INTERNACIONALNI UNIVERZITET TRAVNIK U TRAVNIKU

FAKULTET INFORMACIONIH TEHNOLOGIJA TRAVNIK U TRAVNIKU

ZAVRŠNI RAD

INFORMACIONE TEHNOLOGIJE U FUNKCIJI DIGITALNE FORENZIKE

Mentor:
Prof.dr.sc. Mladen Radivojević

Student:
Arif Ganija

Travnik, 2019.

INTERNACIONALNI UNIVERZITET TRAVNIK U TRAVNIKU

FAKULTET INFORMACIONIH TEHNOLOGIJA TRAVNIK U TRAVNIKU

ZAVRŠNI RAD

INFORMACIONE TEHNOLOGIJE U FUNKCIJI DIGITALNE FORENZIKE

Mentor:
Prof.dr.sc. Mladen Radivojević

Student:
Arif Ganija

Travnik, 2019.

SADRŽAJ

1. Uvod

Razvoj i napredak informacionih tehnologija je temeljni element u omogućavanju i implementaciji novih pristupa poslovanja. Informacione tehnologije predstavljaju nezaobilazan faktor modernog menadžmenta i ključni resurs za donošenje promjenu poslovnih odluka, njihovu operacionalizaciju, kao i kontrolu učinka tako utvrđenih odluka.

Pojavom savremenih računara i široka rasprostranjenost i velika količina najrazličitijih korisničkih programa uticalo je na promjenu života ljudi širom svijeta.

Nastanak računara, i njihovo medusobno umrežavanje i stvaranje jednog informacionog i globalnog okruženja, vezuje za jednu dobru i pozitivnu ideju koja se odnosi na medžusobnu komunikaciju na svjetskom nivou. Međutim mora se prihvatiti činjenica da ona sa sobom donosi i mnogo rizika.

Tehnologija sa jedne strane, može postati moćno oružje u našim rukama, medžutim ono isto tako može biti usmjereno i protiv nas jer je postalo globalno dostupno.

Nažalost možemo da konstatujemo da je ovakav tehnološki progres pratilo i razvijanje ideje o korištenju novih tehnologija u protivpravne svrhe. Naime razvojem informaciono-komunikacionih tehnologija i računarskih mreža dolazi do pojave visokotehnološkog kriminala i on je postao svakodnevnica.

U radu će biti navedene i definicije koje se najćešče pojavljuju u vezi sa visokotehnološkim kriminalom kao i način istraživanja i otkrivanja istog. Jedan od načina je i primjena digitalne forenzike.

Skup procedura i metoda koje se koriste u prikupljanju, analizi i prezentaciji dokaza koji se mogu pronaći na računarima, računarskim mrežama, bazama podataka, mobilnim uređajima, te svim ostalim elektronskim uređajima na kojima je moguće sačuvati podatke naziva se digitalna forenzika.

Digitalna forenzika je nauka novijeg datuma i u vrlo kratkom periodu našla je mjesto u postupcima istrage i dokazivanja krivičnih djela nastalih zloupotrebom računara. Zbog prirode medija koji ih sadrže, digitalni podaci i informacije vrlo su ranjivi i potrebno je izvršiti brzo prikupljanje, arhiviranje i obradu podataka, kako bi se sačuvala reprezentativnost informacije i obezbijedila mogućnost njenog korištenja u svrhu dokazivanja na sudu.

Primarni ciljevi digitalne forenzike su:

- Prikupljanje, obrada, pohranjivanje i zaštita digitalnih dokaza

- Razotkrivanje motiva i cilja napadača
- Korištenje dosadašnjih saznanja za prevenciju i zaštitu od budućih napada

Primjena metoda i tehnika digitalne forenzike u vremenu u kojem živimo je sve značajnija, obzirom da je Internet postao zaseban virtualni svijet u kojem su rizici od napada na podatke i materijalnu imovinu lica sve češći i ozbiljniji. U tom kontekstu, nezamjenjiva je uloga digitalne forenzike kao naučne discipline koja uključuje procese prikupljanja, snimanja i analiziranja digitalnih podataka, kako bi se testirala sigurnost računarskog sistema ili otkrio napadač koji narušava sigurnost IT sistema ili koristi IT sistem za izvršenje nelegalnog djela i prikupili čvrsti digitalni dokazi koji će se koristiti u sudskom postupku za sankcionisanje nelegalnih aktivnosti.

U ovom radu predstavljen je postupak forenzičke analize izuzetih medija sa digitalnim podacima koji čine osnov za sumnju na počinjeno kazneno djelo . U teorijskom dijelu ovog rada su opisane metode prikupljanja digitalnih dokaza, njihove analize i prezentacije. Te metode su u nastavku primijenjene na demonstracijski primjerak digitalnog medija koji se inače koristi kod treniranja u digitalnim forenzičkim istragama. Dobijeni rezultati pokazuju uspješnost primjene metoda i tehnika digitalne forenzike u prikupljanju dokaza o izvršenim krivičnim djelima, što može biti od velikog značaja za pokretanje i izvođenje sudskog postupka u procesu sankcionisanja počinilaca ovih krivičnih djela.

2. Računarski sistemi i osnovne komponente

Da bi smo mogli kvalitetno govoriti i bolje razumjeti funkciju informacionih tehnologija u digitalnoj forenzici potrebno je se nakratko osvrnuti na osnovne komponente računarskih sistema.

Osnovicu informacionih sistema čini informacija, a upravo te informacije se nalaze u računaru koji je predmet analize i prezentacija dokaza digitalne forenzike.

- Računarski sistemi (računari) su elektronske mašine koje obrađuju ulazne informacije (podatke) i iz njih proizvode izlazne informacije (rezultate).[1]
- Računar je mašina bez inteligencije jer izvršava samo ono što mu je zadato instrukcijama.
- Postupak pisanja naredbi (instrukcija) koje računar treba da izvrši naziva se programiranje.

Imajući u vidu da je računar samo mašina koja radi po određenom programu, može se reći da se svaki računarski sistem sastoji od dvije komponente:

- same mašine = HARDVERA
- programa po kojima računar radi = SOFTVERA

Tipičan računarski sistem sastoji se od:

- centralne (unutrašnje) memorije
- aritmetičko-logičke jedinice
- kontrolne jedinice
- jedinice spoljne memorije
- ulazne i
- izlazne jedinice.

2.1. Funkcionalna organizacija računarskog sistema

Kontrolna jedinica je koordinator rada celokupnog računaskog sistema.[2]

Ona:

[1] - http://racunarskapismenost-wordpress-com.cdn.ampproject.org
[2] Isto

- kontroliše izvršenje programa,
- uzima instrukcije iz memorije i prepoznaje ih,
- dekodira i naređuje odgovarajuće akcije drugim jedinica,
- započinje operacije ulazno-izlaznih jedinica i
- prenosi podatke u centralnu memoriju i iz nje.
- Kod savremenih računara sastoji se od skupa čipova kojima se kontroliše i koordinira rad celokupnog sistema.

Ulazne jedinice

Kod višekorisničkih računara za unos podataka i programa koristi se terminal, koji se sastoji od ekrana i tastature.

Kod personalnih računara osim tastature kao ulazne jedinice koriste se miš, digitajzer (grafička tabla), kao i razni drugi specijalizovani uređaji (skenere, digitalni fotoaparat, čitač bar-koda, itd)

Izlazne jedinice

Monitor (kod PC) i ekran terminala (kod višekorisničkih računara)

Za štampanje manjih količina podataka obično se koriste serijski štampači, koji štampaju znak po znak, ili laserski štampači.

Za štampanje velikog broja podataka koriste se linijski štampači koji štampaju cjeli red odjednom. Brzina štampanja ovih štampača iznosi 300-500 redova u minuti. Ploter

Osnovne komponete računara

- monitor (1)
- tastatura (10)
- centralna jedinica (kućište):
- matična ploča (2)
- procesor i soket (3)
- kontroleri (4)
- RAM memorija (5)
- kartice (grafička, zvučna…) (6)
- napajanje (7)
- optički disk (8)
- hard disk (9)

Matična ploča

- Sinonim: osnovna ploča *(mother board)*

- Sadrži procesor, ROM memoriju (u kojoj se nalazi *BIOS** računra), keš memoriju, magistralu koja povezuje sve elemente, skup čipova koji kontrolišu rad računara, kontrolere za priključenje diskova, slotove za dodatne kartice i portove za povezivanje drugih uređaja.
- Najznačajnije karakteristike su tip podržanog procesora *(socket)* i tip podržane memorije (DDR2, DDR3) i broj memorijskih priključaka koji određuje maksimalnu količinu radne memorije računara.
- Najpoznatiji proizvođači su *Asus i Gigabyte*.

Centralna procesorska jedinica (CPU)

Sastoji se od:

- aritmetičko-logičke jedinice (ALU – skup elektronskih kola za izvođenje aritmetičkih (+, -, •, ÷) i logičkih operacija)
- kontrolne jedinice
- registara za prihvat podataka
- CPU određuje tip računara. On izvršava sve instrukcije zadate programom.

Karakteristike procesora

- određene su njegovom arhitekturom (građom, načinom izrade)
- brzina procesora (MIPS) – milion instrukcija po sekundi
- dužina procesorske riječi – broj bita koji se istovremeno prenosi i obrađuje unutar procesora (od prvog četvorobitnog, do današnjih 64-vorobitnih)
- radni takt – generiše ga sat (*clock*), usklađuje početak izvođenja operacija (u Hz, tj. gigahercima)
- interni keš – vrlo brza memorija, danas od 512kB…

Primjeri tipova procesora

- PC486 procesor 80486, radni takt 33-133MHz
- Pentium procesor P5, radni takt 90-233MHz
- Pentium II, procesor P6, takt 300-400MHz…
- Danas tržištem vladaju dva proizvođača,
- Intel sa svojim procesorima Celeron, Pentium DualCore, Core i3, Core i5, Core i7… i
- AMD sa svojim procesorima Sempron, Athlon, Optheron, Phenom, Phenom II, Bulldozer…

Mjesto CPU u računaru

- Procesor se montira na osnovnu (matičnu) ploču. Na osnovnoj ploči se nalaze priključno mjesto (*socket*), koje podržava procesore odgovarajućeg tipa. Zato se ne može bilo koji CPU postaviti na bilo koju matičnu ploču.
- Zbog velikih brzina rada, dolazi do zagrijavanja, pa je potrebno postaviti i hlađenje, tzv. kulere. Oni mogu biti izvedeni pasivno (sistem bakarnih cijevi) ili aktivno (uz odgovarajući ventilator.)

