапка чија што цел е добивање на налог за претрес, треба да се одреди дали постои веројатност да се најдат е-докази што се релевантни за дадениот случај. Во такво случај, надлежното лице треба што порано да го информира локалното одделение за фаќање докази и надворешните стручни лица. Првата одлука што се донесува е во врска со вид /видови заплена што ќе се врши (видовите заплена се опишани на слајд 28). Пред тоа да се стори, потребно е однапред да се соберат што е можно повеќе информации за ИТ системот што ќе се запленува со поддршка од стручните лица, како на пример:   * Компјутерски хардвер /оперативен систем / софтвер/апликации и информации поврзани со медиумот за складирање, * Информации поврзани со комуникациските уреди мрежата (ISP[[4]](#footnote-4), телефон, факс, модем, локална мрежа - LAN[[5]](#footnote-5), опрема на/за мрежа, итн.), * Кој е одговорен за компјутерскиот систем и/или мрежа (на пример, дали има локален администратор или пад администратор е надворешна компанија), * Колку опрема се очекува дека ќе се заплени (се однесува на заплената од Дел 1), * Колку податоци треба да се копираат (се однесува на видовите заплена од Дел • и 4), и * Дали има резервна копија на системот достапен на медиум за складирање (се однесува на заплената од Дел 3).   Подготвителната фаза ги вклучува следните чекови:   * Обезбедува дека постои соодветно овластување за заплената на е-докази (на пример добивање налог за претрес согласно односните закони); * Обезбедување на што е можно повеќе информации за ИТ системот што ќе се запленува (види погоре); * Избирање на членови на тимот (вклучително и инженери, доколку тоа е потребно); * Назначување на поединечни задачи на членовите на тимот; * Брифирање на членовите на тимот за тоа како да ги извршат зададените задачи (тие треба да ја имаат поминато основна обука за тоа); и * Снабдување со потребните алатки и опрема за вршење на заплената логистика).   Како што беше и порано споменато, сите активности треба да се во согласност со политиките на агенцијата/органот и законите на ЕУ, како и државите и локалните закони.  **Членови на тимот за заплена**  Доколку е познато дека на местото на настанот може да има е-докази, тимот за заплена треба да вклучува и службени лица посебно обучени за вршење претрес и заплена на ИТ опрема и е-докази. Во одредени случаи, можеби ќе биде потребно да се консултира и независно стручно лице (види исто така Дел 4). На пример, доколку системот го администрира надворешна компанија или администратор, може и тоа лице да се вклучи како стручен сведок (во случај да не се работи за осомничено лице). Основниот услов е лицата кои први интервенираат на местото на настанот да имаат основна обука за собирање е-докази.  Треба да се изберат членовите на тимот, а потоа надлежното лице треба да им се зададе задачи соодветни за фазите на постапката за заплена (види исто така Слајд 30). Фазите и соодветните задачи се опишани во наредните Делови.  Секој член на тимот треба да има соодветни инструкции за извршување на зададените задачи. На пример, тие треба да знаат кога да ги применат истите начела за постапување со електронски докази, како и за постапување со други материјални докази, а кога да преземат специјални мерки (на пример алуминиумскиот прав не треба да се користи за да се земат отпечатоци од прсти од електронските уреди). Тие исто така треба да знаат дека во одредени случаи тие мора да стапат во контакт со специјализирано одделение и затоа треба однапред да имаат податоци за контакт со таквото одделение.  **Алатки и опрема за заплена**  За прибирање на електронски докази може да се потребни специјални алати и опрема. Технолошкиот напредок ги диктира промените во потребната опрема и алати. Следниов основен пакет на опрема може да биде од помош во текот на претресот и заплената и истиот треба да го обезбеди членот на тимот одговорен за логистика:   * Алати за расклопување и отстранување; * Завртувач (обичен и со крстаст облик – плус и минус, како и оние специјализирани за одреден производител на опрема, на пример за опрема на Hewlett Packard, Apple); * Хексагонален, ѕвездест и завртувач за сигурносни завртки; * Клешта (стандардна и шпиц клешта); * Секач на жица (за отстранување на пластични заврзувачи на кабли); * Мала пинцета; * Документација: * Белешка за претрес и заплена (список на предмети); * Етикети и лента (за обележување и идентификување на составните делови на системот, вклучувајќи ги и доводите и штекери); * Етикети за кабли; * Показни етикети (за заврзување и самолепливи); * Други потребни формулари за документирање на местото на настанот; * Перманентни маркери во боја (за да се означат со шифра и да се идентификуваат одземените предмети); * Фото апарат и/или видео камера (за да се фотографира местото на настанот и приказот на екранот); * Опрема за пакување и транспорт: * Антистатички вреќи (за заштита на опремата која се одзема како што се електронски плочи; треба да се одбегнуваат материјали кои може да произведат статички електрицитет, како што се полиетиленски кеси); * Антистатички меурест најлон; * Пластични заврзувачи за кабли (за собирање на каблите); * Вреќички и лента за докази; * Кутии за пакување на екстерните уреди за чување на податоци како што се УСБ уреди, дигитален видео диск- ДВД , или компактни дискови - ЦД; * материјали за пакување (треба да се одбегнуваат материјали кои може да произведат статички електрицитет како што се пенопластика или топчиња од пенопластика); * Несклопени картонски кутии и готови кутии од поцврст картон со различни големини (оригиналните кутии за пакување треба да се користат секогаш кога истите се достапни); * Комуникациска опрема:   + Мобилни телефони или други средства за комуникација за добивање упатства (кои не треба да се употребуваат во близина на компјутерска опрема);   + Информации за контакт заради барање помош (на пример телефонски број од специјализираното одделение); * Други предмети:   + Џебна светилка;   + Ракавици;   + Рачeн вилушкар;   + Големи ластици;   + Лупа;   + Хартија за печатење;   + Лаптоп компјутер, како и сите стандардни форензички алатки;   + Мрежни кабли (испреплетен пар и вкрстени кабли);   + Достаточен капацитет на тврд диск (на пример терабајтни екстерни тврди дискови);   + Форензички диск со пристап само за читање (за пренос на податоците на вашиот лаптоп);   + Форензички ДВД за подигање (доколку сте поминале обука за негово користење во форензички цели);   + Транспорт (до и од местото на настанот на членовите на тимот, на алатот и опремата за заплена и на запленетите докази).  1. **Обезбедување на местото на настанот**   Лицето кое прво интервенира на местото на настанот треба да ја осигура безбедноста на сите лица на местото на настанот, обезбедувајќи го и интегритетот на сите докази - и на традиционалните и електронските докази.  Оваа фаза ги опфаќа следниве чекори:   * Следете ја националната регулатива за обезбедување на местото на кривичниот настан: * Отстранете ги сите лица од самото место од каде треба да се соберат доказите (вклучително и опрема и довод на електрична енергија); * Заштитете ги нестабилните физички и електронски податоци:   + Идентификувајте, обезбедете, документирајте и фотографирајте го секој уред што содржи податоци што лесно се уништуваат;   + Набљудувајте ги потенцијалните осомничени лица за да тие не бидат во можност да ги изменат или уништат доказите;   + Набљудувајте ги ИТ компонентите заради спречување или уништување на доказите   + Идентификувајте и документирајте ги сродните електронски компоненти кои нема да бидат отстранети од местото на настанот;   + Идентификувајте ги телефонските и мрежните линии приклучени на уредите и документирајте ги и означете ги;   + Одлучете дали се потребни други докази од уредот кој треба да се заплени (на пример ДНК, отпечатоци од прсти, катализатор);   + Доколку е потребно, следете ги општите постапки за постапување со таков вид на докази дадени во соодветниот прирачник;   + Одложете ги деструктивните техники **сè додека** не се соберат електронските докази;   + Соберете ги потенцијалните отпечатоци од прсти откога ќе заврши собирањето на електронските докази (бидејќи тастатурите, компјутерските глувчиња, дискетите, ЦД-та или другите компоненти може потенцијално да имаат отпечатоци од прсти или други материјални докази кои треба да се зачуваат);   + Не користете алуминиумски прав за собирање на отпечатоци од прсти на местото на настанот, бидејќи истиот може да ги оштети опремата и податоците.   + При претресот побарајте и не-електронски, но релевантни докази како што се: * Пишани лозинки и други рачно напишани белешки, * Празни тефтери на кои има отпечаток од претходно напишан текст, * Прирачници за хардвер и софтвер, * Календари или дневници, * Отпечатени текстови или графики, * Фотографии, или * Информации за личните интереси кои подоцна може да бидат корисни за разбивање на лозинките / шифрите (најголем дел од лозинките се директно поврзани со личната средина, како на пример регистарските таблички на автомобилите, партнери/деца, телефонски броеви, хоби, итн.).   • Спроведете прелиминарни разговори:   * Одвојте ги и идентификувајте ги сите лица (сведоци, поврзани лица или други) на местото на настанот и забележете ја нивната позиција односно локација во времето на влегување на местото на настанот; * Користете листа за проверка и евидентирајте ги информациите добиени од сите овие поединци; * Во согласност со регулативата на органот и важечките закони, од овие лица соберете информации како што се:   + Намената на уредот/системот (на пример книговодство);   + Сопственици и/или корисници на уредите/системите најдени на местото на настанот, како и лозинките (видете подолу), корисничките имиња и интернет провајдерот;   + Било која лозинка потребна за пристап кон системот, софтверот или податоците (Едно лице може да има повеќе лозинки на пример за пристап кон БИОС, за пријавување на системот, на мрежата или провајдерот, апликациски датотеки, шифрирани лозинки како за PGP- криптографска компјутерска програма, Truecrypt- отворена програма за шифрирање на тврди дискови или негови делови и на преносни уреди за чување на податоци, електронска пошта, токен за пристап, план за извршување на задачите во компјутерскиот систем, контакт листи);   + Било какви единствени безбедносни планови или уреди за уништување;   + Било кои уреди за чување на податоци кои не се на местото на настанот; и   + Било каква документација која го објаснува хардверот или софтверот инсталиран на системот;  1. **Документирање на местото на настанот**   Документирањето на местото на настанот е тековен процес кој трае за целото време на вкупната постапка за запленување. Од суштинска важност е точно да се документира локацијата и состојбата на компјутерите, уредите за чување податоци, другите електронски уреди и конвенционалните докази. Во претходниот и наредниот дел се дава детален преглед на информациите кои треба да се документираат. Во овој дел се дава само преглед на овие инструкции.  Општо земено, мора да се документираат следните работи, но во текот на фазата на прибирање на доказите може да се создаде и дополнителна документација:   * Физичката состојба на местото на настанот: * Изработете скица на системот, вклучувајќи ја на пример и местоположбата на глувчето и локацијата на компонентите; * Направете фотографии, видео снимки од местото на настанот[[6]](#footnote-6) (доколку е можно опфат од 360 степени); * Компјутерски системи и електронски компоненти/уреди/опрема * Документирајте го следново: * Податоци за вкупната релевантна опрема која е најдена, на пример марка, модел, сериски број; * Состојбата и локацијата на секој компјутерски систем кој содржи или прикажува електронски докази, вклучително и статусот на компјутерот (вклучен, исклучен, состојба на мирување); * Документирајте ги сите конекции (кабловски или безжични) кон и од компјутерскиот систем или другите уреди; * Означете ги сите порти и кабли (вклучително и конекциите кон периферните уреди) што ќе овозможи повторно составување на системот подоцна; * Означете ги неискористените порти за конекции како „некористени“. * Идентификувајте ги приклучните станици на лаптопите за да идентификувате други уреди за чување медиуми; * Документирајте ги податоците за мониторот во времето на интервенцијата * Направeте фотографии на предната страна на компјутерот, како и од екранот на мониторот и останатите компоненти; * Составете белешки на писмено за тоа што е прикажано на мониторот; * Направете видео снимка од активните програми или направете подетална документација за активностите на мониторот; * Документирајте ги релевантните електронски компоненти кои нема да бидат отстранети од местото на настанот; * Информации собрани од лицата најдени на местото на настанот * Извршете разговор со лицата и документирајте ги нивните одговори/ пополнете ги формуларите; * Документирајте го следново: * Податоци за сите лица присутни на местото каде се извршува претресот; * Податоци за сите лица кои го користеле релевантниот компјутерски систем/ опрема; * Забелешки, коментари и информации кои ги даваат корисниците или сопствениците на компјутерите и сведоците; * Дејствијата преземени на местото на настанот; * Составете ревизорска трага / белешка за заплената со опис на преземените дејствија и точниот датум и време.  1. **Собирање докази**   Информатичкиот систем не треба да се заплени како доказ само затоа што се нашол на местото на настанот. Таквата мерка мора да се образложи и да биде пропорционална со предметното дело,па затоа лицето кое издава наредба за претрес треба да донесе свесна одлука дали одреден предмет треба да биде запленет од истражните органи и треба да има разумно сомневање или достаточно докази со кои се оправдува истрагата.  Со електронските докази, како и со сите други докази, мора внимателно да се постапува на начин со кој се зачувува нивната доказна вредност. Ова се однесува не само на физичкиот интегритет на предметот или уредот, туку и на електронските податоци кои истиот ги содржи. Одредени видови на електронски докази затоа бараат посебен начин на прибирање, пакување и транспорт. Електронските докази кои може да се оштетат или изменат со електромагнетски полиња (како што се електромагнетски полиња генерирани од статичкиот електрицитет, магнети, радио станици и други уреди) треба соодветно да се заштитат. Електронските докази треба да се запленуваат во склад со регулативата на релевантниот орган и важечките закони. Подолу се зборува за следниве видови на електронски докази:   * компјутерски системи, * други електронски уреди * дигитални уреди за чување на податоци * Информации поврзани со мрежата (конфигурации и сервиси/апликации) .   Во истрагата на електронски/компјутерски криминал од суштинско значење исто така може да биде и прибирањето на не-електронски докази (или конвенционални докази). Треба да се внимава и да се обезбеди дека таквите докази се прибрани и сочувани. Предметите релевантни за последователното испитување на електронските докази може да постојат и во друга форма (на пример напишани лозинки и други рачно напишани белешки, празни тефтери на кои има стисоци од претходно напишан текст, прирачници за хардвер и софтвер, календари, литература, печатени текстови или графики, фотографии) и истите треба да се обезбедат и зачуваат за идни анализи. Овие предмети често се во близина на компјутерот или релевантните хардверски делови. Сите докази треба да се идентификуваат, обезбедат и да се зачуваат во согласност со регулативата на надлежниот орган и важечките закони Пакување, транспорт и складирање Компјутерите и сродните уреди и опрема се кршливи електронски инструменти кои се чувствителни на температура, влажност, физички удар, статички електрицитет, магнетни извори, па дури и на определени дејствија (на пример вклучување и исклучување). Затоа мора да се преземат специјални претпазни мерки при пакувањето, транспортот и чувањето на електронските докази. За да се одржи непрекинат процесот на постапување со докази, за пакувањето, транспортот и чувањето треба да се води уредна евиденција.  Воопштено со сите компјутерски компоненти и уреди за чување на податоци мора да се постапува со најголемо внимание, со оглед на тоа што нестручното постапување може да предизвика оштетување или уништување на електронските докази   * **Пакување** * Осигурајте дека сите прибрани електронски докази се соодветно документирани и означени пред да се спакуваат. * Секогаш кога е тоа возможно, транспортирајте ги собраните електронски докази во нивните оригинални кутии за пакување. * Доколку не се достапни оригиналните кутии, користете анти-статички материјали за пакување (на пример хартиени или анти-статички пластични вреќи). Одбегнувајте материјали кои може да произведат статички електрицитет, како што се обичните пластични кеси. * НЕ ги превиткувајте, виткајте или гребете уредите за чување податоци како што се дискети, ЦД-РОМ, ленти. * Не лепете налепници на површината на уредите за чување на податоците. Секогаш кога е возможно користете кутии или коверти за пакување на уреди за чување на податоци. * Осигурајте дека сите кутии во кои се сместени доказите се соодветно означени. * Доколку се запленуваат повеќе компјутерски системи, означете го секој систем за да може подоцна одново да се монтира каков што бил најден. * **Транспорт** * Електронските докази треба да ги држите подалеку од магнетските извори. Радио-станици, магнети од звучници, седишта во автомобили кои се загреваат се примери за предмети кои може да ги оштетат електронските докази. * Обезбедете дека опремата е заштитена од удари и шокови (на пример механичко оштетување), топлина и влажност. * Обезбедете дека компјутерите и другите уреди кои не се спакувани во кутии се безбедно сместени во возилото за да се заштитат од удари и силно тресење. На пример, компјутерите треба да се стават на подот на возилото, а мониторите треба да се стават на седиштето со екранот свртен надолу и треба да се врзат со сигурносен појас. * Не ставајте тешки предмети на помали делови од опремата/уреди за чување податоци. * Секогаш кога е можно, не ги оставајте електронските докази долг период во возилото * **Складирање/чување** * Осигурајте дека за доказите е направена инвентарна листа во согласност со соодветната регулатива. * Чувајте ги доказите на безбедно место, вон влијанието на екстремни температури и влага. * Заштитете ги доказите од магнетни извори, влага, прашина и други штетни честички или загадувачи. * Користете соодветно обезбедена просторија за чување на доказите со соодветна   + контрола на пристапот,   + противпожарна заштита (на пример противпожарен аларм, апарат за гасење пожар, забрането пушење во просторијата или во близина на просторијата каде се чуваат доказите),   + температура и влажност и   + заштита од магнетни извори (на пример од радио-локациски уреди). * Не чувајте било какви запаливи предмети во истата просторија или во нејзина близина (на пример хемиски средства за чистење или хартија). * Користете соодветна подна простирка за да одбегнете статичко полнење. * Не ги чувајте електронските докази во простории со водоводни цевки, особено оние кои поминуваат преку таванот. * Морате да знаете дека потенцијалните докази, како што се датум, време и систем-конфигурацијата може да се изгубат заради пролонгирано чување на доказите. Со оглед на тоа што батериите имаат ограничено траење, податоците може да се изгубат ако истите се испразнат. Затоа соодветниот персонал треба да се информира дека уредот кој работи на батерија (на пример Персонален дигитален асистент (PDA), или PC/CMOS) потребно е веднаш да се обработи. | | | |
