ЕВРО БАЛКАН

ЗБОРНИК НА ТРУДОВИ

Прва меѓународна научна конференција
„Влијанието на научно – технолошкиот развиток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија“

Скопје 20-21 декември 2013

ЗБОРНИК НА ТРУДОВИ: Прва меѓународна научна конференција
„Влијанието на научно – технолошкиот развиток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија“

Организатор: Институт за дигитална форензика
Универзитет „Евро-Балкан“ - Скопје

Уредник: Проф.д-р Сашо Гелев

Издавач: Универзитет „ЕВРО-БАЛКАН“ Скопје
Република Македонија
www.euba.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

001.3:330/378(497.7)(063)

МЕЃУНАРОДНА научна конференција (1 ; 2013 ; Скопје)
Влијанието на научно-технолошкиот развиток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија : зборник на трудови / Прва меѓународна научна конференција, Скопје 20-21 декември, 2013 ; [уредник Сашо Гелев]. - Скопје : Универзитет "Евро-Балкан", 2014. - 706 стр. : граф. прикази ; 24 см

Дел од текстот на англиски јазик. - Библиографија кон трудовите

ISBN 978-608-4714-05-7

а) Научен развиток - Општествени науки - Македонија - Излагања на конференции
COBISS.MK-ID 95578634

Програмски одбор

- Проф. д-р Павлина Витанова, ЕВРО-БАЛКАН, копретседател;
- Проф.д-р Сашо Гелев– Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија копретседател
- Проф. Влатко Чингоски, Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија
- Проф. д-р Лада Садиковиќ, Факултет за криминалистика, криминологија и безбедност, Универзитет во Сараево;
- Проф. д-р Здравко Скакавац, Факултет за правне и пословне студије, Универзитет УССЕ, Нови Сад;
- Проф. Д-р Божо Крстајиќ, Електротехнички факултет - Подгорица, Црна Гора
- Доц. д-р Марјан Николовски, Факултет за безбедност, Универзитет Св. Климент Охридски, Битола, Република Македонија
- Доц. д-р Ненад Танески, Војна академија, Скопје, Република Македонија
- Проф. д-р Гордан Калајџиев, Правен факултет, Универзитет Св. Кирил и Методиј – Скопје, Република Македонија
- Доц. д-р Митко Богданоски, Војна академија Скопје, Република Македонија
- Доц. д-р Роман Голубовски, Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија
- Проф. Д-р Драган Михајлов, УКИМ; Република Македонија
- Д-р Никола Протрка, Полициска академија, Загреб, Република Хрватска
- Проф. Д-р Тони Стојановски, Австралија
- Д-р Зоран Нарашанов, Винер осигурување, Скопје, Република Македонија
- Проф. Д-р Стефан Сименов, Академија за внатрешни работи на Република Бугарија

Организацискиодбор

- Проф. д-р Сашо Гелев, претседател;
- Проф. д-р Павлина Стојанова, член;
- Проф. д-р Александар Даштевски, член;
- Доц. д-р Вангел Ноневски, член
- Доц. д-р Јорданка Галева
- М-р Славко Гавриловски, секретар;
- Валентина Гоцевска, член;
- Игор Панев, член;
- Ивана Крајчиновиќ, член
- Драгана Каровска, член

Сашо Гелев
Електротехнички факултет – Радовиш
Универзитет „Гоце Делчев“ – Штип
saso.gelev@ugd.edu.mk
Роман Голубовски
Електротехнички факултет – Радовиш
Универзитет „Гоце Делчев“ – Штип
roman.golubovski@t-home.mk
Ристо Христов
risto.hristovst@gmail.com
Елениор Николов
Воена академија-Скопје
elenior.nikolov@ugd.edu.mk