Mjesto unutrašnje memorije u PC računaru

- Memorija PC računara se postavlja u kućište računara, na matičnu ploču (*motherboard*). Na matičnoj ploči se nalaze keš (*cache*) memorija i ROM memorija, dok se za montiranje radne memorije – RAM, nalaze odgovarajući konektori.
- U unutrašnjoj memoriji su smješteni program i podaci koji se obrađuju.
- Sastoji se od elektronskih kola, od kojih svako može da ima dva stanja koja se označavaju 0 i (0 – stanje kada u kolu nema struje, 1 – kada u kolu ima struje). Zbog toga se ova kola zovu bit (skraćeno od *binari digit* – binarna cifra).
- Pošto jedno elektronsko kolo može da zapamti samo informaciju da i ne (jedan bit), bitovi se udružuju u grupe – registre, koji su kod personalnih računara dužine 8 bita – bajt

Tipovi unutrašnje memorije

- RAM *(Random Access Memory* – Memorija sa slučajnim pristupom). Služi za smještanje podataka i programa na kojima računar trenutno radi. U ovu memoriju se može zapisivati. RAM memorija se može i iščitavati. Po nestanku napajanja, njen sadržaj se gubi. Trenutni kapacitet od 2GB i naviše. Kupuje se u modulima. Tipovi: DDR2, DDR3…
- ROM (*Read Only Memory*). Može se samo iščitavati. Sadržaj joj se ne gubi po nestanku napajanja. Neophodna je za pokretanje računara jer se u nju smještaju instrukcije za to (tzv. BIOS računara – *Basic Input Output System*).
- KEŠ (*cache*) vrlo brza memorija uz procesor (eksterni keš) ili u procesoru (interni). Današnji kapacitet od 1MB.

Magistrale

Komunikacioni put od električnih kola pomoću kojih se razmjenjuju informacije među komponentama.

Tri ključne magistrale:

- magistrala podataka (za razmjenu podataka između procesora i memorijskih lokacija)

- adresna magistrala (prenosi adrese kojima se specifikuje memorijska lokacija na koju se upisuju podaci ili sa kojih se čitaju podaci radi obrade a generiše ih procesor)
- kontrolna magistrala (služi za prenos upravljačkih i kontrolnih signala od procesora ka komponentama i obratno).

Kartice

- Zvučna: zvuk snimljen u digitalnom obliku pretvara u analogni kako bi se mogao reprodukovati na zvučnicima (slušalicama).
- Mrežna: omogućava umrežavanje računara u lokalnu mrežu računara (*lan – local area network*) radi razmjene podataka i zajedničkog korištenja hardvera i softvera.
- FM kartica: omogućava prijem radio talasa na FM frekvenciji.
- FMV kartica: kartica koja putem telefonske linije omogućava slanje faxa, komunikaciju računara i prenos glasa (*fax modem voice*).
- TV kartica: omogućava prijem tv signala.

Grafička kartica

- je uređaj koji podatke uskladištene u računaru u digitalnom obliku obrađuje u odgovarajuće signale koji kontrolišu prikazivanje slike na računaru.
- Slika na ekranu se prikazuje tehnikom bitmapiranja (*bit mapping*). To znači da se svakom pikselu ekrana pridružuje 1 ili više bita u memoriji.

  Na primjer:

- za 1 piksel 1 bit => moguće 21 = 2 boje
- za 1 piksel 8 bita => moguće 28 = 256 boja
- za 1 piksel 16 bita => moguće 216 = 65536 boja (*High Color*)
- za 1 piksel 24 bita => moguće 224 = 16,777 miliona boja
- za 1 piksel 32 bita => moguće 232 = 4,3 milijarde boja

- Kako se za memorisanje slike ne bi trošila RAM memorija računara, grafička kartica ima sopstvenu memoriju. Kapacitet joj se danas kreće od 1GB i više. Zbog programa i igara koji zahtevaju obradu složenih slika, savremene grafičke kartice imaju i grafičke procesore (GPU – *Graphic Processing Unit*).
- Najpoznatije grafiče kartice su: GeForce bazirana na čipovima *kompanije nVidia* i *Radeon* baziran na čipovima kompanije ATI.
- Najnovije grafičke kartice nude isključivo digitalni izlaz (DVI), dok se analogni izlaz (VGA) sve rijeđe sreće.

Jedinice spoljne memorije

- Ove jedinice služe za čuvanje programa i podataka kada računar nije u upotrebi.
- Kada se koristi program, po kome radi i svi podaci koje računar obrađuje nalaze se u unutrašnjoj memoriji ili kroz nju prolaze. Međutim, i za vrijeme rada računara dijelovi programa i podaci, koji trenutno nisu potrebni privremeno se skladište na jedinicama spoljne memorije.

Hard disk

- Kapacitet diskova se mijenjao od preko 20, 40, 80MB pa oko 250 i 500MB,
- Današnji diskovi imaju od 250GB do 1 TB. Trenutno se prave diskovi sa pločama kapaciteta od 20-40GB po ploči i brzinom rotacije 5400-7200 obrtaja u minuti.
- Prosječno vrijeme pristupa 8-10ms

Eksterni hard diskovi

- Kapaciteta 250-320-500GB
- Prenosivi hard disk se napaja preko USB i nije mu potrebno nikakvo spoljno napajanje

Jedinica diskete

- U upotrebi su diskete od 3,5” (3,5 inča) kapaciteta 1.44MB.
- Postoje i diskete od 100 i 250MB, a uređaj koji čita ove diskete zove se ZIP drajv CD ROM diskovi
- Primjenom laserske tehnologije nanosi se zapis na metalnu površinu.
- CD uređaj primjenom laserskog zraka detektuje neravnine na površini i očitava podatke.
- Kapacitet CDa je 640-700MB (800MB)

DVD (*Digital Video Disk*)

- Prvobitno nastao zbog potrebe snimanja dugometražnih filmova na CD
- Moguće je korišćenje sa jedne ili sa obe strane
- Kapaciteta su od 4,7 GB

Fleš (USB) diskovi

- Sastoji se od memorijskih modula čiji se sadržaj ne briše kad ostanu bez napajanja strujom.
- Kapaciteta su 1GB, 2GB, 4GB, 8GB, 16GB, 32GB i više.
- Kod novijih računara se često i hard disk priključuje na USB priključak koji se nalazi u unutrašnjosti računara (160GB-500GB)

Izvor napajanja

- je uređaj koji mrežni naizmjenični napon frekvencije od 50Hz i 220V prevodi u jednosmjerni napon od 5 ili 12 volti koji napaja komponente kućišta i periferijske uređaje (koji nemaju sopstveni priključak za električnu energiju). Snaga izvora se izražava u vatima i kreće se od 300W i više. Izvor mora biti dovoljnog kapaciteta i stabilnosti. U protivnom sistem otkazuje.
- Ako nestane napajanja, uređaj zvani UPS (neprekidni izvor napajanja, praktično akumulator) može obezbediti autonomni rad od 15-ak minuta, što je dovoljno da se rad na računaru okonča na siguran način.

2.2. Uticaj komponetni na performanse (brzinu) rada računara

Procesor

- što veći radni takt, to bolje: 2,2GHz, 3,4GHz, 3,8GHz
- što više jezgara (*core*), to bolje: Dual, Quad, 8-core jezgra su u stvari mikrprocesori koji se nalaze na istom čipu
- što više keš memorije, to bolje: npr. 2 MB

Ram memorija

- što veći kapacitet, to boje: npr. 4GB, 8GB
- što brža memorija, to bolje: npr. 1333MHz, 1866MHz

Hard disk

- što veća keš memorija diska, to bolje: npr. 16MB, 64MB
- što veća brzina prenosa, to bolje: npr. 6Gb/s

Grafička kartica

- što više grafičke memorije, to bolje: npr. 1 GB, 2GB

3. Forenzika

U uvodu ovog rada je data definicija digitalne forenzike. Kako je digitalna forenzetika dio opšte naučne oblasti koja se zove forenzika, postoji potreba definisanja forenzike. Jedna o definicija forenzike je: “Forenzika je proces korištenja naučnih metoda pri sakupljanju, analizi i prezentaciji dokaza na sudu.“ Praksa u starom Rimu kod optuživanja kriminalnih radnji bila je slijedeća: slučaj bi se predstavljao pred grupom javnih osoba na forumu. Potom bi optuženik i tužitelj javnim govorom pokušali uvjeriti ljude kako je njihova verzija događaja istinita, gdje bi se iznosili dokazi, kako materijalni tako i nematerijalnih - latentni (latentno - lat. latens = nevidljiv, sakriven; ono što je

skriveno, a može se pojaviti ako su ispunjeni potrebni uslovi), a potom bi forum donosio presudu. Osnovna zadaća forenzike je pronalaženje, skupljanje i analiza sakrivenih – latentnih dokaza.

U ovo grupu dokaza može se svrstati veliki broj dokaza, ali među najpoznatije latentne dokaze spadaju dokazi kao što su otisak prsta ili DNK profil, nađeni na mjestu učinjenog djela. Pored ovih dokaza u novije vrijeme se kao dokazi koriste i latentni dokazi pronađeni na računarima ili drugim digitalnim uređajima. Forenzika se bazira na provjerenim naučnim metodama i procedurama kako pri otkrivanju, tako i pri čuvanju i analizi nađenih dokaza. Kada se ove metode upotrijebe po utvrđenim standardima i propisanim zakonskim odredbama postaju vrlo važni dokazi za određene istrage. Kao početak forenzike u naučnim krugovima uzima se godina 1248, kada je kineski liječnik Hi Daun Yu napisao knjigu pod imenom „*The washing away of wrong*“. Forenzetika se razvija oko 750 godina i pored toga što je 1904. godine izvršena prva datiloskopija neke osobe, međutim korištenje otiska prsta kao dokaza počelo je u SAD-u tek 1930. godine. Osamdestetih godina XX stoljeća DNK profil je korišten u razne svrhe, a kao valjan dokaz na sudovima DNK profil se koristi tek krajem devedesetih godina XX stoljeća.

Digitalna forenzika je usko polje opšte forenzike i kao disciplina je vrlo mlada, te da bi se digitalni dokazi, koji spadaju u grupu latentnih dokaza, mogli koristiti na sudovima i drugim institucijama, neophodno je uvođenje standardizacije metoda i procedura za skupljanje, čuvanje i analizu digitalnih dokaza. Pored standardizacije procedura i metoda neophodno je izraditi i usvojiti zakonske norme u ovoj oblasti, te na kraju obezbjediti visokostručan i certificiran kadar za rad u ovim oblastima. Treba napomenuti da digitalna i računarska forenzika još nije formalno priznata kao naučna disciplina.

3.1. Digitalna forenzika

Digitalna forenzika je nauka koja ima za cilj prikupljanje, čuvanje, pronalaženje, analizu i dokumentovanje digitalnih dokaza tj. podataka koji su skladišteni, obrađivani ili prenošeni u digitalnom obliku.

Svrha i cilj digitalne forenzike je istraživanje i analiza računara u svrhu prikupljanja dokaza, a to mogu biti podatci pronađeni na medijima za pohranu digitalnih uređaja kojima su izvršene ilegalne radnje ili su bili meta ilegalnih radnji. Također, pronađeni dokazi mogu upućivati na konkretne ilegalne radnje osumnjičenih osoba, a te se radnje ne moraju vezati direktno za računar.