| **42 - 51** | | | **Истражување и анализирање на електронски докази**  **Компјутерска форензика**  Терминот компјутерска форензика се користи за опишување на систематската анализа на ИТ опрема со цел барање дигитални докази. Форензичката анализа вообичаено се одвива по извршувањето на кривичното дело. Во споредба со редовните истраги, извршувањето на ваков вид анализа носи со себе посебни предизвици, со оглед на тоа дека компјутерската технологија постојано се менува, и се повеќе податоци се чуваат во дигитален формат, со што се зголемува обемот на потенцијални докази. Главниот фокус е на можноста доказите да се користат во правната постапка. Со тоа до одредена мера за ограничува можноста за вршење форензички испитувања, бидејќи има ограничувачки правни стандарди. Дури и ако со новиот технолошки развој се овозможи нови форензички истраги, нивната примена е ограничена бидејќи тие нови инструменти се покриени со постојната правна рамка.  **Фази на вклученост на форензички експерти**  Форензичките експерти не само што се вклучено во кривичната постапка, туку играат и важна улога во граѓанската постапка и во развивањето стратегии за заштита и образованието. Во кривичната постапка, нивната вклученост се одвива во четири фази:   * Идентификација на релевантни докази. Форензичките експерти играат важна улога во развивањето на истражни стратегии. Тие ги поддржуваат органите за законот така одлучуваат која истражна техника е најдобра да се примени во даден случај, пред таа да се изврши. Исто така, Форензичките експерти како консултанти играат активна улога во истрагата, на пример со анализа на мрежната инфраструктура на местото каде што живее/работи осомниченото лице, со цел идентификација на можни локации за уреди за складирање. * Заштита/заплена/собирање докази. Прибирањето на дигиталните докази може да се одвива на физичката локација каде што тие се зачувани, или пак од далечина. Истражителите кои ги преземаат првите чекори за прибирање на доказите (лица кои први интервенираат) имаат значителна одговорност за целиот истражен процес. Ако донесат погрешна одлука во врска со заштитата на податоците, тогаш може да се изгубат значајни траги. Еден таков предизвик, на пример, е прашањето како да се постапи со компјутерот на осомниченото лице, што работи. Постапката што се предлага е компјутерот да се изгаси со пресекување на доводот на електрична енергија, наместо со командите на оперативниот систем. Но, во случаи кога лицето користело технологијата за енкрипција, прекинувањето на снабдувањето со струја може да доведе до дешифрирање на датотеките. Лицето кое прво интервенира треба да ја донесе таа одлука, во зависност од фокусот на истрагата.   Форензичката стручност не е релевантна само во однос на истрагите што се одвиваат на локациите каде што се чуваат релевантните податоци. Форензичките експерти можат да ја поддржат истрагата и со изготвување на барања до провајдерите и да ја помагаат истрагата со изготвување на соодветен историјат на случајот, кои се потребни за докажување на сигурноста на прибраните докази.   * Анализа на компјутерската технологијата и дигиталните докази. Наредната фаза ги покрива сите аспекти на анализата на дигиталните докази и запленетиот хардвер. Вообичаено тоа е најсложената фаза на целиот истражен процес. Лицата кои први интервенираат честопати запленуваат неколку уреди за чување податоци. Секој еден од овие уред може да содржи илјадници датотеки. Самиот обем на податоци што треба да се анализира претставува огромен предизвик за истражителите. Затоа, идентификацијата на релевантните информации за истрагата и нивното поврзување е една од најглавните задачи на вештите лица. Нивната работа вклучува активности од пребарување на компјутерски систем за нелегална содржина до анализа на записи за евиденција. Не сите процеси што ќе ги направи лицето при вршењето на компјутерски криминал оставаат траги. Со анализирање на сите достапни докази, вештите лица сепак успеваат да го реконструираат начинот на кој што е извршено делото. Третата фаза исто така вклучува изготвување на целосен извештај, кои што ги содржи и сите чекори во истрагата и методите користени за добивање докази.   **Примери на форензичко испитување**  Во четирите фази (а особено во третата) можни се повеќе форензички испитувања. Изборот на правата истражна техника зависи од различни фактори - особено на видот на престапот што се истражува  Меѓу најчесто користените техники спаѓаат:   * Анализа на хардвер. Доколку истражителите запленат компјутерски хардвер, тогаш вештите лица го анализираат хардверот за да соберат информации во врска со системот. Таквата истрагата може, на пример, да биде релевантна за докажување дали лицето имал можност да го приклучи компјутерскиот систем на интернет. Исто така, поради преносот на информации поврзани со системот во текот на процесот на регистрирање, и анализата на хардверот може да биде релевантна доколку се знае дека осомниченото лице користело одредена хардвер конфигурација. * Анализа на функцијата на компјутерскиот систем. Додатно на хардверот, компјутерскиот софтвер игра важна улога во работењето на компјутерскиот систем. Вештите лица, на пример, можат да ги одредат функциите на компјутерскиот вирус или на друг вид на малициозен софтвер. Тие исто така можат да ги реконструираат оперативните процеси на софтверот. Анализата на софтверот може исто така да е важно и за одредување дали производството или продажбата на софтверот што се може да се користи за легитимни исто како и за недозволени цели (двојна употреба) е криминализирано. * Анализа на инсталиран софтвер во компјутерскиот систем. Анализата на софтверот инсталиран во компјутерскиот систем може да им даде на истражителите информации значајни за натамошниот тек на истрагата. Ова е особено случај кај софтверот за енкрипција и алатките што се користат за безбедно бришење на датотеки. Доколку во компјутерот на осомниченото лице има инсталирано таков софтвер, тогаш натамошната истрага може конкретно да фокусира на тие прашања. * Идентификација на релевантни дигитални информации. Компјутерските податоци може да се чуваат во различни видови уреди за складирање. Дури и на самиот тврд диск постојат многу можности за зачувување на датотека. Затоа, идентификувањето на локацијата каде релевантните докази се чуваат претставува голем предизвик. Еден нов тренд што претставува додатен предизвик во идентификувањето на релевантни информации е се пораспространетата употреба на складирање на далечина. Како што се нагласува погоре, широкопојасниот пристап и серверите за чување на далечина влијаат врз начинот на кои што се чуваат информациите. Со користење на ваквиот вид чување, осомниченото лице може да го попречи запленувањето на компјутерскиот хардвер на осомниченото лице што им овозможува на органите на законот да пристапат до информациите што се чуваат на уреди за далечинско складирање. Форензичката анализа во овој случај може да се користи за проверка/потврда дали осомниченото лице користело сервиси за далечинско складирање. Идентификацијата на релевантни дигитални информации не е само врзано со датотеките. Базите на податоци на софтвер алатките што осомниченото лице ги користи за наоѓање информации на неговиот компјутер може исто така да содржат релевантни информации. Дури и времените датотеки што ги генерира системот можат да користат докази за кривичната постапка. * Идентификација на скриени датотеки. Сторителите на криминал може да користат и техники за криење датотеки во уредите за складирање, со цел да ги попречат органите на законот да ја анализираат содржината на таа датотека. Тоа е особено релевантно во истраги поврзани со нелегална/недозволена содржина. Со форензичката истрага може да се идентификуваат скриените датотеки и истите да станат достапни преку анализата. * Повторно оспособување на избришани датотеки. Доколку лицата користат алатки со кои се обезбедува безбедно бришење, повторното враќање на тие информации обично не е можно. Но во случаи кога сторителите не се запознаети со такви алатки, бришењето на дигиталните информации не мора да значи дека тие се недостапни за органите на законот, бидејќи тие можат да бидат повторно оспособени со користење на специјални форензички софтвер алатки за дешифрирање на шифрирани датотеки и сегменти, и за повторно оспособување на лозинки. * Дешифрирање на шифрирани датотеки и сегменти, и повторно оспособување на лозинки. Криминалците се повеќе користат технологии за енкрипција. Оваа технологија предизвикува огромни предизвици за органите на законот, бидејќи тие не се во можност да пристапат и да ги испитаат шифрираните информации. Со