МЕТОДОЛОГИЈА НА СПРОВЕДУВА НА КОМПЈУТЕРСКАТА ФОРЕНЗИКА

Апстракт *– Компјутерската форензика (дигитална форензика) во споредба со другите науки е релативно млада наука. Компјутерската форензика е воспоставена во 1999 година. Од тогаш таа е незаменлива алатка во делот за санкционирање на компјутерскиот криминал. Доброто познавање на методологијата на компјутерската форензика во најголема мерка може да помогне во расветлување на извршениот криминал. Но, не придржувањето кон методологијата на компјутерската форензика ги прави добиените докази неважечки-нерелевантни и не може да се искористат во докажување на извршениот криминал.*

Во овој труд ќе биде објаснета методологијата на изведување на компјутерската форензика со која се добиваат цврсти несоборливи докази кои може да се искористат во докажување на извршен криминал.

Колку што ми е познато во Република Македонија се уште никој сериозно не се занимава со проблемот на компјутерската форензика. Се надевам дека овој труд ќе анимира голем број на млади ентузијасти да навлезат во оваа област.

Клучни зборови *– компјутерска форензика, дигиталнна форензика, дигитален компјутерски доказ,*

METHODOLOGY OF IMPLEMANTATION OD COMPUTER FORENSICS

Abstract *– Compared to other sciences, computer forensics (digital forensics) is a relatively young discipline. It was established in 1999 and it has been an irreplaceable tool in sanctioning cybercrime ever since. Good knowledge of computer forensics can be really helpful in uncovering a committed crime. Not adhering to the methodology of computer forensics, however, makes the obtained evidence invalid/irrelevant and as such it cannot be used in legal proceedings.*
This paper is to explain the methodology of implementing computer forensics in the way that one can obtain valid and indisputable evidence that can be used in the process of proving the committed crime.
In the Republic of Macedonia there has been no serious investigation of this problem so far. This paper will hopefully inspire a number of young enthusiasts to delve into the field.
Compared to other sciences, computer forensics (digital forensics) is a relatively young discipline. It was established in 1999 and it has been an irreplaceable tool in sanctioning cybercrime ever since. Good knowledge of computer forensics can be really helpful in uncovering a committed crime. Not adhering to the methodology of computer forensics, however, makes the obtained evidence invalid/irrelevant and as such it cannot be used in legal proceedings.
This paper is to explain the methodology of implementing computer forensics in the way that one can obtain valid and indisputable evidence that can be used in the process of proving the committed crime.
In the Republic of Macedonia there has been no serious investigation of this problem so far. This paper will hopefully inspire a number of young enthusiasts to delve into the field.
Keywords *– computer forensics, digital forensics, digital computer evidence*

ВОВЕД

Компјутерската форензика е гранка на форензичката наука, која се занимава со легални методи на собирање и обработка на дигиталните докази сместени на компјутер (или друг носач на дигитални податоци). Со компјутерската форензика се испитуваат сите медиуми за сместување и пренос на податоци со цел пронаоѓање и анализирање на документи или други дигитални докази, а кои се поврзани со некоја нелегална активност.

Денеска постојат многу дефиниции за дигиталната форензика и дигиталниот доказ. Еве неколку дефиниции:

„Дигитална форензика е примена на науката и инженерството во решавање на легални проблеми на дигиталните докази“

„Дигитална форензика е наука за собирање, чување, испитување, анализирање и презентирање на релевантни дигитални докази кои се употребуваат во судското процесирање“

Поимот „форензика“ доаѓа од латинскиот збор „forensi“ што значи „ на отворен простор или јавно“.

Компјутерските форензичари ги испитуваат сите медиуми за сместување податоци (FDD, HDD, CD/DVD ROM, USB, Tape driver, итн). [2] Поимот компјутерска форензика се врзува за некое малку подалечно време, кога Интернетот не бил ваков каков што е денеска. Денеска повеќе се зборува за „Cyber forenzici“, бидејќи местото на извршување на кривичното дело не може да се поврзе само за компјутерот и масата на која се наоѓал компјутерот во моментот на извршување на тоа дело. Ова истрага се проширува во виртуелниот свет, во светот на Интернетот, мрежата и се проширува на другите дигитални уреди (gsm, gps, дигитални фотоапарати, smart телефони, PDA и др.