Računar se koriste više od pola stoljeća, ali se tek s pojavom personalnih računara, početkom osamdesetih godina prošloga stoljeća, povećava stopa digitalnog (računarskog) kriminala. S napretkom digitalne tehnologije raste i broj slučajeva zloupotrebe osobnih i poslovnih računara, mobitela, računarskih mreža, kreditnih kartica i sl. Primjeri zloupotrebe kreću se od povrede autorskih prava, industrijske špijunaže, poslovnih prevara,

preko ilegalnih bankovnih transakcija, napada na računarske sisteme i krivotvorina, pa sve do dječje pornografije. Kao i u gore spomenutom slučaju, podaci koji se nalaze na digitalnim uređajima ili medijima za pohranu mogu se prilikom istrage iskoristiti u svrhu pronalaženja krivca.

Digitalna forenzika u svijetu postoji već desetljećima, a na našem području također bilježi impresivne rezultate uz eminentne stručnjake na tom području. Potrebno je neprestano usavršavati svoje znanje te ulagati u nove vještine i alate koji su neophodni da bi se uspješno odgovorilo na veliki porast *cyber* kriminala.

Kompleksnost problema na koje forenzičari nailaze uvjetovali su specijaliziranje stručnjaka za različita područja.

Tako se digitalna forenziku može podijeliti na:

- računarsku forenziku,
- forenziku mobilnih uređaja,
- mrežnu forenziku,
- forenziku baza podataka.

Računarska forenzika je grana forenzičke nauke koja se bavi prikupljanjem, pretraživanjem, zaštitom i analizom dokaza u digitalnom obliku te uključuje njihovu prezentaciju kao materijalnih dokaza u kasnijim eventualnim sudskim postupcima.

Forenzika mobilnih uređaja uključuje skup metoda pretraživanja dokaza s mobilnih uređaja. Posebno se pažnje pridaje načinu forenzičke pohrane memorije mobilnog uređaja, odnosno stvaranju memorijske slike uređaja. Memorijska slika može biti dokaz i koristiti se za daljnju istragu

Mrežna forenzika se bavi upotrebom naučno dokazanih tehnika za prikupljanje, identifikaciju, pretraživanje, povezivanje, analizu i dokumentaciju digitalnih dokaza iz više aktivnih digitalnih izvora koji odašilju i primaju podatke u svrhu otkrivanja činjenica vezanih uz planiranje i uspješno obavljanje kriminalnih radnji.

Forenzika baza podataka se bavi pretraživanjem i analizom baza podataka ili posebnih transakcija i relacija (eng. *tables*) izvučenih iz baze na način koji ne uništava podatke u svrhu rekonstrukcije podataka ili događaja koji su se zbili u sistemu. Prilikom prikupljanja baza podataka za analizu one se obavezno moraju kopirati te se analiza mora obaviti na kopiji izvorne baze kako bi otkriveni dokazi bili prihvatljivi u eventualnom sudskom procesu. Forenzička analiza baze podataka može uključivati vremenske zapise o ažuriranju zapisa u relaciji kako bi se utvrdile akcije korisnika baze. Osim toga, forenzički pregled može biti usredotočen na identificiranje transakcija u sustavu baze podataka ili aplikaciji koja sadrži dokaze o kriminalnim radnjama, kao što je pronevjera novca.

U naprednijim sredinama forenzičari se bave određenim operativnim sistemom, specijaliziraju se za Windows, Linux, Mac OS. Forenzičar, kao uostalom i svi

informatičari, mora redovno pratiti razvoj tehnologije. Razlike između različitih inačica istog programa, a pogotovo operativnog sistema često su suštinske prirode.

Forenzičar, slijedeći strogo uredžena pravila, prikuplja medije za koje sumnja da se na njima nalaze dokazi za kojim traga, osigurava ih od bilo kakvih promjena, pronalazi eventualne dokaze i radi analizu kako bi rekonstruisao aktivnosti koje su vršene nad njima i pripremio razumljiv izvještaj koji će moći poslužiti za vođenje sudskog procesa ili interne istrage u kompaniji.

Kao zanimljiv primjer možemo navesti sljedeće. Digitalni forenzičari, surađujući s jednim od najvećih odvjetničkih ureda u SAD-u, pronašli su više od 30 hiljada povjerljivih podataka snimljenih na dva CD-a. Forenzičari su pokušali otvoriti dokumente, ali neuspješno. Zaključili su da su podatci ili šifrirani i sažeti pomoću računarskog programa ili su toliko oštećeni da su nečitljivi.

Daljnjim pretraživanjem i analizom, pronađen je GIF dokument koji ima nestandardno zaglavlje koje sprječava njegovo otvaranje. Nakon popravka zaglavlja GIF-a, forenzičari su u njemu pronašli informaciju koja je omogućila otvaranje svih 30 hiljada dokumenata.

Digitalna forenzika ima široku primjenu i nije ograničena samo na policijsko-sudske i vojno-obavještajne aktivnosti. Bankarski sektor, osiguravajuća društva i kompanije raznih profila imaju potrebu i moraju biti izuzetno oprezni sa podacima kojima raspolažu jer je mnogim kompanijama nanesena nemjerljiva šteta zbog industrijske špijunaže i generalno zloupotrebe IT sistema. Napad uvijek ima veći izgled za uspjeh ako se izvede iznutra i zato ozbiljne kompanije ne štede truda ni novca da se zaštite od insidera koji su spremni raditi za konkurenciju ili nanijeti štetu iz drugih njima poznatih razloga. Ovdje forenzička istraga dolazi do punog izražaja.

Digitalna forenzika je skup naučno dokazanih metoda i specijaliziranih alata za identifikaciju, prikupljanje, očuvanje, pretraživanje, interpretaciju, analizu i prezentaciju dokaza koji su povezani s rekonstrukcijom ilegalne upotrebe računara, istraživanjem podataka, potvrđivanjem autentičnosti podataka ili pružanjem objašnjenja tehničkih mogućnosti podataka i računarskog korištenja. Ko, što, gdje i kako - pitanja su na koja digitalni forenzičar mora odgovoriti prilikom istrage.

Digitalna forenzika primjenjuje se prilikom prikupljanja dokaza u krivičnim postupcima i pravnim slučajevima gdje policija i sudski vještaci analiziraju digitalne uređaje i medije za pohranu koji pripadaju optuženicima. Unutar poslovnih sistema, forenzika se može koristiti za prikupljanje dokaza protiv zaposlenika za koje se sumnja da su se bavili nedozvoljenim aktivnostima ili za analizu napada na računarske sisteme, kako bi se identifikovao počinitelj i procijenila učinjena šteta. Spašavanje podataka i utvrđivanje grešaka u radu računarskih programa još je jedan primjer upotrebe digitalne forenzike.

Ovisno o razlogu istrage, forenzičar će se fokusirati na određeni dio informacijskog sistema, računara, operacijskog sistema, memorije, podataka, medija za pohranu itd. Dokaze koje može pronaći digitalni forenzičar najčešće nije moguće otkriti standardnim alatima operacijskog sistema, već su potrebni specijalizirani forenzički alati koji mogu pretraživati i analizirati podatke skrivene običnim korisnicima. Kako bi otkrio dokaze,

digitalni forenzičar mora dobro poznavati arhitekturu i način rada sistema i uređaja koje ispituje te biti vješt u rekonstruiranju događaja na osnovu otkrivenih dokaza.

Dokazi i podaci, relevantni za istragu, mogu se pronaći u tekstualnim dokumentima, slikovnim i video datotekama, elektroničkoj pošti, kalendarima, bazama podataka, sažetim dokumentima, sigurnosnim kopijama, skrivenim ili šifriranim dokumentima, konfiguracijskim podatcima, kolačićima, sistemskim zapisima (engl. *logs*), SMS i MMS porukama, popisima poziva, mrežnim paketima, swap i privremenim datotekama, zapisima internetskog preglednika itd.

Razvoj digitalne tehnologije i njeno svakodnevno korištenje povećava porast računarskih zločina i potrebu za što boljom sigurnosti računara kako bi se spriječili bilo kakvi incidenti. Stručnjaci digitalne forenzike, uz temeljna znanja forenzičkih metoda, moraju neprekidno proširivati svoje znanje i usavršavati računarske vještine kako bi uvijek bili jedan korak ispred počinitelja.

Digitalna forenzika vještina je analize elektronički zapisanih podataka, bilo da se oni nalaze na tvrdom disku računara, USB memoriji, mobitelu, igraćoj konzoli, video-kameri ili bilo kojem drugom elektroničkom uređaju. Svi ti uređaji u sebi nose podatke, razne zapisane datoteke, razne (mjesecima, pa čak i godinama prije) obrisane datoteke, lozinke, slike, filmove, šifrirane podatke, skrivene podatke te evidenciju o tome koje programe, aplikacije i podatke je osoba koja se koristi tim uređajem rabila. Sve to može biti dokaz na sudu u slučajevima kao što su povreda intelektualnog vlasništva, industrijska špijunaža, hakerski napadi, ucjena, korupcija, prevara, dječja pornografija, terorizam, razvod braka s problematičnim posljedicama, itd.

Međutim, kako bi neki digitalni zapis bio priznat na sudu mora imati nedvojben slijed sticanja. To zapravo znači da mora biti jasno kako se do tog podatka došlo, ko je tom dokazu pristupao, što je s dokaznim materijalom rađeno, itd.

Dakle, kad digitalni forenzičar izvadi tvrdi disk iz kriminalčevog računara mora ga nekoliko puta zrcalno (bit po bit) umnožiti, a ne samo kopirati podatke, a sam tvrdi disk mora pospremiti na sigurno. Pri samom pregledu podataka na kopiranom tvrdom disku (memorijskom čipu, mobitelu, kameri, bilo kojem drugom elektroničkom uređaju) treba paziti da se ne napravi nešto što bi uticala na podatke koji služe kao dokaz u slučaju.

Primjerice, svako pokretanje standardnog računara automatski mijenja stotinjak raznih podatka koje korisnik ne vidi, no koji mogu uticati na integritet pojedinih datoteka pa čak ih i obrisati. Tako se, na primjer, mogu izgubiti datumi koje treba precizno odrediti da bi se rasvijetlio istraživani slučaj.

Pri analizi dokaza digitalni forenzičari služe se raznim alatima - softverima i bazama podataka. Tu je prije svega riječ o posebnim računarskim programima za digitalnu forenziku koji pomno pretražuju sve što se nalazi na dotičnom uređaju. Ponekad je riječ o hiljadama datoteka. Svaku treba pomno pregledati. I tu nije samo riječ o tekstovima, slikama i video zapisima. Tu su i zapisi o tome kada i gdje je sumnjivac pristupao

Internetu, koliko dugo je bio online, što je gledao, s kim je kontaktirao e-poštom i putem društvenih mreža, kad i kako se koristio internetskim bankarstvom. Računalo iz njegova automobila može nam reći gdje je to vozilo sve bilo.