форензичка анализа, можно е да се преземат мерки а дешифрирање на податоците и уредите за чување податоци. Исто така, вештите лица ги поддржуваат органите на законот во изготвувањето на стратегии за пристапување до шифрирани датотеки – на пример, со користење на одгатнувач (*key-logger)*. * Сторителите не само што можат да го попречат пристапот до одредени информации со енкрипција, тие користат и систем за заштита на лозинки. Со форензичката анализа може повторно да се оспособат лозинките, и на тој начин органите на законот можат да влезат во системите за заштита на лозинки. * Анализа на датотеки. Датотеките што се чуваат на уред за складирање податоци може да се анализираат на повеќе начини. На пример, форензичката анализа може да се усредоточи на содржината на датотеките. Додатно на рачното испитување на сомнителни датотеки, форензичката истрага може да вклучи и автоматски пребарувања со клучни зборови за датотеки со текст и алатки кои автоматски пребаруваат познати слики на компјутерот на осомниченото лице. * Како што беше нагласено погоре, компјутерските податоци можат доста лесно да се манипулираат. Форензичките испитувања можат да ги докажат измените направени на податоците и фалсификувањето на дигитални документи. * Исто така, истрагите можат да ги земаат предвид и мета-податоците. Овие видови анализи можат да го одредат времето кога документот последен пат бил отворен или модифициран. Исто така, анализата на мета-податоци може да се користи за идентификација на авторот на датотеката со заканувачка порака или серискиот број на камерата што се користела за фотографирање на слики со детска порнографија * Анализа на авторство. Доколку на блоговите и форумите на интернет се постираат заканувачки текстови или говори на омраза, анализата на датотеките/записите за евиденција нема да не доведат авторот на текстот доколку лицето користи интернет кафе или анонимни комуникациски услуги. Но, со софистицирана лингвистичка анализа може да се утврди дали осомниченото лице ги напишал написите пред тоа, и дали оставил информации што можат да помогнат во неговата идентификацијата. * Одржување на интегритетот на податоците. Како што беше и претходно истакнато, заштитата на интегритетот на дигиталните докази е клучно за нивното прифаќање на судот. Вештите лица го обезбедуваат интегритетот на податоците во текот на собирањето на доказите. Тоа на органите на законот во одредени случаи им овозможува да не пристапуваат кон заплена на хардвер, а наместо тоа да копираат релевантни датотеки, заштитувајќи го нивниот интегритет од какви било измени/промени во текот на истражниот процес. Тоа особено се однесува на создавање на слики во уреди за складирање. * Следење на ИП. Сторителите што користат интернет за извршување на кривично дело (на пример, преземање на слики со детска порнографија или напад на компјутерски системи) оставаат траги. Анализата на преносните податоците, како на пример записите за евиденција што се чуваат на интернет серверите, може да ги доведе истражителите до врската што сторителот ја користел за да се логира на интернет. Таквата истрага може да е сложена ако сторителите користеле технологија за анонимна комуникација. Но дури и во такви случаи, истрагата не е невозможна. Еден таков пример е форензичката алатка CIPAV (Проверувач на компјутерски и интернет протокол адреси) која што била користена во САД за идентификување на осомничено лице кое користело анонимни комуникациски услуги. * Анализа на е-пошта. Е-поштата е многу популарен начин за комуникација и затоа има многу голема улога во компјутерската форензика. Со оглед на тоа дека е доста лесно да се идентификува испраќачот на е-пошта со заканувачки пораки или со прилог од недозволена содржина, сторителите честопати користат бесплатни е-пошта адреси отворени со лажни информации. Но дури и во такви случаи, испитувањето на информациите од заглавијата и записите за евиденција на е-меил провајдерот може да доведе во одредени случаи до идентификација на осомниченото лице. * Следење на финансиски трансакции. Одреден број кривични дела, меѓу кои и продажбата на детска порнографија, претпоставуваат финансиски трансакции. Податоците од комерцијалните системи и институциите вклучени во финансиските трансакции може да се искористат за идентификување на сторителот. Пример за тоа е и една истрага во Германија, каде што сторители што преземале детска порнографија од еден комерцијален веб сајт биле идентификувани преку нивните кредитни картички. Компанијата што ги издала овие картички направила анализа на плаќањата на клиентите, и идентификувала одредени клиенти кои ги користеле кредитните картички за купување детска порнографија онлајн. Но, ваквите истраги стануваат се по тешки, со оглед на тоа дека сторителите користат методи на анонимно плаќање. * Прибирање преносни податоци во реално време и престретнување содржина. Форензичките истраги може да вклучат и следење процеси на пренос на податоци во реално време. Проектот на Советот на Европа за компјутерски криминал [www.coe.int/cybercrime](http://www.coe.int/cybercrime) им овозможува на истражителите да реагираат на процесите истовремено кога лицето под истрага дејствува. * Следење на активности на јавно достапни сервиси. Јавно достапните сервиси може да се користат за размена на материјали заштитени со авторски права, или на материјали со недозволена содржина. Вештите лица можат да ги следат ваквите сервиси во текот на одредена истрага. Пример за тоа е следењето на форумите за разговор/чет. * Далечинска форензика. Моментно се водат дискусии за потребата од далечински форензички алатки кои би овозможиле собирање живи податоци од далечина и далечинско следење, без осомниченото лице да знае дека неговиот систем е под истрага. * Вршењето на вакви истраги бара конкретна обука и добро дефинирани процедури втемелени врз широко прифатени стандарди и методологии.   **Како се врши форензичко испитување**  Има два начина на кои што може да се врши форензичкото испитување:   * Рачни операции. И покрај тоа што постои технологијата за автоматизирање на истражниот процес, во компјутерската форензика во најголем дел работата се уште се врши рачно. Ваквите рачни операции можат да се проследени со тешкотии. особено во истрагите каде што има големо количество податоци. * Алатки за анализа. Некои процеси – особено пребарувањата со клучни зборови, реконструкцијата на избришани датотеки или дешифрирањето на шифриран материјал – можат да се автоматизираат со софистицирани алатки за форензичка анализа.   Во повеќето истраги има комбинација од рачни операции и користење на форензички софтвер алатки што ги автоматизираат процесите.   * Изготвување /Изведување на докази во суд. Вообичаено, вештите лица не ги изведуваат доказите на суд. Но, тие можат да имаат важна улога во кривичната постапка. Вештите лица може да бидат стручни сведоци што им помагаат на лицата вклучени во судската постапка да ги разберат процесите врз основа се создаваат докази и процедурите што се користат за нивно прибирање и оценување, | | | |
| **52 – 59** | | | **Дел 3 – Правни прашања** | | | |
|  | | | **Посебни прашања поврзани со дигитални докази**  Современите форми на криминал на мрежи, против мрежи или во рамките на мрежите наметнуваат потреба за поддршка од страна на стручни и специјализирани лица за собирање и анализирање на докази и за нивно точно толкување на суд.  Тоа, се разбира, не е ништо ново: веќе со векови, стручните лица им помагаат на судиите, обвинителите и адвокатите да ги разберат техничките прашања. На пример, со векови веќе, докторите се од клучна важност во утврдувањето, разјаснувањето и судското оценување на медицинските аспекти на можните случи на убиство. Но ново е тоа што дигиталната средина носи нови и тешки прашања, кои се уште тешко се разрешуваат.  Всушност, постојаниот технички развој не секогаш е проследен со континуиран преглед и ажурирање на правните инструменти, и не секогаш процесните правни алатки ги легитимираат техниките за прибирање електронски докази.  Од друга страна, почетните и континуираните обуки за органите на законот, обвинителите и судиите не се секогаш во тек со најновите технички иновации.  Под едно вакво сценарио, имаме состојба на зголемен број на нови кривични прекршоци, за чие што разбирање е потребно специјализирано знаење. Техничка стручност е потребна не само за докажување на кривичното дело; таа е потребна за да се разбере точно за каков вид криминал станува збор. Сите ние разбираме што е „убиство“, и медицинските стручњаци се потребни само за да ја утврдат причината за смрт. Од друга страна пак, ускратувањето на услуги, е кривично дело кое се дефинира со одредено техничко знаење за компјутерските мрежи.  Повеќето земји во светот немаат посебна регулатива за електронски докази. Некои имаат посебни правила за одреден аспект, на пример за пресретнување на комуникации. Но општо земено, правните системи го регулираат собирањето електронски докази според претходно постоечки правила кои се однесуваат на светот офлајн. Во некои случаи, судовите ја прифаќаат новата реалност поврзана со доказите, и се прилагодуваат на правилата, но некогаш не. Во вториот случај, мора да се додадат нови одредби на постојната правна рамка.  Во многу европски земји се уште нема законодавство за електронски докази, ниту пак критериуми што судовите треба да ги користат при разгледување и оценувањето на електронските докази.  