Поимот „дигитален доказ“ подразбира било каков релевантен податок доволен да го докаже криминалното дело извршено врз компјутерскиот или мрежниот медиум наменет за складирање податоци, вклучувајќи примероци на текст, слика, видео, говор.

Дигиталниот компјутерски доказ е составен од мноштво вистински докази, од кои ниту еден не смее да се исклучи од било која причина. Доказите мора да бидатпотполни, меѓусебе да се надополнуваат и да немаат таканаречена пукнатина за донесување на заклучок, односно за утврдување на цврстиот доказ.

Според „The Scientific Working Group on Digital Evidence(SWGDE) терминот доказ се употребува за „нешто материјално“ кое може да биде признаено од судот. Тоа мора да биде собрано на легален и законит начин. Некои објекти (податоци или материјални средства) стануваат докази единствено кога во нив поверува службата на спроведување на законот. Според истиот извор, под поимот дигитален доказ се подразбира секоја информација или доказ кој има вредност која е сместена или трансмитирана (префрлена) во дигитален облик.

Компјутерската форензика е многу значајна за успешно процесуирање на криминалците во областа на компјутерскиот криминал. Значи дека за време на целата форензичка истрага мора да се почитуваат одредени принципи за да може дигиталниот доказа да биде прифатен од страна на судот. Денеска имаме голем број на модели и рамки за успешна форензичка истрага. Најпознати модели се:

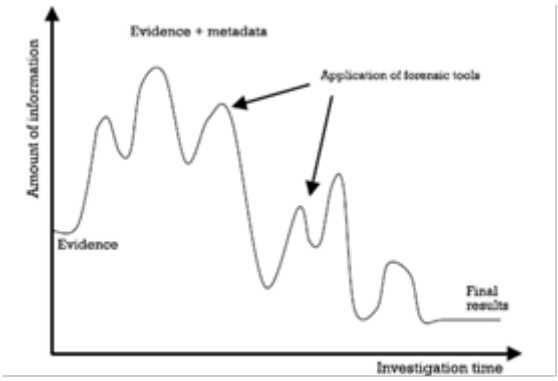
- Lee’s model
- Casey model
- DFRW framework
- Reith, Carr and Gunch model

- Kruss & Heisser model
- USDOJ model
- Ciardhuain Extended model

Сите модели на судските вештаци треба да им понудат:

- Прифаќање и прифатливост
- Сигурност
- Повторливост
- Интегритет
- Причина и последица
- Документираност

За време на форензичката истрага мора да се испочитуваат сите 6 начела. Количината на податоци кои се процесираат е огромна. Пребарувањето понекогаш може да трае и со денови и недели и да се анализираат терабајти со податоци, а на самиот излез да се добијат само неколку мегабајти податоци кои може да му помогнат на истражителот.



Сл.1 Количина на обработени информации за време на форензичката истрага

На слика 1 прикажан е односот на количината на податоци кои влегуваат во системот на форензика и податоците кои ги имаме на излезот како резултати на пребарувањето

Основи на дигиталната форензика

Кога од некој сервер ќе му се нанесе одредена штета, односно ќе се направи некое кривично дело кое се санкционира според законите мора да се преземат одредени активности за зачувување на сите траги кои би можеле да се искористат во истрагата. При спречување на одреден упад на сервер мора да се постигнат следните цели:

Прво и основно е дека не треба да се истревожи натрапникот-бидејќи може да се направи неповратна штета.

Второ што мора да се направи е дека не смее да се дозволи продолжување на безбедносниот инцидент-односно да се спречи зголемувањето на штетата.