Šta je s mobitelima? Bolje da ne znate šta se sve može doznati iz tog uređaja od kojeg se danas gotovo nikada ne odvajamo. Dokazi koji se mogu izvući metodama digitalne forenzike koju smo ovdje opisali tek toliko da objasnimo bit te funkcije i struke, često su upravo oni dokazi na kojima advokati dobivaju slučaj. Papiri se gube, svjedoci zaboravljaju ili mijenjaju iskaz, no podaci koji se prikupe metodama digitalne forenzike ne mogu se osporiti jer su rezultat naučnih metoda istraživanja.

Detektivska agencija Mreža specijalizirala se za forenziku mobilnih uređaja. Koristimo najsofisticiranije softvere na svijetu za forenziku mobilnih uređaja. Naši klijenti su podjednako kako korporacije, koje nastoje zaštiti svoj poslovni uspjeh, siguran protok informacija te provjeriti i osigurati svoj sigurnosni sustav od hakerskih napada, tako i fizičke osobe koje dolaze s klasičnim pitanjima, a koja se odnose na vraćanje izbrisanih poruka, vraćanje izbrisanih slika, vraćanje izbrisanih dokumenata, provjere sigurnosti mobilnih uređaja.

4. Razlika između informacionih tehnologija i računarskih nauka

U samoj osnovi, Računarske nauke i Informacione tehnologije se ne razlikuju kada se pominju uopšteno, a za to postoji dobar razlog: mnogi ljudi smatraju da to znači manje više isto. Međutim, u strogoj računarskoj terminologiji, ta dva izraza se zaista razlikuju.[3]

Računarske nauke se odnose na procese koji se koriste za izradu upotrebljivih računarskih programa i aplikacija zajedno sa svom teorijom koja stoji iza tih procesa. Na drugoj strani, Informacione tehnologije se odnose na primjenu računarskih programa u rješavanju poslovnih procesa, tj. na primjenu tehnologije u poslovanju. Informacione tehnologije su veoma široke u smislu opsega zato što se primjenjuju praktično na svaku vrstu procesa koji može da zahtjeva automatizaciju, počevši od poslovanja, naučnog istraživanja do muzičke industrije, telekomunikacija i bankarstva.

Ova dva izraza mogu također da se razlikuju u zavisnosti od škole ili fakulteta, gdje u nekim školama koriste jedan od ovih izraza za nastavni predmet u kojem su kombinovani moduli iz Informacionih tehnologija i iz Računarskih nauka. U školama koje su pretežno inženjerski usmjerene, koristiće izraz računarske nauke kao 'kišobran' za svu teoriju koja se odnosi na informacione tehnologije. U tim slučajevima, oni izraz 'računarsko inženjerstvo' obično koriste za proces izrade računarskih programa, kako na sistemskom tako i na aplikacijskom nivou.

Skoro u svim školama, predmet računarskih nauka obuhvata učenje o računarskom programiranju što znači učenje osnova metodologije programiranja, struktura podataka, algoritama, teorije kompleksnosti pa sve do učenja kako funkcioniše operativni sistem,

[3] https://www.raf.edu.rs

mada se u predmetu računarskih nauka, programiranje nižeg nivoa obično ne izučava toliko detaljno kao u predmetu računarskog inženjerstva.

Posmatrajući računarstvo u globalu, najbolje je da ove izraze organizujemo hijerarhijski. Na nižem nivou imamo računarsko inženjerstvo koje se na nivou 'čipova' bavi unutrašnjim strujnim kolima, strujom i elektronikom računara. Slijedi nivo računarskih nauka koji je dosta širok, pošto će računarski naučnik zaista biti upoznat sa materijom nižeg nivoa u računarskom inženjerstvu, a također i sa programiranjem višeg nivoa koje se povezuje sa čipovima i kolima kako bi mašine radile. Zatim su na višem nivou Informacione tehnologije koje se koncentrišu na proučavanje aplikacija ili rešenja razvijena na prethodnom nivou. Informacione tehnologije pronalaze načine da se ta rešenja integrišu u radni okvir poslovanja.

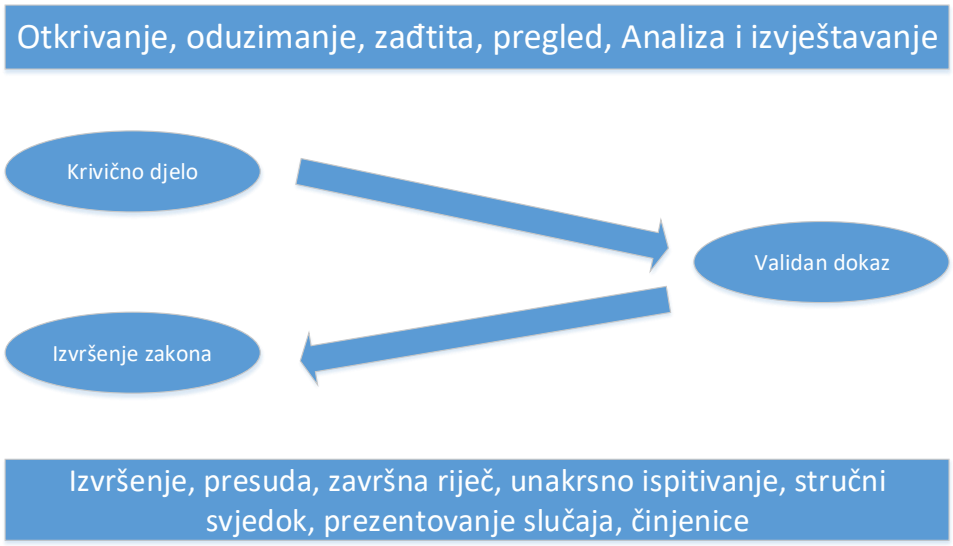
Dakle ;

- računarske nauke se odnose na procese koji se koriste za izradu računarskih programa, dok se Informacione tehnologije odnose na primjenu tih programa u poslovanju.
- u računarskoj terminologiji, Računarske nauke su na 'nižem nivou' dok su Informacione tehnologije na višem nivou.
- informacione tehnologije integrišu računarske nauke u svijet poslovanja, kada su potrebna automatizovana rešenja.
- računarski naučnici treba da poznaju funkcionisanje računara na nižem nivou dok za Informacione tehnologije to nije neophodno.

4.1. Računarska i digitalna forenzika

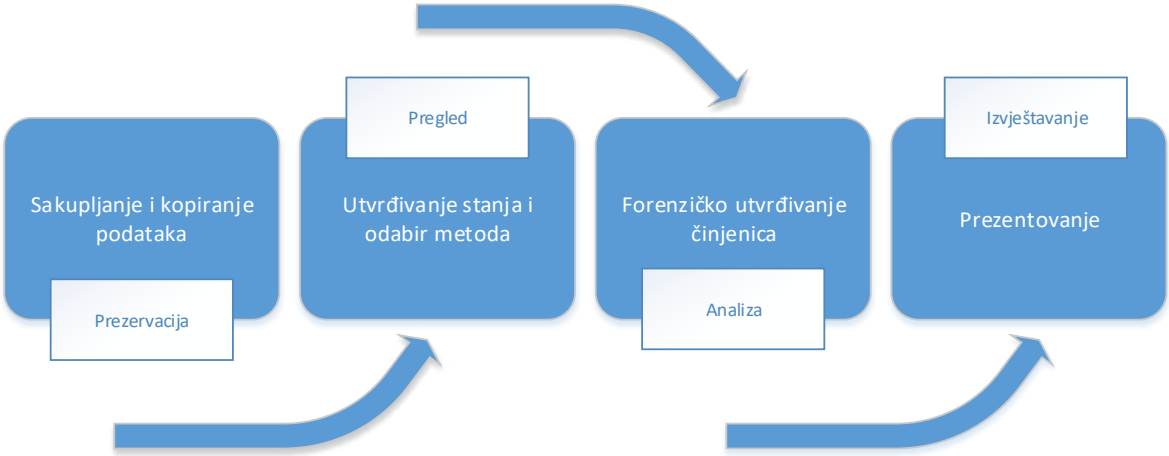
Računarska i digitalna forenzika predstavljaju proces istrage sa ciljem utvrđivanja ilegalnih aktivnosti koje dovode do krivičnog djela. Ovaj proces istrage, odnosno računarsku i digitalnu forenziku, sačinjavaju metode prikupljanja, pohranjivanja (čuvanja), analize i prezentacije dokaza, koji se mogu pronaći na personalnim računarima, serverima, radnim stanicama, prenosnim medijima, računarskim mrežama, bazama podataka, mobilnim uređajima, te svim drugim informatičkim i digitalnim uređajima koji imaju mogućnost obrade, prenosa ili skladištenja (čuvanja) podataka u elektronskom obliku.[4] Proces istrage mora se bazirati na naučno provjerenim metodama i zakonski propisanim procedurama. Podaci koji su prikupljeni na ovim osnovima tek tada mogu i imaju vrijednost dokaza na sudskim i drugim procesima kao što su građanski procesi ili disciplinski procesi unutar preduzeća i ustanova u postupcima upravljanja ljudskim resursima.

[4]Doc.dr. Jasmin Azemović *; CSI::SQL server: „Metode kontrole pristupa"* , FIT, Mostar, 2011.



Ilustracija 1 - Shematski prikaz procesa istrage

Obzirom da sudski organi traže validne podatke vrlo je važno da se sačuva oprema kojom se je vršilo prikupljanje podataka, također vrlo je važno sačuvati procedure ili da ne dođe do promjene podataka na istraživanom uređaju.



Ilustracija 2 - Faze elektronske istrage

Dakle, svi računarski sistemi i digitalni uređaju sadržavaju velike količine podataka koji se mogu iskoristiti kao dokazi. Računarski istražitelji - forenzičari istražuju sve medije za pohranu i čuvanje podataka (*HDD, USB Drives, CD/DVD ROM, Tape Drives* itd.) sa osnovnim ciljem pronalaženja, prikupljanja i analiziranja podataka koji će postati validni dokazi. Računarska forenzika je možda neadekvatan naziv za današnji stepen razvoja informatičkih tehnologija. Ovaj naziv bio je adekvatan dok je u upotrebi bio samo računar. Danas za ovaj nivo razvoja informatičkih tehnologija, interneta, globalizacije računarskih mreža i na kraju sve veća upotreba digitalnih uređaja ove metode istrage mogu se nazvati ***„cyber-forenzika“.*** Naime, mjesto izvršenja dijela ne može se više vezati za računar i sto na kojem je smješten računar. Istrage se proširuju u virtualni svijet, u svijet Interneta, globalnih i lokalnih mreža, i dalje proširuju na ostale digitalne uređaje (mobilne aparate,

GPS, digitalne fotoaparate, digitalne kamere i sl.). Pojam "digitalni dokaz" računarskom, mrežnom mediju ili digitalnom mediju za pohranu podataka, uključujući uzorke teksta, slike, videa, glasa. Digitalni računarski dokaz čini gomila posrednih stvarnih dokaza, od kojih se ni jedan ne smije isključiti. Dokazi moraju biti potpuni, da se međusobno dopunjuju (da su isprepleteni) i da nemaju tzv. pukotina za donošenje zaključaka, odnosno za utvrđivanje čvrstog dokaza. Prema SWGDE[5] termin „dokaz" se upotrebljava za „nešto materijalno" što će biti priznato od strane suda. On mora biti prikupljen na legalan i zakonit način. Neki objekat (podatak ili materijalna stvar) postaje dokazom jedino, kada u njega povjeruje sud koji je ustanova zadužena za provođenje zakona. Prema istoj organizaciji pojam digitalnog dokaza predstavlja svaka informacija ili dokaz koji ima vrijednost koja je u digitalnoj formi.