Прибирањето и оценувањето на електронските докази е деликатна активност, бидејќи задира во основните права, како што е приватноста или доверливоста/тајноста на телекомуникациите. Понекогаш, на судиите не им е јасно дали тие права се почитуваат.  Компјутерскиот криминал е глобален. Фактите поврзани со делото може истовремено да се случуваат во повеќе земји и јуриздикции. По својата природа, компјутерскиот криминал е транснационален. Кривичните дела извршени во информатички и комуникациски мрежи предизвикуваат сериозни проблеми за разјаснување каде се случило кривично дело, а со тоа и соодветните органи на законот што треба да го водат случајот.  Конвенцијата од Будимпешта за борба против компјутерскиот криминал не може да ги разреши сите проблеми поврзани со оваа проблематика, но прави обид да најде решенија за одредени тешки ситуации.  Страните на Конвенцијата, како и во други случаи, ќе ги истражуваат кривичните дела извршени на нејзина територија. Но, Конвенцијата додатно вели дека Страните треба да се прогласат за компетенти за гонење и судење на предмети каде што граѓаните на таа држава вршат кривично дело надвор од нејзините граници, под услов таквото дело да е исто така казниво согласно законите во местото каде што таквите активности се случиле.  Ова е важно практично прашање. Иако некои земји имаат одредби за дефинирање на универзална јурисдикција, тоа не е општо и универзално прифатен принцип.  Но, во многу ситуации е тешко да се разграничи кој суд има јурисдикција согласно општите правила. На пример, едно компјутерско кривично дело може сосема лесно да се изврши во исто време во неколку земји, врз неколку жртви, или може да биде извршено од различни лица, од различни локации.  Со оглед дека нема целосна усогласеност на кривичните јуриздикции меѓу земји во светот, може да се јави ситуација каде што два суда, од две различни земји бараат јурисдикција врз едно дело, и покрај општите правила од Конвенцијата за компјутерски криминал.  На ниво на Европската унија беше издадена важна Директива исклучиво за собирање дигитални докази: Директивата 2006/24/EC, на Европскиот парламент и на Советот на Европскиот Парламент и на Советот о 15 март, 2006 година е првиот задолжителен документ во Европската Унија за задржување на генерирани и обработени податоци во врска со одредбата на јавно достапни сервиси за електронски комуникации или за комуникациски мрежи од јавен карактер. | | | |
|  | | | **Практични вежби** (доколку се предвидени)  За оваа сесија не се предвидени практични вежби, бидејќи нема гаранции дека нивото на технологијата и пристапот до интернет на сите места каде што ќе се одржува оваа обука ќе биде на потребното ниво.  В иднина, обучувачите можат да ја дополнат обуката со додавање на вежби, во услови каде што одржувањето на обуката го дозволува тоа. | | | |
|  | | | **Проверка на знаењето**  За оваа сесија нема конкретна проверка на знаењето додатно на ова наведено погоре, а што се предвидува за целата обука. Нема барање за формално оценување. | | | |
| 63 - 64 | | | **Преглед / Резиме**  Обучувачот треба да го резимира/тестира стекнатото знаење за да осигури дека е доволно за исполнување на следните задачи:  Дискусија за следните видови докази:   * Објасни ги принципите на најдобрите практики во врска со заплената и работењето со електронски докази * Идентификувај ги предизвиците на следните извори на електронски докази: „статични “, „живи податоци” и интернет * Идентификувај ги предизвиците при добивање докази од други јруиздикции * Дискутирај ги прашањата за прифатливост на електронските докази во судските постапки, во однос на веродостојноста, точноста и целовитоста   Ова може да се постигне со групна дискусија, прашања поставени до учесниците, квизови или други видови признати методи.  Оваа лекција има за цел да даде упатства во однос на видовите и нивото на знаење за електронски докази што им е потребна на судиите и обвинителите за делотворно исполнување на нивните улоги. Не претендира да биде целосна анализа на прашањата, и каде тоа е соодветно, укажува каде можат да се добијат додатни информации.  Се препорачува изготвувачите на обуката да обезбедат материјали ажурирани со најнови податоци и аспекти кој влијаат врз криминалното однесување; влијанието врз правните, процесните и доказните правила во јурисдикцијата каде што се одржува обуката. Има промени во технологијата кои ќе влијаат врз системот на кривичното право, како на пример, складирањето во полупроводници и Web 2.0. Тоа се важни прашања што треба да се вклучат во програмите за обука, со оглед на нивното се пораширено присуство. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Сесија 1.3.4 Меѓународна соработка | | | **Времетраење: 90 Минути** | |
| **Потребни ресурси**   * Преносен компјутер или персонален компјутер со *Windows 7* *и Office 2010* * Проектор * PowerPoint презентација | | | | |
| **Цел:**  Целта на оваа сесија е да потсети на важноста на меѓународната соработка и да даде преглед на расположливите инструменти за меѓународна соработка во полето на компјутерскиот криминал, а особено Конвенцијата од Будимпешта против компјутерски криминал. Тоа е вовед во расположливите инструменти, начините на кои тие се користат, нивната навременост и делотворност. | | | | |
| **Задачи**  На крајот на оваа сесија, учесниците ќе бидат во можност да :   * Ја препознаат глобалната димензија на интернетот и меѓународната димензија на компјутерскиот криминал * Ја објаснат важноста од меѓународна соработка и ги препознаат расположливите инструменти за меѓународна соработка во полето на компјутерскиот криминал * Ја идентификуваат потребата од брзи и ефикасни канали за меѓународна соработка и расположливи инструменти, начините како се користат, навременоста и делотворноста * Ги опишат напорите на меѓународните организации во врска со спроведувањето на модалитетите на меѓународната соработка * Дискутираат за Конвенцијата од Будимпешта против компјутерскиот криминал – идентификување на општите принципи, времените мерки и мрежата за взаемна правна помош која функционира 24 часа, седум дена во неделата. | | | | |
| **Слајд бр.** | **Содржина:** | | | |
|  | **Вовед**  Во оваа сесија ќе се нагласи важноста на меѓународната соработка во истрагата на конкретни случаи на компјутерски криминал. Подетално ќе се разгледаат инструментите на меѓународната соработка, пред се Конвенцијата од Будимпешта против Компјутерски криминал. | | | |
| **2** | 1. Дел 1 на презентацијата ќе се фокусира на меѓународната димензија на компјутерскиот криминал. Со оглед дека оваа тема е веќе обработена во други сесии, приод ќе биде доста кус. 2. Во Дел 2 ќе се наведат одредени одговори на компјутерскиот криминал на меѓународно ниво. 3. Во Дел 3, во врска со меѓународниот одговор за компјутерскиот криминал, ќе се нагласи улогата на Конвенцијата од Будимпешта против компјутерски криминал. 4. На крај, Дел 4 ќе се фокусира на алатките за меѓународна соработка наведени во Конвенцијата од Будимпешта. 5. Дел 5 ќе направи преглед на главните теми на презентацијата. | | | |
| **3** | **Задачи на сесија**  Целта на оваа сесија, е воопштено да се согледа глобалната димензија на интернетот и меѓународната и транснационалната димензија на компјутерскиот криминал.  Да се објасни важноста од меѓународната соработка и инструментите за меѓународна соработка во полето на компјутерскиот криминал.  Додатно на инструментите достапни за меѓународна соработка, да се идентификува потребата од брзи и ефикасни канали за ваквиот вид соработка.  Да се направи преглед на напорите на меѓународните организации за спроведување на новите модалитети на меѓународна соработка.  Особено, да се разгледа Конвенцијата од Будимпешта против компјутерскиот криминал – со идентификување на општите начела, времените мерки и мрежата 24/7 на итна меѓународна соработка. | | | |
| **4** | **Дел 1 – Меѓународната димензија на компјутерскиот криминал**  Ќе се направи многу кус преглед на меѓународната димензија на компјутерскиот криминал. | | | |
| **5** | Очигледен факт е дека интернетот доживува глобална експанзија и дека пристапот до него е достапен и го користат скоро сите на планетата.  Во рамки на мрежите, криминалот се зголемува. Следствено, на компјутерскиот криминал мора да му се пристапи како на глобален феномен. Целосната реалност на компјутерскиот криминал не може да се разбере без признавањето на меѓународната димензија. | | | |
| **6** | Во тој контекст, компјутерскиот криминал е најтранснационален вид криминал. Лицата кои сакаат да го истражуваат компјутерскиот криминал мора да бидат свесни дека оваа задача бара ефикасна меѓународна соработка. Всушност, со оглед на неговата глобална природа, борбата против компјутерскиот криминал без ваквата соработка не да биде успешна. | | | |