Трета работа е дека не смее да се модифицира системот (на тој начин се врши компромитирање на форензиката).

Идеално е доколку може да се постигне да оној кој провалува мисли дека ништо не е променето и да мисли дека се е нормално.

Многу значајно е да се напомене дека „**не смее да се гаси серверот“**. Секогаш постои подобра опција.

А зошто да не се гаси серверот? Бидејќи сите тоа го работат, па провалникот ќе очекува да го изгасиме серверот и на тој начин тој би се заштитил:

- Работејќи директно во RAM меморијата
- Креирајќи/модифицирајќи ги постоечките скрипти кои се изведуваат при гасење на серверот

Со гасењето на серверот се губи дел од податоците:

- Состојба на мрежата
- Меморија
- Активни процеси

Од моментот кога ќе се случи одреден инцидент, при спроведување на форензиката се издвојуваат три основни дела:

1. Интервенција и прибирање на податоци (докази)
2. Анализа на собраните податоци
3. Изработка на извештај (еден дел од ова се одвива и во првите два дела)

За да може квалитетно да се реагира потребно е да се подготвен за:

- Брза реакција
- Собирање на податоците без да се има влијание врз податоците
- Чување на собраните податоци во целост
- Да се врши истражување во кое мора да се користат делови од системот на кои не е сигурно дека може да им се верува

Основни насоки при спроведување на форензиката се:

- Минимизирање на губењето на податоци
- Се собираат **СИТЕ** податоци кои може да се соберат
- Се анализира **се**
- Мора да се погрижиме дека во секој момент може да се докаже интегритетот на форензиката (значајно е и ако целта е да се открие изворот на упад)

Основа за успешна форензика е **подготовката**. Потребно е да се има најмалку едно cd/dvd на кои статички се преведени извршните датотеки. Се советува да се користи посебен форензички диск за сместување на собраните податоци.

Покрај минималниот алат постои и голем број напредни форензички алати кои се доста скапи и специјализирани. Постои софтверски и хардверски алати. Но најсилен алат секако е знаењето. Многу е лесно да се прави анализа кога се знае што се наоѓа на серверот. Кога еднаш ќе се добие слика за серверот, многу полесно е да се издвојат „ необичните“ однесувања.

Неопходно е да се направи CD кое ги содржи извршните датотеки за сите посебни наредби кои се изведуваат за време на форензиката, поточно за време на собирање на податоците. Такво cd мора да постои за секоја архитектура која постои во системот. На cd-то мора да се наоѓаат следните наредби:lsof; ps; nmap; nc; memdump; dcfldd; netstat; arp; route; ifconfig; lees; more, cat; dd; md5sum; sha1sum.

Дискот кој се користи за форензика мора да биде празен и подготвен за работа. Големината на дискот треба да е барем еднаква на најголемиот диск во системот

Интервенција и прибирање на податоци

Пред било каква акција треба да се разговара со администраторот на апликацијата и серверот, да му се објасни ситуацијата и да се проба да се соберат што повеќе општи информации:

- Каде се наоѓа системот?
- За што служи?
- Како е конфигуриран
- Кои активни/пасивни заштити постојат на системот
- Како најдобро да се пристапи, кои податоци кои постојат на серверот

Потребно е да се запре сигурносниот инцидент(да се спречи појавување на било каква понатамошна штета) и

Потребно е се да се документира.

Целта ние во оваа фаза да се пријавиме како root на серверот. Но доколку не може да се добијат root овластувања-форензиката продолжува со рестартирање во knopix или некој resque cd/dvd. Но во тој случај недостасува голем број на податоци-и ова треба да се документира.

Како да се препознае дали постои инцидент?

- Има голем број на излезни конекции
- Познат daemon кој се врти под сомнителен корисник
- Се проверува оптоварувањето на серверот и сите процеси кои стваараат зголемено/невообичаено оптоварување
- Се врши брза проверка со: ifconfig; lsof –i –n –P –I; ps e –Alf – cols 300
- Исто така се врши проверка со nmap + разговор со администраторот.