4.2. Pravila forenzike digitalnih sistema

Uzimajući u obzir složenost problematike i posljedice koje mogu nastati korištenjem elektronskih podataka kao dokaza na sudu, preduzećima ili drugim agencijama za provođenje zakona, potrebno je da metodologija, pravila i procedure računarske forenzetike moraju biti jasna i striktno definisana. Bitno je naglasiti da metodologije koje se primjenjuju u ovoj oblasti moraju biti naučno osnovane, a procedure i pravila zakonski definisana. Da bi se počelo sa radom prikupljanja podataka neophodno je:

- **prvi korak,** obezbijediti validan nalog (tužilaštva) ili dozvolu od vlasnika uređaja koji je predmet istrage.
- **drugi korak,** obezbjeđuje se forenzetička kopija jer se istraga vodi na forenzetičkoj kopiji, nikad na orginalu, jer se orginal čuva na odgovarajući način,
- **treći korak** je izračunavanje matematičkom metodom (*hashing* funkcijom) jedinstvene vrijednosti podataka koja se mijenja u slučaju bilo kakve pa i najmanje promjene na podacima koji se istražuju. Dobijena vrijednost podataka zove sa *hash* vrijednost podataka. *Hash* funkcije ima definiciju: funkcija svakom elementu domene pridružuje jedan i samo jedan član kodomene. Međutim takva funkcija nije bijekcija (jedan na jedan) jer više različitih članova domene ima pridružen isti član domene, ovo praktično znači ako su dva izlaza dobijena različite vrrijednosti onda su i ulazi različiti, engl. *hash* znači sjeckati ili miješati, upravo ta funkcija to radi sa podacima. Ovo nam obezbjeđuje da je kopija na kojoj vršimo istragu autentična orginalu.
- **četvrti korak,** istraga se provodi provjerenim i priznatim forenzetičkim alatima (softver i hardver)
- **peti korak, forenzička analiza podataka,** pri čemu su prva četiri koraka su bili samo priprema za obezbjeđenje validnih podataka i ovim korakom počinje pravi posao.

[5] SWGDE - The *Scientific Working Group on Digital Evidence*

- **šesti korak**, sačinjavanje izvještaja, koji treba da je pregledan, jasan i bez suvišnih podataka
- **sedmi korak,** obezbjeđenje mogućnosti za ponavljanje procedura kojima je se došlo do nekog rezultata
- **osmi korak**, prezentacija rezultata analize na sudu ili pred nekim upravljačkim organom koji je naručio analizu.

Navedeni koraci moraju se poštovati ukoliko izostavimo bilo koji korak šteta može biti puno veća i može se odmah dovesti u pitanje valjanost dobijenih dokaza. Posebno se ovo odnosi na dokaze koji se prezentiraju na sudu u nekom krivičnom postupku. Moramo biti svjesni da druga strana traži formalne razloge da te dokaze ne prihvati.

5. Pravni izvori digitalne istrage

U razvijenom dijelu svijeta ulažu se ogromna sredstva kako bi borba protiv *cyber* kriminala polako počela da sustiže nivo širenja samih kriminalnih djela. U SAD je situacija specifična, jer oko 80% stanovništva koristi Internet kod kuće. U takvoj Internet džungli, naravno, postoji i veliki broj zloupotreba, pa su Amerikanci formirali posebna operativna odeljenja za borbu protiv računarskog kriminala u okviru FBI, CIA i tužilaštva. Međutim i pored ovolikog antikriminalnog angažovanja, u SAD priznaju da su rezultati za sada nezadovoljavajući i da je broj otkrivenih djela minimalan. Ovaj američki "minimalan" broj za naše pojmove zapravo znači da "pljušte optužbe". Skoriji primjer je velika akcija američke Savezne komisije za trgovinu (FTC) i nekoliko drugih Vladinih agencija, koje su pokrenule 45 sudskih procesa protiv osoba koje su se bavile raznim vidovima kriminalne aktivnosti na Internetu. Pored tužbi protiv pojedinaca, najveća tužba podnijeta je protiv kompanije „Alyon Technologies", koja je ilegalno preusmjeravala korisnike Interneta na svoju vezu i pokušala da im to naplati.

U još jednom razvijenom dijelu svijeta, Evropskoj Uniji, situacija nije ništa povoljnija. Još prije nekoliko godina se na ministarskom nivou EU upozoravalo da treba što prije uvesti nove zakone, kako bi se zaustavio brzorastući kriminal koji se širi Internetom, a uključuje razne prevarante i raspirivače dječije pornografije. Tada je ocijenjeno da su neusaglašeni zakoni u mnogim državama – ono što omogućava takvo kriminalno djelovanje. Sve je dugo bilo samo na nivou priče, do skoro. Naime, zemlje EU su dobile prvo "tijelo" koje će djelovati na cijelom prostoru Unije – Agenciju za mrežnu i informacionu bezbijednost. Ova agencija je počela sa radom 1. januara 2004. godine i za period do 31. decembra 2008. godine odobren joj je budžet od 24,3 miliona eura. Jedan od glavnih zadataka Agencije bit će pomoć organima za borbu protiv računarskog kriminala zemalja članica, posebno njihovim timovima za hitno reagovanje.

Zašto je potreban zakonski i pravni okvir za istragu računarskog kriminala? Formalna procedura je neophodna za složeni zadatak istraživanja slučajeva računarskog kriminala: projektni plan; biznis plan, program, vremenski plan, budžet, kadrovi. Krajnji

cilj je prikupiti dovoljno informacija da se kriminalni akt dokaže pred sudom. Nažalost konzistentna tehnologija neophodna za rješenje računarskog kriminala ne postoji. Treba znati da svaki upadač u IS ostavlja trag, bez obzira koliko težak za praćenje. Svaki računarski kriminal je rješiv uz veliko strpljenje i dovoljno znanja. Istraživanje i gonjenje računarskog kriminala zahtijeva vrijeme i novac, pa vješti ekspert može odužiti proceduru u nedogled. Zato je potrebna formalna struktuirana, zakonski i pravno zasnovana, procedura istrage računarskog kriminala.

U najjednostavnijem slučaju zakonski okvir za istragu računarskog kriminala mora obezbijediti proceduru za vođenje istrage o računarskom kriminalu. Što je jasnije definisan proces istrage u računarskom kriminalu, to je veća vjerovatnoća za uspiješan ishod istrage. Najsigurniji istražni postupak u slučaju računarskog kriminala je tipa korak po korak. Prvo se mora donijeti zaključak da je žrtva napadnuta – procijeniti incident. Značajno je u kružnom procesu menadžmenta računarskog incidenta, na osnovu rezultata istrage zatvoriti sve bezbjednosne rupe koje se otkriju u sistemu zaštite i time poboljšati otpornost IS na napade.

Proces istrage nije jednostavan niti isti za sve tipove kriminala, ali postoje neke sličnosti svi tipovi zahtijevaju strukturu istražnog procesa, profesionalce koji razumiju predmetnu tehnologiju i profesionalce koji vode istražni postupak. Obje ove sposobnosti se rijetko mogu naći u jednoj osobi. Svi tipovi računarskog kriminala zahtijevaju odgovore na 5 pitanja: ko, šta, gdje, kada i zašto?

5.1. Međunarodni pravni izvori

Od posebnog značaja za oblast računarskog kriminala su Konvencija UN protiv transnacionalnog organizovanog kriminala sa dopunskim protokolima, Palermo, 2000., kao i Konvencija Savjeta Evrope o računarskom kriminalu (*Cybercrime*), usvojena u Budimpešti, 23. novembra 2001. godine. Palermo Konvencija predstavlja značajan napredak u globalnom određenju – definisanju transnacionalnog organizovanog kriminala i utvrđivanju promjena koje države treba da sprovedu u okviru svog krivičnog zakonodavstva, da bi suprostavljanje organizovanom kriminalu bilo efikasnije. Njeno donošenje poslijedica je, prije svega, opšteg povezivanja država i regiona na ekonomsko–finansijskom planu, čime je organizovani kriminal dobio mnogo širi prostor za djelovanje. Konvencija Savjeta Evrope o računarskom kriminalu (*Cybercrime*), predstavlja u odnosu na Palermo konvenciju, kada je u pitanju računarski kriminal, konkretizaciju mjera koje treba preduzeti u cilju gonjenja učinilaca krivičnih djela iz predmetne oblasti. Kako se to navodi već u preambuli Cybercrime Konvencije, jedan od razloga za njeno donošenje, jeste uvjerenje da efikasna borba protiv računarskog kriminala zahtijeva uvećanu, brzu i funkcionalnu međunarodnu saradnju u krivičnim stvarima.

Konvencijom Savjeta Evrope definiše se nekoliko aktivnosti, koje, ukoliko se počine sa predumišljajem, predstavljaju prestupe u oblasti računarskog kriminala za koje se predviđaju kazne:

- Namjeran pristup bez dozvole bilo kom računarskom sistemu kao cjelini ili nekom njegovom dijelu.
- Namjerno presretanje, bez dozvole, prenosa računarskih podataka koji nisu namijenjeni javnosti.
- Namjerno oštećivanje, brisanje, kvarenje, mijenjanje ili prikrivanje računarskih podataka bez dozvole.
- Namjerno i ozbiljno ometanje funkcionisanja računarskog sistema unošenjem, prenošenjem, oštećivanjem, brisanjem, kvarenjem, mijenjanjem ili prikrivanjem računarskih podataka.
- Proizvodnja, prodaja, nabavljanje radi upotrebe, uvoz ili distribucija sredstava namenjenih za izvršavanje bilo kog navedenog zločina, ili lozinki ili sličnih podataka koji se koriste za pristup računarskim sistemima, sa namjerom da se počini neki navedeni zločin.
- Namjerno unošenje, mijenjanje, brisanje ili prikrivanje računarskih podataka kojim dolazi do stvaranja podataka koji nisu izvorni sa namjerom da ovi podaci budu prihvaćeni kao da su izvorni.
- Namjerno unošenje, mijenjanje, brisanje ili prikrivanje računarskih podataka ili bilo kakvo miješanje u rad računarskog sistema sa nepoštenom namjerom da se pribavi lična ekonomska korist.