| **7** | Во конкретни рамки, кога едно кривично дело се врши во компјутерскиот простор, органите на кривичното право се соочуваат со многу тешки прашања што ќе треба претходно да се решат, пред да се преземе што било друго.  Со оглед на тоа дека интернетот е насекаде, не е секогаш лесно да се одреди правно релевантната локација на кривичното дело. На пример, ако сторителот дејствува на местото А и го таргетира компјутерот на жртвата во местото Б, а противправната комуникација што ја користи криминалецот се врши со провајдер од местото Ц, и ако сите тие локации се под различна јурисдикција, првото прашање што органите на законот мора да го решат, е ја одредат правно релевантната локација на кривичното дело. Ако, на пример, сторителот делува на местото А и таргетирана жртва е на местото Б, но противправната комуникација што ја користел криминалецот се вршела преку провајдер лоциран на локација Ц, и ако сите овие локации потпаѓаат под различни јуриздикции, првото прашање што службениот орган мора да го реши е правно релевантната локација на кривичното во однос на јурисдикцијата. Мора да биде јасно кое е местото каде е извршено кривичното дело, за да се одреди кое материјално право може да се примени и која е надлежната јурисдикција (полиција, обвинител, судија).  Истражителот мора да ја почитува сопствената јурисдикција –територијална надлежност. Согласно оваа гледна точка, таа е ограничувачката рамка за кривичните истраги.  Во реалноста, се јавуваат два вида неразрешени прашања.   * Првото се однесува на преку граничните истраги: како еден службен орган може законски да истражува надвор од неговата земја, доколку се јави потреба од итно дејствување? Како може тој да добие и собере докази „од соседството“ т.е. од друга земја, доколку смета дека доказите можат брзо да исчезнат? * Второто прашање се однесува на истрагите во „облак“. Никој не знае каде (физички) одредени податоци можат да се чуваат. Тие наводно се чуваат во „облак“. Можно е никој да не знае која е националната јруиздикција за некој податоци во „облак“. Како може едно службено лице да добие и собере податоци што се чуваат во „облак“, без оглед каде и да се наоѓа физичката локација каде што се чуваат. | | | |
| **9 - 10** | **Дел 2 – Меѓународен одговор на компјутерскиот криминал**  Со оглед на глобалната експанзија на интернетот и тоа дека потенцијално го користат сите луѓе на планетата, на компјутерскиот криминал мора да му се пристапи како на глобален феномен. Целта на Дел 2 е да се опишат некои од најважните практични чекори што се преземаат како одговор на компјутерскиот криминал во Европа. | | | |
| **11 - 13** | Интерпол е добро позната меѓународна организација, чие што членство го сочинуваат органи на законот од целиот свет. Со јануари, 2012 година, Интерпол има 190 членови од сите континенти. Задачата на Интерпол е да ја зајакнува и овозможува меѓународната полициска соработка. За таа цел, Интерпол има организирано глобален полициско-комуникациски систем и развиено конкретни бази на податоци и анализи на полициски информации.  Интерпол е меѓу првите меѓународни институции кои почнаа да покажуваат загриженост за прашањата поврзани со компјутерскиот криминал, и меѓу првите да организираат групи за дискусија на експерти на оваа тема во 1995 година. Од тогаш, Интерпол ги развива напорите со кои на полицијата и на други органи на законот низ целиот свет им се помага да ги зајакнат способноста за борба против Компјутерскиот криминал.  За постигнување на таа цел, Интерпол изгради мрежа од лица за контакт (Национални централни референтни точки - NCRP), со која на членките им се нуди постојана поддршка. Во септември, 2011 година, мрежата имаше околу 120 референтни лица низ целиот свет. Овие референтни лица го усвоија аранжманот на лицата за контакт 24/7, согласно Член 35 на Конвенцијата од Будимпешта против компјутерскиот криминал. Во некои држави Страни на Конвенцијата, референтните контакт лица се назначени и како контакт лица во Г8. Сите контакт лица од Г8 се вклучени во оваа мрежа. Целта на оваа структура е да им овозможи на полицијата веднаш да можат да идентификуваат експерти во други земји и веднаш да добијат помош за истраги поврзани со компјутерски криминал и прибирање докази. Оваа мрежа е на располагање 24 саати на ден, седум дена во неделата.  Опфатот на работата на мрежата на националните централни референти лица е да овозможи размена на полициски и разузнавачки информации помеѓу незините членки, како и да овозможи техничка и оперативна поддршка. Всушност, главната цел на Мрежата е да осигури дека типичните полициски информации се разменуваат што е побрзо можно, преку конкретни и соодветни канали на Интерпол; тоа подразбира информации за осомничени терористи, лица по кои се има издадено потерница, отпечатоци од прсти, профили на ДНК, изгубени или украдени патни документи, украдени возила, украдени уметнички дела, и сл. Овој вид на потенцијално важни информации што ги обезбедува Интерпол е секако многу корисно при конкретни истраги. Но, точно поради опфатот на мрежата, таа не може да се користи за итно барање за зачувување на компјутерски податоци, на пример, или пак за зачувување на преносни податоци, или какво била мерка за добивање или зачувување на докази. Со други зборови, соработката што може да се оствари преку оваа конкретна мрежа на Интернет се базира врз истите принципи што се однесуваат и на општата соработка во рамките на Интерпол. | | | |
| **14** | Европската Унија е поддржувач на Конвенцијата од Будимпешта, учествувајќи дури и во нејзината изработка. Од тогаш наваму, Европската Унија ги охрабрува сите држави членки да ја ратификуваат Конвенцијата. Всушност, голем број држави членки на ЕУ веќе ја имаат ратификувано, а сите ја имаат потпишано.  Се разбира, во рамки на Европската Унија има широка низа на алатки за меѓународна соработка, додатно на најновите пристапи, базирани врз принципот на взаемно признавање. Најголемите предности на европскиот систем се темелат врз можноста за директни контакти помеѓу судските власти од државите членки. Со ваквата можност, секој судија или обвинител може директно да поднесе барање до друг судија или обвинител. Ова е многу моќна алатка во однос на истрагите, а може да се применува и во случаи на компјутерски криминал. | | | |
| **15** | Исто така, во 2005 година Европската Унија усвои задолжителен инструмент, со кој меѓу другото се регулира и мрежата на контакт лица 24/7 за истраги на компјутерски криминал. Тоа е Рамковната одлука на Советот 2005/222/JHA од 24 февруари, 2005 година, за напади врз информатички системи. Во оваа Рамковна одлука се даваат правилата во врска со „постојната мрежа на контакт лица“. Во Член 11, 1, се вели дека сите држави членки на Европската Унија треба да го обезбедат користењето на постојната мрежа на оперативни контакт лица која е достапна 24 часа на ден, седум дена во неделата. Оваа одредба се однесува на одреден број дела (противправниот пристап до информатички системи, противправниот напад на систем, противправното манипулирање на податоци, и поттикнувањето и помагањето и обид).  Во членовите на рамковната одлука тоа не се споменува, но јасно е дека *постојната мрежа*  е мрежата на Г8/Советот на Европа. | | | |
| **16** | Европол е автономна организација на Европската Унија чија што цел е да ја подобри делотворноста на соработката помеѓу органите на законот.  на државите членки на Европска Унија. Од 1999 година, активностите на оваа организација вклучува и овозможување на анализи на информации поврзани со кривични дела, и споделување податоци помеѓу државите членки. Меѓу другите можности, Европол може да послужи како одличен канал за зголемување на ефикасноста согласно Член 26 на Конвенцијата од Будимпешта, во врска со спонтани информации.  Во јануари, 2013 година, во Европол се формираше Европски центар за компјутерски криминал (EC3). | | | |
| **17** | Никој не знае како Евроџаст ќе се развива в иднина, но во моментот тоа е веќе важна агенција на Европска Унија, посветена на судската соработка (на ниво на обвинители и судии) меѓу државите членки на Европската Унија. Опфатот на работата на Евроџаст е меѓународната соработка за борба против каков било вид значаен криминал, преку координација на активностите што ги преземаат националните власти одговорни за гонење.  Во тој контекст, Евроџаст има надлежност да ја промовира координацијата помеѓу надлежните власти од државите членки и да го овозможи спроведувањето на барањата за меѓународна взаемна правна помош и барањата за екстрадиција.  Евроџаст е формиран како правно лице во декември, 2000 година, по препораката од состанокот на Европскиот совет во Темпере, и во него има по еден претставник од секоја од 27-те држави членки. „Компјутерскиот криминал“ е една од областите под надлежност на Евроџаст. | | | |
| **18** | И повторно, со цел да унапреди борбата против организираниот криминал и тероризмот во Европската Унија преку зголемување и поедноставување на соработката помеѓу судските власти, во јуни 1998 година во Европската Унија е формирана Европската судска мрежа за кривични предмети  Во основа, тоа е мрежа на судски лица за контакт што ги вклучува централните власти во секоја држава членка одговорна за судска соработка, подразбира национални лица за контакт во секоја држава членка и во крајна инстанца, мировни судии за врска.  Една од задачите на Европската судска мрежа за кривична материја е да обезбедува информации, кои им се достапни на судиите, со што се олеснува меѓународната соработка помеѓу разните судски организации и правни системи. Во тој контекст, Европската судска мрежа го изготви *Атлас*, компјутерска алатка што на практичарите им овозможува лесно да ги идентификуваат надлежните власти во државите членки кои добиваат и ги извршуваат барањата за взаемна правна помош.  Со оваа мрежа се обезбедуваат лица за контакт кои им стојат на располагање на судските власти во земјата, кои можат да ги контактираат заради овозможување на судска соработка помеѓу државите членки и кои им служат како поддршка на овие власти при подготовката на барања за судска соработка.  Овој вид мрежа, со која што се овозможува брзо и лесно поднесување на барања за преку гранична соработка, може да биде многу значајна за собирање на електронски докази. | | | |