Доколку се работи за лажна тревога – од ова може да се научи и како да се документира настанот.

Собирање на податоци

Прв чекор е да се утврди дали навистина е во прашање упад и дали сеуште е активна
Кога ќе се пронајде основано сомнение собирањето на податоците оди по редослед по кој се менуваат и самите податоци
Состојба на меморијата> состојба на процесите> состојба на мрежните конекции> состојба на дискот.
Најдобро е компјутерот од кој се врши форензиката и компромитираниот сервер да се спојат на ист хаб. Доколку ова не може да се направи, се препорачува да се ограничи сообраќајот кон и од серверот за да може да се направи форензиката и да се спречи понатамошната штета.[4]
Се користи netcat за да се пренесат податоците со што помало влијание на системот. За пренесување на осетливи податоци може да се врши криптирање на преносот со помош на ssh тунел ili cryptcat наредба.

Потребно е да се направи слика на моменталната состојба на работната меморија и swap-от.

Потребно е да се соберат податоците од метадата датотечниот систем. Овие податоци од датотечниот систем се исклучително подложни на промени – една наредба може да го промени последното време на пристап кон сите датотеки кои се користат за извршување. Неопходно е што побрзо да се соберат податоците

Потребно е да се соберат сите можни податоци за процесите-доколку упадот и понатаму е активен овде сигурно се наоѓаат податоци. Но мора да се внимава бидејќи процесите скоро секогаш се покриваат. Сите процеси кои се одвиваат со даемоните во /home се сомнителни.

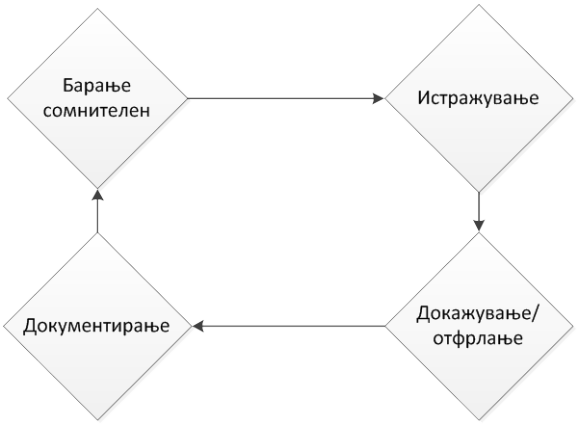
Потребно е да се соберат податоците за состојбата на мрежата. Доколку упадот е откривен и пријавен и доколку се уштре трае во податоците за состојбата на мрежата сигурно се наоѓаат докази.

Секако мора да се соберат податоците од дискот. Најдобро е да се соберат „raw data“ податоците од сите партиции/дискови. Доколку проблем претставува големината на меморијата која ја има форензичкиот диск тогаш од круцијално значење е на некој начин да се добијат податоци за моменталната состојба. (Виртуелен сервер; Сервер со raid поле-да се издвојат и клонираат дисковите доколку тоа е можно; Сервер на SAN-от-да се копира на друг диск;...)
Мора да се забележи дека постои разлика во собирање на податоци од исклучен сервер(податоците не се мунуваат) и од активен сервер(податоците во секој момент се менуваат).

Откако ќе се заврши со собирање на податоците и се изврши верификација на собраните податоци, во склад со политиката на установата која го поседува серверот да се изврши или запирањена работата на серверот или негово преинсталирање

Анализа на собраните податоци

Анализата на собраните податоци претставува кружен циклус. Анализата завршува кога ќе се пронајде причината или кога ќе се исцрпат сите опции.