Kršenje autorskih prava, definisanih u zakonima zemlje članice koji se odnose na obaveze koje je ona preuzela po Pariškom aktu od 24. jula 1971. o Konvenciji iz Berna o zaštiti literalnih i umetničkih djela, zatim po Ugovoru o komercijalnim aspektima prava na intelektualnu svojinu i WIPO (*World Intellectual Property Organization*) ugovoru o autorskim pravima od 14. maja 1967., kad je to djelo učinjeno pomoću računarskih sistema. Članom 12 se definiše i građanska, administrativna ili krivična odgovornost pravnih lica, ukoliko je računarsko kriminalno djelo učinjeno od strane fizičkog lica radeći po njihovom nahođenju ili u ime organizacije ili usled nepostojanja nadzora ili kontrole od strane rukovodećeg lica čime je omogućeno izvršavanje računarskog kriminalnog djela.

5.2. Zakoni u BiH i računarska, digitalna i cyber forenzika

Zloupotreba, neovlašteni pristup i korištenje elektronskih podataka sa informatičkih sistema i digitalnih uređaja zove se računarski kriminal. Međutim, posjedovanje i korištenje ovih podataka nije uvijek predstavljao akt kršenja formalnog prava. Uviđajući do kakvih negativnih posljedica po opštu i ličnu sigurnost može dovesti neovlašteno preuzimanje i korištenje podataka koji su preuzeti sa informatičkih sistema i digitalnih uređaja. U 1977. godini potekla je inicijativa da se uspostavi pojam računarskog kriminala. Inicijativa je potekla od U.S. Senate Government Operations Committee-a. Interpol je bio

prva međunarodna organizacija koja se bavila problemom računarskog kriminala i legislative. U izvještaju sa Interpolove konferencije održane 1981. godine, prvi put obrađen je problem računarskog kriminala, te legislative, identificirani su potencijalni problemi. Vijeće Europe je 1985. uspostavilo još jedan komitet sastavljen od eksperata, kako bi se razgovaralo o računarskom kriminalu. Dok su 1989. godine donesene i konkretne preporuke. UN je 1990. godine donio i rezoluciju o računarskom kriminalu. Rezolucija je postala veoma bitan element kod pisanja strategija ili Zakona o računarskom kriminalu u EU, skoro sve zemlje iz Europe su potpisale ovu rezoluciju. Bosna i Hercegovina ovu rezoluciju je prihvatila i potpisala 2006.godine. Za ilustraciju povećanja računarskog kriminala neka posluže ovi podaci, tako je u 70-im godinama dvadesetog stoljeća u SAD zabilježeno oko 500 krivičnih djela uz pomoć računara ili informacionih tehnologija. U 90-im godinama dvadesetog stoljeća nastaje veliki porast ovih krivičnih djela, povećanje je bilo u takvom obimu da klasične laboratorije za vještačenje su bile preopterećene za vještačenja, tako da metod off-line pregledanja zaplijenjenog materijala (izuzeti dokazi i uređaji, vještačenje se vrši u specijaliziranim laboratorijama) nije bio dovoljno brz i efikasan tako da se prešlo na metod on-line, koji znači da su se počinioci hvatali na djelu, naime istražitelji su prešli u *cyber* prostor. U tabeli 1 i 2 dat je pregled članova krivičnih zakona u BiH koji se odnose na ovu oblast.

Član Zakona	Opis krivičnog djela	Minimalna kazna	Maksimalna kazna
Član 393.	Oštećenje računarskih programa i podataka	Novčana	5 godina zatvora
Član 394.	Računarsko krivotvorenje	Novčana	5 godina zatvora
Član 395.	Računarska prevara	6 mjeseci zatvora	12 godina zatvora
Član 396.	Ometanje rada sistema i mreže obrade elektronskih podataka	Novčana	3 godine zatvora
Član 397.	Neovlašteni pristupzaštićenom sistemu i mreži elektronske obrade podataka	Novčana	5 godina zatvora
Član 398.	Računarska sabotaža	1 godina zatvora	8 godina zatvora

Tabela 1 - Pregled članova Krivičnog zakona Federacije BiH koji se odnose na računarski kriminal

Član Zakona	Opis krivičnog djela	Minimalna kazna	Maksimalna kazna
Član 176	Neovlašteno korištenje ličnih podataka	Novčana	1 godina zatvora
Član 238	Neovlašteno ulaženje u zaštićenu kompjutersku bazu podataka	1 godina zatvora	8 godina zatvora
Član 271	Upad u računarski sistem	6 mjeseci zatvora	10 godina zatvora
Član 276	Falsifikovanje kreditnih kartica za bezgotovinsko plaćanje	Novčana	10 godina zatvora

Tabela 2 - Pregled članova krivičnog zakona Republike Srpske koji se odnose na računarski kriminal

Tada i nastaje pojam ***cyber forenzika,*** koja je kompleksnija i savršenija od računarske forenzike. *Cyber* forenzika je kompleksnija od računarske forenzike zato što se dokazi pronalaze u računarskim mrežama, na internetu, i čak u drugim dijelovima svijeta. Porast *cyber* kriminal neka ilustruje podatak da je u 2004. godini, neovlaštenim korištenjem elektronskih podataka u SAD-u zarađeno oko 105 milijardi dolara

Uvidjevši opasnost od širenja ovog kriminala, a posebno je podstaknuto širenjem upotrebe interneta. U cilju ispunjavanja obaveza iz rezolucije UN i obaveza koje je morala ispuniti prema zahtjevima Europske unije u smislu usklađivanja zakona sa normama koje važe u EU, Bosna i Hercegovina je izvršila dopunu Kaznenog Zakona Federacije Bosne i Hercegovine i Krivičnog Zakona Republike Srpske sa nekoliko članova zakona koji se odnose na krivična djela računarskog, digitalnog i *cyber* kriminala i na taj način sankcionisala ovo krivično djelo.

6. Steganografija

Steganografija (od Grčkih riječi *steganos* i *graphein – u prevodu bi značilo skriveno pisanje*) se koristi u raznim formama preko 2500 godina. Ima svoju upotrebu u vojsci, diplomatiji, kriminalu, terorizmu. Ukratko, steganografija je izraz koji se odnosi na bilo koji broj postupaka koji će sakriti poruku unutar nekog objekta, gdje skrivena poruka neće biti očita posmatraču.

U današnje vrijeme, steganografija se povezuje sa prikrivanjem informacija ili poruka unutar računarskih datoteka kao što su slike, audio i video sadržaji. Za razliku od kriptografije, koja obrađuje informaciju na način da samo odabrana osoba ili osobe mogu pročitati njen sadržaj, glavni cilj steganografije jeste skrivanje poruke. Dakle, u slučaju kriptografije postojanje poruke je evidentno, dok sa steganografijom samo postojanje poruke je skriveno. Iako su ovo dvije odvojene discipline, one se često koriste zajedno kako bi se informacija dodatno osigurala.

6.1. Kako sakriti informaciju

Osnovni zahtjev u steganografiji jeste da poruka nije vidljiva. Klasična steganografija informacije sakriva unutar tzv. LSB odnosno najmanje značajnih bita. To su biti koji, ukoliko se njihova vrijednost izmjeni, neće značajno uticati na izvornu datoteku. Kod datoteke koja sadrži sliku, moguće je izmijeniti redundantne bite koji sadrže informacije o boji. Promjenom ovih bita unosi se degradaciju u sliku, ali s obzirom da je ljudsko oko mnogo osjetljivije na osvjetljenje nego na intenzitet boje, ta degradacija neće biti vidljiva ljudskog oku.

Međutim, korištenjem određenih algoritama i analiziranjem datoteka, mogu se uočiti nepravilnosti koje mogu sugerirati da se u datoj datoteci nalazi dodatna, skrivena informacija. Zbog toga, u ovom radu će biti predstavljena i metoda pomoću koje je moguće prenijeti informaciju koristeći sliku uz minimalnu degradaciju. Štaviše, degradacija slike je nula.

Ilustracija 3 - Orginal slika

Ilustracija 4 - Stego slika

6.2. Steganografija kroz historiju

Jedan od prvih primjera steganografije je povezan sa Grkom Histiaeus-om. Naime, Histiaeus je bio zarobljenik svoga suparnika. Pokušavao je da pronađe način kako da pošalje poruku svojoj armiji. Njegovo rješenje je bilo obrijati glavu jednom njegovom podaniku, te na njoj „istetovirati“ poruku. Nakon što je podanikova kosa ponovo narasla, prenio je sakrivenu poruku.

Trithemius, njemački naučnik, izdao je 1499. godine knjigu pod nazivom *Steganographia,* jednu od prvih knjiga koja je proučavala steganografiju. Međutim, steganografija se spominje još i u vrijeme antičkoga Rima, kada se koristi tehnike poput nevidljive tinte. Steganografija je postala aktualna i u drugom svjetskom ratu. Njemačka vojska je koristila mikro-tačke. Na prvi pogled obične tačke u rečenicu zapravo su služile za prikrivanje informacija.

Danas, može se reći da je doba elektronske steganografije. Poruke i informacije se skrivaju u kompjuterskim datotekama koje se mogu razmjenjivati putem Interneta. Štaviše, upravo je Internet i omogućio korištenje steganografskih metoda običnom čovjeku. Širom

Interneta, mnogi steganografski softver alati su dostupni svakome, a veliki broj njih je i besplatan.

7. Proces forenzičke istrage digitalnih dokaza

Osnovni zadatak pri otkrivanju i dokazivanju kriminalnog djela je da se utvrdi činjenično stanje i da se prikupe dokazi potrebni za preduzimanje odgovarajućih mera protiv počinilaca krivičnog djela.

Rješavanje svakog problema, pa i računarskog kriminala, obuhvata slijedeće faze:

- otkrivanje računarskog kriminalnog djela i počinioca
- rješavanje i dokazivanje računarskog kriminalnog djela

7.1. Otkrivanje djela i počinioca

Do saznanja o računarskom kriminalnom djelu može se doći na više načina, među kojima su najčešći:

- anonimne i pseudonimne prijave
- Nadzor i kontrola

Kao izvor informacija o izvršenoj zloupotrebi mogu da posluže i anonimne ili pseudonimne prijave, koje nikako ne treba bezrezervno prihvatati, ali ni olako odbaciti, dok se ne izvrši provjera njihove istinitosti.

Ipak, nadzorne i kontrolne procedure predstavljaju svakako najpouzdaniji način otkrivanja i sprečavanja svih oblika ilegalnih aktivnosti, pod uslovom da su dobro osmišljene, cjelovite i permanentne, sa predvidivom i nepredvidivom dinamikom. Postoji izvjestan broj osnovnih indicija koje mogu ukazati na postojanje nekog računarskog kriminalnog djela. Pod indicijama se u kriminalistici podrazumijevaju činjenice koje svojim značenjem upućuju na mogućnost postojanja delikta i učinioca.