| **19** | Европската Конвенција за взаемна помош за кривична материја на Советот на Европа од 1959 година, е очигледно основата за Конвенцијата од Будимпешта против компјутерскиот криминал. Всушност, Конвенцијата од Будимпешта и нема за цел да ги покрие сите прашања поврзани со меѓународната соработка; конвенцијата се однесува само на новите и претходно непостојни или побрзи канали и модалитети за соработка.  Сите држави членки на Советот на Европа (со исклучок на Сан Марино) ја имаат ратификувано Конвенцијата, што значи дека од сите страни на Конвенцијата од Будимпешта,единствената држава што не е членка на СЕ, а е страна на Конвенцијата од 1959 година е САД.  Овој факт само и додава вредност на Конвенцијата од Будимпешта за создавања, по прв пат, за заедничка правна рамка за меѓународна полициска и судска соработка помеѓу повеќето европски држави и САД. Ова е посебно важен аспект бидејќи во Член 14, 2 се вели дека процедурите за меѓународна соработка согласно Конвенцијата се применуваат кај кривични дела утврдени согласно Членовите 2 – 11 на Конвенцијата, како и кај кривични дела извршени преку компјутерски систем, и за собирање докази во електронска форма за кое било друго кривично дело. | | | |
| **21** | **Дел 3 – Меѓународен одговор на компјутерскиот криминал: Конвенцијата од Будимпешта за борба против компјутерскиот криминал** | | | |
| **22 – 25** | Како што веќе беше споменато во другите сесии, Конвенцијата од Будимпешта е отворена за потпишување на 23 ноември, 2001 година и стапи на сила во јули, 2004 година. До април 2013 година, 57 држави станаа или страни, потписници, или се поканети да пристапат кон Конвенцијата.  Во конкретни случаи на истрага на материја поврзана со компјутерскиот криминал, Страните на Конвенцијата добиваат можност да користат нови и многу иновативни алатка за истрага, главно во случаи кога се бара меѓународна соработка. Овие нови можност можат да се користат кога кривичното дело што се истражува е едно од делата опишани во Конвенцијата, но исто така и во други случаи, кога кривичното дело е извршено со компјутерски систем или кога доказите за кривичното дело се снимени или се чуваат на дигитални уреди. Тоа е наведено во Член 14 на Конвенцијата.  Ова е за прв пат меѓународната заедница да вложи заеднички напори за постигнување согласност за универзален договор за материја поврзана со компјутерскиот криминал и електронските докази, со надеж дека на крај, повеќето држави ќе застанат зад нејзината цел. Денес, таа останува прв и единствен обврзен меѓународен инструмент за борба против компјутерскиот криминал.  Секоја земја што ќе ја ратификува и ќе стане Страна на Конвенцијата во тој процес се стекнува со пристап до многу релевантниот универзален *форум* за соработка на полициските сили и на судските органи.  Конвенцијата воведува нови канали за меѓународна соработка. Некој од нејзините одредби се многу иновативни и исклучително, но може да се сметаат за соодветни и потребни одговори за новата реалност на компјутерски криминал.  Но и покрај тоа, Конвенцијата против компјутерскиот криминал не се стреми кон тоа да биде единствениот обврзен меѓународен инструмент за меѓународна соработка. Во Член 23 на Конвенцијата се вели дека таа ќе се применува во рамките на други постојни релевантни инструменти за меѓународна соработка за кривична материја. Следствено, Член 27 ги наведува општите принципи кои треба да се следат во отсуство на применливи меѓународни конвенции или договори.  Од друга страна, мора да се истакне дека правилата воведени со членовите на Конвенцијата создаваат нови алатки и канали за соработка помеѓу страните што не беа можни со кој било друг претходен инструмент. | | | |
| **27** | **Дел 4 - Конвенцијата од Будимпешта- алатки за меѓународна соработка**  Правилата на Конвенцијата во врска со меѓународната соработка се дадени во третото поглавје на Конвенцијата. Повеќето правила во ова поглавје се оперативни и процесните правила кои ги има и во други меѓународни конвенции. Но, има и такви кои се многу иновативни и треба да се разгледаат подетално. | | | |
| **28 - 29** | Во Член 26 се наведува ситуација кога властите на една Страна во текот на одредена истрага на национално ново откриваат информации што смета дека треба да се испратат до властите на друга Страна, но без за тоа да има барање од таа држава. Тоа се случува во ситуации кои информациите се сметаат за корисни или потребни за започнување на истрага за кривично дело опишано во рамките на Конвенцијата. За разлика од порано, кога взаемната помош обично била пасивна, при што државата А бара помош од државата Б, Конвенцијата поттикнува на еден повеќе проактивен пристап. Но, согласно Член 26 точка 2, ваквото „спонтано“ давање информации може да подлежи на некои услови, како на пример, барање за доверливост или користење податоци за специфични цели. | | | |
| **30 - 32** | Членот 29 е една од најважните одредби на Конвенцијата од Будимпешта. Во Член 29 се дефинираат правилата во врска со експедитивното зачувување на податоци што се чуваат компјутерски систем. Се воведува рамка паралелна на националните одредби во врска со експедитивната заштита на податоци. Главно, оваа одредба и овозможува на една Страна на Конвенцијата да побара на заштита на податоци од друга Страна, доколку во исто време таа изрази намера за пристапување кон формално барање за помош за претрес, заплена или слична мерка.  Во таков случај, замолената страна мора да дејствува согласно потребите, и со сите потребни мерки треба да ги зачува побараните податоци, согласно националното законодавство на таа држава. Како што веќе се нагласи, ова е нова алатка на меѓународна соработка, која е резултат на специфичноста на дигиталната средна. Преку-граничната соработка бара многу време. Итниот карактер на мерката е потребен поради потребата да се зачува нешто што може за многу кратко време целосно да се избрише.  Важно е да се истакне дека ова е само мерка за зачувување, од итни причини, и не значи автоматско откривање на заштитените податоци. Всушност, за случаите каде што е дозволено откривањето на податоци постојат точно одредени правила согласно кои тоа се врши, а пред се доколку не се работи само за податоци за извршен сообраќај.  Во практични рамки, тоа значи дека може да се изврши итно заштитување на податоци, но дека подоцна може да се утврди дека има причини заради кои податоците нема да се обелоденат на страната што го бара тоа.  Важно е да се има предвид дека двојната инкриминираност не е услов за земјата подносител да поднесе барање за зачувување на податоци. | | | |
| **33 - 34** | Откривањето на преносни податоци се обработува во Член 30 на Конвенцијата од Будимпешта. Во врска со тоа, Конвенцијата пропишува лесен модел за меѓународната соработка. Нема конкретни правила за итно откривање, исто како што нема такви правила и на национално ниво, во поглавјето со процесните одредби. Без тоа експлицитно да го каже, Конвенцијата ги усогласува националните правила за итна зачувување на докази и откривањето со тие на меѓународната соработка. | | | |
| **35 - 36** | Во Член 31 на Конвенцијата се дефинира општото правило за взаемна помош во врска со пристапувањето до зачувани компјутерски податоци. Во овој Член, и во Член 23 на кој што се однесува, се изразува општо залагање на страните за соработка во гонењето на компјутерскиот криминал во „најширока можна смисла“, но не се утврдуваат нови обврски при соработката. Сета соработка подлежи на постојните договори и меѓународни инструменти со кои што се регулира преку- граничната соработка за традиционални/конвенционални истраги.  Практично, тоа значи дека Член 31 ја доближува компјутерската средина до општите правила кои веќе со години важат за реалниот простор. | | | |
| **37 - 38** | Со Член 32 се дефинира можноста што на органите за законот на Страната на Конвенцијата им се дава за добивање на докази што физички се чуваат во компјутер што се наоѓа на територијата на друга Страна, без барање за меѓународна соработка. Ова може да се направи во случај кога во текот на некоја конкретна истрага на надлежните лица им требаат информации од отворен извор што се наоѓаат во компјутер во друга земја, или од компјутер чиј што пристап е овластен од законски овластено лице.  Во врска со информациите од отворен извор, мора да се напомене дека истрагите од „отворен извор“ се нешто што во повеќето земји сите граѓани можат да го прават по сопствена иницијатива. Оваа одредба едноставно има за цел да ги овласти претставниците на органите на законот да го тоа прават исто така, а воедно, тие докази да бидат валидни.  Од друга страна, оваа одредба има и многу нов пристап. Во реалниот свет нема вистински еквивалент на оваа можност: во минатото службеното лице требало физички да оди во друга земја и да побара помош од локалните власти. Тоа лице не можело да прави што било на сопствена рака, и секое истражно дејствие се сметало за дејствие направено во име на националните власти на местото на настанот.  Во Член 32 се вели токму обратното. Согласно овој Член, кој било претставник на органите на законот од некоја земја може да добие информации од која било друга земја на светот, дури и ако се работи за информации „не-отворен извор“, доколку лицето кое има законско овластување за откривање на тие податоци законски и доброволно се согласи на тоа. За ваквата истражна активност не е потребно какво било овластување од државата со јурисдикција во местото каде што информациите се чуваат. Некои држави не ја прифаќаат Конвенцијата поради оваа формулација и сметаат дека таа е спротивна на принципот на суверенитет. Но, не постои каков било друг предлог или решение за сложениот проблем на преку-граничните истраги или истрагите во „облак“. Реалниот живот кажува дека во повеќето случаи е невозможно да се истражува компјутерскиот криминал или да се прибираат електронски докази на меѓународно ниво преку традиционалните канали. Невозможно е затоа што времето што е потребно за тоа не соодветствува на нестабилната и кревка природа на електронските докази. Затоа поефикасно е граничните истраги да ги води претставник на органите на законот кој го работи случајот.  Понекогаш е навистина невозможно да се користат регуларните канали на соработка. Таков е примерот на услугите во „облак“, каде што корисниците (и истражителите) не знаат каде точно физички се чуваат податоците што им требаат на полиција. | | | |