Слика 2: Анализа на собраните податоци

Основно прашање е од каде да се почне. И овде секако се бара некој сомнителен облик на однесување. [5]

Доколку се посовневаме дека има упад во одреден период се врши проверка на log датотеката за тоа време. Недостаток на истите околу тоа време е трага дека напаѓачот се стекнал со root овластување над серверот.[1] Доколку нема ништо во log датотеките на серверот во централниот loghost, и ако истите не се разликуваат се бара понатаму.

Дополнителен добар начин за започнување на форензиката е покренување на алат за откривање rootkit-от **chkrootkit** или **rhunter**. Се бараат знаци:

- за модификација на извршните датотеки (тројанци)
- за бришење на lastlog, wtmp, wtmpx
- за тројанци кои како модули се вчитуваат во Кернелот
- за логови од sniffer
- конфигурациски датотеки од rootkit програмата

Анализа на собраните податоци за состојба на процесите. При анализа на состојбата на процесите треба да се бараат сите процеси кои се

покренати под погрешно име и/или се на необични порти и/или прв пат се стартувани во времето кога се сомневаме дека на серверот е направен упад. Овде е многу значајно да го согледаме значењето на времето на серверот и понатаму за сите такви записи да се бараат повеќе податоци или во извршната датотека или за корисникот во чие име е покренат процесот.

Анализа на собраните податоци за состојба на меморијата. Најтешко е од меморијата да се соберат податоци кои се корисни за процесот на форензика. Постојат одредени специјализирани алатки за ова, но во меморијата се пребарува како датотека. Најкорисно е за лоцирање на оние процеси кои користеле голем дел од меморијата

*Анализа на собраните податоци за состојба на мрежат*а. Како излез од lsof наредбата се добиваат сите отворени датотеки и socketi. Посебно треба да се обрне внимание на оние порти кои слушаат. Исто така треба да се обрне внимание на се поголемата количина на излезни конекции-ова може да претставува индикација за напад на оддалечен сервер. Сомнителни се и сите датотеки кои се отворени од директориум кои почнуваат со. (сокриени директориуми)

Анализа на собраните податоци од метадата датотечниот систем. Голема количина податоци се наоѓа на самиот диск, но податоците за промените се тие од кои се наоѓа кои податоци на дискот се значајни.

Со fls наредбата се собираат метадата податоци за зададена датотека/директориум

Inode е запис кој ја опишува датотеката. За да може да се соберат податоци за записите на партициите прво мора да се соберат податоците за партициите. Со наредбата mmls како излез се добива испис на партицијата; јавува и кој простор не е доделен на ниедна партиција; ги излистува сите партиции вклучувајќи го и swap.

Откако ќе се собере пописот на партициите се спроведуваат fls и ils наредбите. Fls собира „timeline“ податоци за алоцираните и неалоцираните датотеки. Некои податоци се избришани ама метадата податоците во inod-от (или во дел од нив) се сочувани. Ils наредбата собира податоци за таквите датотеки и потребно е нејзиниот излез да се спои со излезот од fls наредбата.. Излезот од двете наредби се движи по дискот и собира податоци од inod записот како наидува на нив-несредено, расфрлано и нелогично распоредени записи. Во inod записот се бележат 3 работи за датотеките кои се обележуваат со M a C:

- M-„modified time“- време кога последен пат е менувана содржината на датотеката
- a-„accessed time “ време кога последен пат е направен пристап до датотеката (читање)

- C-„changed time “ време кога последен пат е модифицирана досржината на inod записот.

Записите во датотеката креирана со наредбите fls и ils се сортирани по датотечното стебло.

Од собраните метадата податоци може да се бараат и дополнителни работи како:

- Log датотеки и history датотеки
- Било кои податоци кои во името содржат “.“
- Промени во /dev директориумот
- Скоро модифицираните извршни датотеки („bin“ 3 клучен збор)
- Скоро креираните датотеки.