Za uspješnu identifikaciju problema potreban je uvid u određene evidencije, datoteke i baze podataka, testiranje nekih programa, provjera nekih podataka, obavljanje razgovora sa jednim ili više neposrednih izvršilaca i dr. Pri tome, sve vrijeme treba voditi računa da se ne otkrije sumnja, jer očuvanje tajnosti u ovakvim situacijama je od vitalnog značaja. Dalja analiza slučaja podrazumijeva utvrđivanje prirode i obima kriminalnog djela, tj. da li se radi o jednokratnoj akciji ili jednoj iz niza sličnih; da li je u pitanju jedan ili više učinilaca; da li su djela učinjena iznutra ili spolja; kolika je približna vrijednost izazvanog gubitka i koje i kakve negativne posljedice se zbog toga mogu očekivati.

Nakon identifikovanja i analize slučaja, prelazi se na njegovo rješavanje, koje se može sprovesti interno, u okviru radne organizacije ili prijavom nadležnim organima. U svijetu postoji praksa internog rješavanja računarskih kriminalnih djela, što nepovoljno utiče na globalnu borbu protiv računarskog kriminala, jer mnogi oblici ispoljavanja računarskog kriminala na ovaj način i dalje ostaju nepoznanica, pa se stoga ne mogu pravno sankcionisati.

7.2. Održivi podaci

Primarni izvor ovakvih podataka na OS je *filesystem*. *Filesystem* je jedan od informaciono najbogatijih izvora za digitalnog forenzičara.

Slijedi nekoliko vrsta podataka koje je moguće pronaći u OS *filesystem*-u:

- **Configuration files** poseduju informacije o listi servisa za startovanje, lokaciji log i privremenih fajlova, kao i o hardverskim podešavanjima (štampači, rezolucija, itd..)
- **Logs files** sadrže informacije o raznim događajima na OS i događajima vezanim za aplikacije. Tipovi informacija: *System* events-svi događaji vezani za OS, Audit *records*-uspešna/neuspešna provjera identiteta, *Application events*-promjene konfiguracije OS, *Command history*-istorija komandi za svakog korisnika, *Recently accessed files*-hronološka lista fajlova kojima se pristupalo
- **Application files** – sadrže različite tipove podataka: Izvršne skripte, Dokumentaciju, Konfiguracione fajlove, Log fajlove, Istoriju datoteke, Slike, Zvukove, Dokumentaciju
- **Data files –** Sadrže skladištene informacije za aplikaciju. Uobičajne datoteke: Tekstualni fajlovi, Tabele, Baze podataka, Audio fajlove, Grafičke fajlove.
- **Swap files –** Uloga *swap* fajlova je da proširi RAM memoriju. Koristi se za privremeno skladištenje podataka. *Swap* fajlovi sadrže: Informacije o OS, Informacije o aplikaciji, Korisnička imena, Heševe lozinki, Kontakt informacije.
- **Dumpfiles –** Fajlovi podataka koji nastaju u momentu nastanka greške u radu neke aplikacije (radi rješavanja problema).
- **Hibernationfiles** – čuvaju informaciju o trenutnom stanju sistema. Bilježi stanje memorije i otvorenih fajlova,
- **Temporary files** – Tokom instalacije softvera na OS se kreiraju privremeni fajlovi koji se nakon uspješnog procesa automatski brišu. Ovi fajlovi ne budu obrisani uvijek, a mogu da sadrže različite tipove informacija.

7.3. Neodrživi podaci

Podaci u RAM memoriji.

Podaci se konstantno mijenjaju u toku rada OS.

RAM *Slack space*–Slično kao i kod drugih medija, aplikacije nekad zahtijevaju više memorije nego što stvarno koriste (bolje performanse).

RAM *Free space* – Slično kao i kod drugih medija, memorijski prostor je oslobođen, ali i dalje se nalaze podaci u vidu smeća.

Postoje i drugi izvori neodrživih podataka na OS.

- **Network configuration** –IP adrese, domen.
- **Network connections** –analiza ip adrese i portova za dolazni i odlazni saobraćaj na OS-u
- **Running processes** –na osnovu liste OS procesa moguće je analizirati ponašanje korisnika.
- **Open files** –analiza OS liste otvorenih fajlova.
- **Login sessions**–informacije o trenutno logovanim korisnicima, trajanju sesije, praćenje navika korisnika, analiza aktivnosti korisnika u vreme događaja.
- **Operating system time**-tačno vreme i vremenske zone, vreme na OS i vreme u BIOS-u mogu da se razlikuju zbog vremenskih zona.

7.4. Razjašnjavanje i dokazivanje računarskih kriminalnih djela

Sa razvojem informaciono-komunikacione tehnologije (ICT) počinju i prvi sudski procesi. Kratak pregled historije sudskih procesa prikazan je u tabeli.

Godina	zemlja	događaj
1977.	SAD	Sudski slučajevi u kojima se javljao kompjuter: -291 na federalnom nivou -246 na nivou federalnih država
1980.	SAD	Nastaje Kompjuterska forenzika
1991.	SAD	Kompjuterska forenzika dobija pravo građnstva
1991.	SAD, Portland	Zasjedanje International Association of Computer Specijalists, IACS. Računarski prikupljeni dokazi ravnopravni i validni kao i bilo koji drugi
1991.	SAD, Južna Karolina	Predstavnici 6 međunarodnih agencija susrelo se sa predstavnicima američkih federalnih agencija da prodiskutuju o kompjuterskoj forenzici i potrebi za standardizacijom postupaka kod računarskih istraga.
1993.	SAD	FBI je bio domaćin Međunarodne konferencije o računarskim dokazima na kojoj je bilo preko 70

		predstavnika raznih državnih i međunarodnih agencija.
2000.	SAD	Najznačajniji slučaj Simon Property Group v. mySimon Inc. Prvi put se pojavljuje računarski forenzičar, na zahtev jedne strane, koji će nakon istrage podneti izvještaj sudu, a sud će ga priznati kao validan
2001.	SAD	Prihvaćena Pravila vezana za elektronske dokaze (Rules of Electronic evidence) od strane Vrhovnog suda SAD

Tabela 3 - Kratak pregled historije sudskih procesa

Računa se da je sada preko 90% svih dokumenata u elektronskoj formi, a da preko 70% nikada nije ni bilo u papirnoj verziji. Usavršavaju se i postepeno odvajaju nove od tradicionalnih forenzičkih disciplina. Napuštaju se klasične laboratorije i istrage se prenose istovremeno u virtualni i realni svijet. Počinje korištenje direktnih digitalnih informacija i podataka koji su značajni za slučaj, za razliku od drugih djela kod kojih su u pitanju njihove interpretacije. Uobičajeni alati koje ovi forenzičari koriste su softverski, često isti oni koje upotrebljavaju i počinioci, mada se u novije vrijeme sve više koriste posebni, za te namjene dizajnirani. Elektronski dokumentovani dokazi su onaj specifikum koji ih prati. Oni istovremeno služe za dokazivanje i utvrđivanje slabosti sistema sigurnosti i mogućnosti dolaženja do posebno osjetljivih i važnih podataka (npr. do sadržaja elektronske pošte pomoću kojih se utvrđuju namjere i motivi za određene kriminalne aktivnosti i ponašanja). Ti elektronski dokazi, pored prednosti imaju niz nedostataka, a krucijalni je da se lako prilagođavaju potrebi i često rutinski brišu, prikrivaju.

Ne ulazeći u raspravu koji kompjuterizovani dokazi mogu ili ne mogu biti prihvatljivi za sud, jer je to još uvijek otvoreno pitanje, što zavisi od vrste i prirode slučaja, navesti ćemo one koji se najčešće javljaju:

- tekuće i neko prethodno stanje podataka i programa (tekuća i *back-up* stanja), sistemska statistika i evidencije (različiti računarski dnevnici (*log*-ovi), dnevnici transakcija, žurnali, obračunski zapisi),
- kontrolni izvještaji,
- štampani izvještaji (listinzi),
- ručne evidencije,
- radni nalozi,
- izjave pojedinih radnika i dr

7.5. SOP – Standard Operation Procedure[6]

Da bi se osigurala bezbjedna akvizicija (otkrivanje, fiksiranje i uzimanje), menadžment (skupljanje, čuvanje i prenos) i forenzička analiza digitalnih dokaza i da bi se sačuvale tačnost i pouzdanost dokaza, zvanični istražni organi i privatne institucije za forenzičku analizu digitalnih dokaza, moraju uspostaviti i održavati efikasni sistem

[6] http://www.ijces.com/ - International Journal of Computer Engineering Science

kontrole kvaliteta. Standardna radna procedura (SOP–Standard Operation Procedure) je dokumentovano uputstvo za kontrolu kvaliteta cjelokupnog postupka istrage, akvizicije, menadžmenta i forenzičke analize digitalnih dokaza. SOP mora obuhvatiti propisno registrovanje svih aktivnosti istrage računarskog incidenta, kao i korištenje drugih, u kriminalistici široko prihvaćenih procedura, opreme i materijala.

Kada se formulišu standardne radne procedure (SOP's) treba razmatrati slijedeće elemente:

- Naslov – treba da bude opisno ime za proceduru
- Namjena – zašto, kada i ko koristi proceduru
- Oprema/materijal/Standardi/kontrole- identifikuje koji se predmeti zahtijevaju za izvršavanje procedure. Ovo može uključiti opremu za zaštitu, hardver, softver i konfigurisanje.
- Procedure – opis korak-po-korak kako se procedura izvodi. Ako je neophodno procedura treba da sadrži mjere opreza koje treba preduzeti da se minimizira degradacija.
- Kalibracija – opisuje svaki korak koji se zahtjeva da osigura tačnost i pouzdanost procedure. Gdje je primjenjivo, treba dokumentovati podešavanje instrumenata i kalibracionu proceduru.
- Kalkulacija - opisuje bilo koju matematičku operaciju koja je primenjena u proceduri.
- Ograničenja – opisuje sve akcije, interpretacije, ili opremu koja nije odgovarajuća za proceduru.
- Sigurnost- identifikuje i adresira potencijalne hazarde kod korištenja procedure.
- Reference- identifikuje dokumenta interna i eksterna za agenciju koja se koristi u pogledu procedure, koja se odnosi na proceduru i principe iza njih.