| **39 - 40** | Член 33 се занимава со меѓународната соработка за пресретнување на комуникации. Не се работи за нова алатка за меѓународна соработка; и други меѓународни инструменти го имаат тоа. Но, Член 33 има посебен опфат: собирање на преносни податоци во реално време.  Од друга страна, најважното правило наведено во Член 33 се однесува на ограничувањата при примената на оваа истражна мерка. А, ограничувањата се условите и постапките дадени согласно домашното законодавство. Така што, овој модус на соработка државите ќе го применуваат во истите случаи како и при собирањето на преносни податоци во реално време за слични домашни предмети. | | | |
| **41 - 43** | Член 35 е една од најважните оперативни одредби на Конвенцијата. Со Член 35 на сите Страни на Конвенцијата им се наметнува обврска да воведат лице за контакт кое е постојано достапно (т.е. мрежа на контакт лица 24/7).  Општата цел на овие лица за контакт е да ја овозможуваат меѓународната соработка. Тоа го прават со давање технички совети на другите контакт лица, со активирање на соодветните механизми за итно зачувување на податоци, итно собирање докази или идентификација и откривање на осомничени лица.  Оваа оперативна мрежа на експерти за високо-технолошки криминал има за цел да им помага и на експерти од други земји или јуриздикции во кривичните истраги со меѓународна димензија. Таа служи за да справување со новите предизвици што го носи брзиот високо-технолошкиот криминал. Понекогаш, истражителите на компјутерскиот криминал имаат потреба од многу брзо заштитување на електронски податоци, со цел да се овозможи лоцирањето и гонењето на осомниченото лице. Оваа нова потреба не може да се задоволи преку кој било традиционален канал на меѓународна соработка. Тоа е додадената вредност на оваа мрежа: овозможува брза неформална помош и соработка, дури и ако потоа мора да биде проследена со барање за формална соработка | | | |
|  | **Практични вежби (доколку се предвидени)**  За оваа сесија не се подготвени практични вежби. | | | |
|  | **Проверка на знаењето**  Обучувачот треба да го провери знаењето преку поставување релевантни прашања за сите аспекти на сесијата. | | | |
| **45 - 46** | **Преглед / Резиме**  Обучувачот треба да направи преглед/ го тестира знаењето за следите точки:   * Согледување на глобалната димензија на интернетот меѓународната димензија на компјутерскиот криминал * Објаснување за важноста од меѓународна соработка и да се согледаат достапните инструменти за меѓународна соработка во полето на компјутерскиот криминал * Идентификација на потребата од брзи и ефикасни канали на меѓународна соработка и достапните инструменти, начините како се користат, временските рамки и делотворноста * Опис на напорите на меѓународните организации во врска со спроведувањето на модалитетите на меѓународната соработка * Дискусија за Конвенцијата од Будимпешта за борба против компјутерскиот криминал – идентификување на општите принципи, времените мерки и мрежата за взаемна правна помош која функционира 24 часа, седум дена во неделата | | | |
| Сесија 1.3.5 Затворање на обуката | | | | **Времетраење 90 Минути** |
| **Потребни ресурси**   * Персонален компјутер или преносен компјутер со Windows 7 и со MS Office 2010 * проектор * PowerPoint презентација * Формулари за евалуација | | | | |
| **Цел:**  Целта на оваа сесија е да им овозможи на учесниците да дадат повратни информации за обуката и да им помогнат на обучувачите да увидат како можат да ја подобрат обуката. Во оваа сесија, обучувачот треба да направи резиме на содржината на обуката, осврнувајќи се на целите и задачите. | | | | |
| **Задачи:**  На крајот на оваа сесија, учесниците ќе бидат во можност да:   * Дадат соодветни повратни информации за обуката и нејзината делотворност * Ги пополнат формуларите за оценување на обуката на СЕ * Го идентификуваат наредниот степен на обука што им е потребен за унапредување на нивното знаење и вештини за темата. | | | | |
| **Вовед**  Ова е важна сесија и треба да се искористи за добивање повратни информации од учесниците за содржина и методологијата користена за одржување на оваа обука. Во текот на оваа сесија треба да се пополнат и/или финализираат формуларите за евалуација. Обучувачот треба да направи преглед на сите сесии покриени со обуката и да провери дека се исполнети сите зададени задачи. По завршувањето на оваа сесија, обучувачот има задача да осигура дека сите повратни информации се земени предвид, и дека потребните промени се внесуваат во обуката, било како мали тековни модификации или во рамки на закажаните поголеми промени за осовременување. | | | | |
| **Слајд бр.** | | **Содржина:** | | |
| **1** | | ***PowerPoint*** (или друг вид презентација)  Обучувачот има на располагање PowerPoint презентација која може да му помогне да ја развие дискусијата за сите сесии опфатени со оваа обука. Обучувачот треба да ги подели формуларите за евалуација пред започнувањето на сесијата. Во одредени околности, обучувачот може да ги подели формуларите и на почетокот на обуката, со што учесниците ќе имаат можност да го пополнуваат во самиот тек на обуката, додека сесиите им се се уште во свежо сеќавање. Тоа е заради тоа што постои одредена тенденција учесниците да не ги пополнуваат целосно формуларите на крајот на обуката. | | |
| **2 - 3** | | Како и во претходните сесии, треба да се следи сличен формат на Агенда и задачи што се задаваат на почетокот на сесијата. | | |
| **4 - 21** | | Распоредот е добар начин да се потсетат учесниците за содржината на обуката и се вклучува за да му помогне на обучувачот.  Обучувачот треба да ги помине агендите и задачите зададени во сите сесии. Повратните информации и сугестиите на учесниците треба да се забележат, за да се употребат в иднина | | |
| **22** | | Обучувачот е задолжен да обезбеди дека сите учесници го имаат пополнето формуларот за евалуација. Обучувачот треба да ги собере пополнетите формулари и да му ги предаде на претставникот на Советот на Европа што е порано можно. | | |
|  | | **Практични вежби (доколку се предвидени)**  За оваа сесија не се предвидени други практични вежби освен формуларот за евалуација на Советот на Европа. | | |
|  | | **Проверка на знаењето**  Оваа сесија му нуди на обучувачот можност за проверка на знаењето што го стекнале учесниците преку поставување прашања во фазата на давање коментари за обуката. | | |
|  | | **Преглед / Резиме**  Обучувачите треба да обезбедат соодветни можности за учесниците да ги споделат своите коментари за обуката и да обезбедат дека тие се соодветно прибрани. | | |

# Евалуација

Евалуацијата е важен дел од обуката и за неа треба да се остави доволно време со што на учесниците ќе им се овозможи да го споделат своето мислење/коментари за обуката и наученото.

Оваа обука е од општа природа, и затоа повеќето од материјалите се со PowerPoint презентации и не предвидуваат практични вежби што вообичаено се поврзуваат со овој вид обука.

Изготвен е и формулар за обука, даден подолу во овој Дел. Обучувачите се задолжени да обезбедат дека сите учесници го имаат пополнето формуларот што треба да се врати во Советот на Европа и се искористат за унапредување на обуката во иднина.

# Оценување

Во рамките на оваа обука не е поднесено барање за оценување. Но, во земјите каде што оваа обука може да стане дел од програма што е подложна на оценување, за тоа може повторно да се размисли. Доколку се воведе оценување, за тоа треба да се користат методологии што се користат во таа земја.

.

**Додаток**

**Материјали за обука и материјали за учесниците на обуката**

1. Заедничкиот регионален проект на Европската Унија и Советот на Европа Компјутерски криминал@IPA (Регионална соработка во областа на кривичното право: зајакнување на капацитетите во борбата против компјутерскиот криминал) има за цел да ги зајакне капацитетите на властите кои работат на кривична материја од Западниот Балкан и Турција делотворно да соработуваат во борбата против компјутерскиот криминал [↑](#footnote-ref-1)
2. <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf> [↑](#footnote-ref-2)
3. http://register.consilium.europa.eu/pdf/en/03/st14/st14583.en03.pdf [↑](#footnote-ref-3)
4. Oвозможувач на интернет услуги [↑](#footnote-ref-4)
5. [↑](#footnote-ref-5)
6. [↑](#footnote-ref-6)