Анализа на собраните податоци од дискот. Сликите на дисковите и/или партициите кои се собрани можат со помош на mount наредбата да се оспособат за работа и да се користат за форензиката. Мора да се забележи дека на дискот се наоѓаат најмногу податоци. Добри места за почеток со работа се(иако не се препорачува да се тргне со прегледување на дискот):

- Прегледување на \home\ директориумот во потрага по скриени директориуми и датотеки
- Прегледување на сите log датотеки во периодот околу времето на упад
- Пребарување на системските партиции во потрага по неодамна направени промени
- Прегледување на целиот диск во потрага по датотеки со „недозволени“ овластувања.

Во ова прегледување greb и find се главни алатки но постојат и други.
Во комбинација со собраните метадата податоци може да се направи временски дијаграм на текот на упадот и на сите активности.

Со прегледување на записот на дискот може да се види во каква состојба бил системот во моментот на упад-дали одржувањето на системот било на ниво или..

Изработка на извештај

При изработка на извештајот добро е да се издвојат две работи:

a. Што е направено
b. Што е пронајдено

а) Во делот кој опишува што е направено на прецизен начин се опишуваат и аргументираат сите чекори кои се преземени при собирање на податоците. Се води прецизен временски дневник. Се аргументираат сите прескокнати чекори. Се забележува секоја проверка која е направена со цел да се докаже некомпромитираност на доказите/

b) Во делот кој опишува што е пронајдено се потврдуваат сите наоди со администраторот на серверот или со корисниците на кои се однесуваат тие податоци. Прецизно се опишува зошто се смета дека од собраните докази следи донесениот заклучок. Потребно е извештајот да има одреден облик(доколку се само нафрлани мисли се губи голем дел од кредибилитетот).[3]

Во конечниот извештај мора да се наоѓаат следните компоненти:

- Дневник на преземени акции и собрани материјали
- Начин на кој влегол натрапникот во серверот
- Овластувања кои ги стекнал натрапникот
- Попис на апликации кои ги инсталирал натрапникот и го покренал системот
- Опис на состојбата на серверот во моментот на упад
- Опис на ранливостите искористени во упадот

Секако може да се додаде и совет за понатамошни акции и совет како да се избегнуваат слични инциденти во иднина

Заклучок

Во изнесениот труд објаснети се општите поими за компјутерската форензика и објаснети се етапите во спроведување на истата.

Значајно е да се забележи дека компјутерската форензика е доста комплицирана работа бидејќи:

- Потребно е да знаеме да работиме со луѓето и со компјутерите
- Треба секогаш да се биде подготвен
- Потребно е да се разбере системот како и сите негови функции за да може правилно да се толкува
- Потребно е доста големо трпение (доказите може да се наоѓаат било каде)
- Потребно е да знаеме да ги поврземе работите и
- Потребно е да се биде темелен во работењето

Компјутерската форензика е многу сериозна работа бидејќи се истражуваат акции на криминалци, може да се направат непоправливи штети и можно е собирање на приватни податоци-што значи дека форензиката мора да биде квалитетно обработена.

На крај значајно е да кажеме дека мора да се заштитиме, со редовно правење на backup, со активни и пасивни линии на одбрана, со што би се сопреле „сите упади“.

ЛИТЕРАТУРА

[1] Ovie L.Carroll, Stephen K. Brannon, Thomas Song: Computer Forensics: Digital Forensic Analisys Methodology, United States Attorneys'Bulletin, January 2008

[2] M.Milosavljevic, G.Grubor: Digitalna forenzika racunarskog sistema, UNIVERZITET SINGUDUNUM, Beograd 2009

[3] G.Grubor, I.Franc: Evolucija modela digitalne forenzicke istrage, UNIVERZITET SINGUDUNUM, Beograd 2010

[4] Forensic Information Technology Working Group, Guidelines for best practice in the forensic examination of digital technology, www.fitwg.com 2003

[5] Adelstein, F., Live Forensics: Diagnosing Your System Without Killing it First, Help Net Security News, 2009