7.6. Standardi i kriterijumi:

a) Sve agencije koje zapljenjuju i/ili ispituju digitalnu opremu moraju voditi i održavati odgovarajući SOP dokument, potpisan od strane menadžerskog autoriteta i koji sadrži jasno definisane sve elemente politike i procedura. SOP mora biti obavezna za zvanične i druge forenzičke organe zbog prihvatanja rezultata i zaključaka na sudu.
b) Menadžment agencije mora revidirati SOP jedanput godišnje da obezbijede neprekidnost njihove efikasnosti i pogodnosti za primjenu, zbog brzih tehnološki promjena.
c) Korištene procedure moraju biti generalno prihvaćene u oblasti forenzičke analize digitalnih dokaza i da ih u akviziciji, analizi i čuvanju podržavaju naučne metode. U izboru metoda evaluacije naučne vrijednosti tehnika i procedura mora se biti

fleksibilan. Validnost procedure treba uspostavljati demonstriranjem tačnosti i pouzdanosti specifične tehnike (korisna je javna naučna rasprava).

d) Agencija mora posjedovati pisanu kopiju odgovarajućih tehničkih procedura koje koristi u radu. Potrebni hardverski i softverski elementi alata moraju biti navedeni u spisku uz opis propisanih koraka za upotrebu i jasno navedena sva ograničenja upotrebe tehnika i alata. Lica koja primjenjuju procedure moraju biti dobro upoznata sa njima i dobro obučena za rad sa korištenim alatima. Agencija mora koristiti adekvatne hardverske i softverske alate koji su efikasni za realizaciju procedura akvizicije i/ili analize digitalnih dokaza. Treba biti dovoljno fleksibilan u pogledu raznovrsnosti izbora metoda koje su najbolje za konkretni problem. Hardverski i softverski alati za akviziciju i/ili analizu digitalnih dokaza moraju biti testirani i sa važećim certifikatom o verifikaciji funkcionalnog kvaliteta nadležne nacionalne institucije i moraju biti u dobrom radnom stanju.

e) Sve aktivnosti koje se odnose na akviziciju (zapljenu), skladištenje, ispitivanje, prijenos digitalnih dokaza moraju biti registrovane u pisanoj formi i na raspolaganju za pregled i svjedočenje. Generalno dokumentacija koja podržava zaključke forenzičke analize moraju biti tako pripremljeni da ih drugo kompetentno lice može iznijeti i u odsustvu orginalnog autora. Mora se uspostaviti i održavati lanac čuvanja dokaza za sve digitalne dokaze. Stalno se moraju voditi pisane zabilješke i zapažanja o slučaju (mastilom ili dijagrami u kolor hemijskoj olovci) sa inicijalima autora kod svake korekcije (precrtane jednom crtom). Svaka zabilješka mora biti lično potpisana, sa inicijalima ili DS ili drugom identifikacionom oznakom autora. Bilo koja akcija koja ima potencijal da izmijeni, ošteti ili uništi bilo koji aspekt originalnog dokaza mora se izvršavati od strane kvalifikovanog lica na forenzički ispravan način. Svaki način mora biti potvrđeno tačan, pouzdan i kontrolabilan. Obučeno forenzičko osoblje mora koristiti kvalitetne forenzičke programe i odgovarajuću opremu.

7.7. Procedure za pronalaženje i zapljenu računara

1. Snimiti na forenzički računar sve logove svih dokaza uzetih na mjestu kriminalnog djela
2. Dati detaljne informacije o vlasniku kompromitovane kompjuterske opreme
3. Izraditi detaljan izvještaj sa opisom svih preduzetih akcija
4. Pratiti ček listu aktivnosti iz procedure istrage na mjestu kriminalnog akta
5. Jedina sigurnost za integritet podataka je kredibilitet ispitivača, koji ima znanje i iskustvo za propisno procesiranje elektronskih dokaza.
6. Detaljan izvještaj o procesiranju i strukturi osumnjičenog HDD
7. Identifikacioni materijal, imena i serijski brojevi sve korištene opreme i računarskih programa.
8. Izvještaj o slučaju koji sadrži što više informacija.
9. Uspostavljanje i održavanje lanca čuvanja, kao i za druge tipove dokaza.

10. Čuvati elektronske dokaze u propisanom okruženju (temperaturnom, vlažnosti, prašine, magnetskih polja, i.t.d.)
11. Identifikacino označavanje svih ostalih medija za skladištenje (osim HD) kao što su trake, kertridži printerski, zip ili flopi diskovi, CD ROM, DVD treba označiti prema slijedećem:
    - Podaci certifikovani/testirani/ispitani
    - Ime ispitivača-analitičara
    - Zaštita diska od upisivanja prije pregleda, kopiranja, analize kopije (ne originala), antivirusno skeniranje
    - Označiti svaku disketu sa a-1, a-2, i.t.d.
    - Odštampati direktorij za svaku disketu
    - Ako se otkriju inkriminisane informacije, odštampati sadržaj fajla i označiti štampani materijal sa istom alfanumeričkom oznakom.

7.8. Procedure za obezbjeđivanje kopija dokaza:

1. Napraviti radnu kopiju originalnog dokaza
2. Odštampati izvještaj sa napravljene kopije, sve dok sadržaj ne postane suviše velik.
3. Sažeti izvještaj, podnijeti kopirani elektronski dokaz
4. Podaci sadržani u memorijskim uređajima i medijima samo za čitanje, ponekad se traže kao dokazi u formi čvrste kopije (printinga)
5. Tehnička prezentacija pred sudom

8. Modeli za forenzičku istragu

8.1. Korporacijski model istrage

Funkcionalni korporacijski model istražnog postupka može se opisati slijedećim fazama:

- Priprema za incident: sa odgovarajućom obukom i infrastrukturom;
- Detekcija incidenta: identifikovati sumnjivi incident;
- Prva reakcija: prepoznati i potvrditi da se incident dogodio, sakupiti preliminarne, nestabilne i posredne dokaze (koji se vremenom degradiraju);
- Formulisanje strategije reakcije: na bazi poznatih indikatora;
- Dupliranje: napraviti fizičku *miror* sliku kompromitovanog sistema;
- Istraga: ispitati sistem radi identifikacije ko, šta i kako je izvršio napad;
- Implementacija mjera zaštite: izolovati kompromitovan sistem prije nego što je vraćen u normalni režim rada;
- Nadzor mreže: posmatrati mrežu radi identifikacije novih (ponovljenih) napada;
- Oporavak: vratiti sistem u originalno stanje sa dodatnim mjerama zaštite;
- Izvještavanje: dokumentovati reakciju na incident (kriminal) i izvijestiti;
- Završna faza: revidirati saniranje incidenta i eventualno poboljšati proces.

8.2. Zvanični model istrage

U SAD Department of Justice objavio je model procesa istrage u Vodiču za istragu elektronskog mjesta krivičnog djela. Vodič odgovara fizičkom mjestu krivičnog djela, tako da je akcenat stavljen na te zahtjeve, a manje pažnje obraća na forenzičku analizu digitalnih sistema. Faze modela su slijedeće:

- **Priprema**: pripremiti opremu i alat potreban za istragu
- **Sakupljanje**: naći i sakupiti elektronske (digitalne) dokaze
- **Osigurati i procijeniti mjesto krivičnog djela**: obezbijediti mjesto radi bezbijednosti lica i integriteta podatka i identifikovati potencijalne dokaze
- **Dokumentovanje**: dokumentovati fizički opis mjesta uključujući fotografije računarskog sistema
- **Sakupljanje dokaza**: (forenzička akvizicija) zaplijeniti fizički računarski sistem, ili napraviti fizičku (*miror*) kopiju podataka na forenzičkom računarskom sistemu
- **Pregled**: tehnički pregled i ispitivanje sistema radi nalaženja potencijalnih dokaza
- **Analiza**: (digitalna forenzička analiza) istražni tim pregleda rezultate tehničkog pregleda radi procijene njihove važnosti za slučaj
- **Izvještaj**: izvještaj se pravi poslije svakog slučaja računarskog (incidenta) kriminala.

Ovaj model je baziran na standardnoj istrazi fizičkog mjesta krivičnog djela i kao i prethodni model, ne obraća mnogo pažnje na proces forenzičke analize digitalnog mjesta krivičnog djela i ne ispunjava zahtjeve modela za proces istrage digitalnih dokaza.

9. Zaključak

U prvom dijelu ovog rada predstavljen je pojam računarskih sistema i osnovne komponente računarske i digitalne forenzike. Objašnjene su metode digitalne forenzike koje sačinjavaju sam proces istrage.

Istaknuto je da se proces istrage mora zasnivati na naučno provjerenim metodama i zakonski propisanim procedurama. U radu je detaljno opisan i dat pregled osnovnih pravila forenzike digitalnih sistema.

Također, ušlo se u problematiku legalnih-zakonskih aspekata digitalne istrage sa strane međunarodno pravnih izvora tako i sa strane zakonske regulative u BiH. Prikazani su članovi koji se odnose na računarski kriminal u krivičnim zakonima Federacije BiH, Republike Srpske i Brčko distrikta, što je vidljivo da je pravno uređena ova oblast u BiH.

Objašnjena je steganografija kao najčešća metoda skrivanja relevantnih dokaza .

Postoje dvije vrste podataka na operativnom sistemu;

- podaci koji postoje nakon gašenja računara-održivi,
- podaci koji ne postoje nakon gašenja računara-neodrživi.

Upravo ove dvije kategorije su od velikog interesa za vođenje forenzičkog postupka.

Primarni izvor održivih podataka je *filesystem. Filesystem* je jedan od informaciono najbogatijih izvora za digitalnog forenzičara.

Opisan je proces forenzičke istrage digitalnih dokaza kao i SOP - Standard Operation Procedure. Objašnjeni su standardi, kriterijumi i procedure za upravljanje dokazima.

U današnjem i budućem vremenu znanje i obrazovanje će predstavljati preduslov razvoja svake ekonomije i globalnog okruženja, a time i razvoj finansijskog tržišta i finansijskih institucija, odnosno adekvatno sprečavanje računarskog kriminala gdje informacione tehnologije u potpunosti ostvaruju svoju funkciju u digitalnoj forenzici.

Literatura

1. Adamović S., Digitalna forenzika, Univerzitet Singidunum, Beograd,
2. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition, by Eoghan Casey, Academic Press © 2004
3. International Journal of Computer Engineering Science - http://www.ijces.com/
4. Krivični zakoni FBiH, Republike Srpske i Brčko distrikta - http://www.tuzilastvobih.gov.ba/
5. First Responders Guide to Computer Forensics, Copyright © 2005 by CERT Training and Education
6. The Computer Forensic Reference Data Sets by NIST - http://www.cfreds.nist.gov/
7. Milosavljević M., Grubor G., (2009), "Digitalna forenzika", Univerzitet Singidunum, Beograd
8. Wasson Charles. System Analysis, Design, and Development: Concepts, Principles, and Practices. John Wiley and Sons. 2005.
9. Solomon David. An Introduction to Computer Security: The NIST Handbook. National Institute of Standards and Technology.2010.
10. Andress Jason. The Basics of Information Security, Springer 2010
11. Solomon David. Elements od Computer Security, Springer Science and Business Media, 2010

Internet adrese:

- http://www.forensicfocus.com/
- http://www.accessdata.com/
- http://racunarskapismenost-wordpress-com.cdn.ampproject.org
- https://www.raf.edu.rs