Mogućnost primjene računalne forenzike kao element sigurnosti informacijsko komunikacijskih sustava

Tomašić, Karlo

Master's thesis / Diplomski rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:016162

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Karlo Tomašić

MOGUĆNOSTI PRIMJENE RAČUNALNE FORENZIKE KAO ELEMENT SIGURNOSTI INFORMACIJSKO KOMUNIKACIJSKIH SUSTAVA

DIPLOMSKI RAD

Zagreb, 2015.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

MOGUĆNOSTI PRIMJENE RAČUNALNE FORENZIKE KAO ELEMENT SIGURNOSTI INFORMACIJSKO KOMUNIKACIJSKIH SUSTAVA

CAPABILITIES OF APPLICATION OF COMPUTER FORENSICS AS SECURITY ISSUE OF THE INFORMATION AND COMMUNICATION SYSTEMS

Mentor: Prof. dr. sc. Dragan Peraković

Student: Karlo Tomašić, 0066155312

Zagreb, 2015.

SAŽETAK

Informacijsko komunikacijski sustavi jedan su od fundamentalnih stupova modernog društva, što znači da su zastupljeni u gotovo svim aspektima istoga, a informacijsko komunikacijske tehnologije predstavljaju tehnološku okosnicu sustava. Svaka tehnologija podložna je zlouporabi, pa se tako informacijsko komunikacijski sustavi koriste i u kriminalne svrhe, a tu na scenu stupa računalna forenzika čiji je cilj identifikacija računalnih kriminalnih radnji, te u idealnom slučaju i preventivno djelovanje naspram istih što je moguće samo ako se prate najsuvremeniji trendovi razvoja informacijsko komunikacijskih tehnologija. Posebno je važno da se postupak računalne forenzike provede metodično uz pridržavanje striktnih pravila prikupljanja i obrade dokaza da bi oni bili prihvaćeni na sudu što je i prikazano.

KLJUČNE RIJEČI: informacijsko komunikacijski sustav; računalni kriminalitet; računalna forenzika;

SUMMARY

Information and communication systems are one of the fundamental pillars of modern society which means that they are represented in nearly all aspects of the society and information and communication technologies constituting a technological backbone of IT system. Each technology can be subject of illegal and criminal abuse, the same is with information and communication systems. In those cases computer forensic comes into play whose goal is to identify cybercrime and, in ideal case, preventive action against cybercrime. This is possible only if most modern trends of information and communication technologies are followed. It is particularly important that process of computer forensics is conduced methodically with abidance of strict rules in gathering and processing of evidences so that they could be accepted in court.

KEY WORDS: information and communication system; cybercrime; computer forensic;

SADRŽAJ

1.UVOD 1
2.SIGURNOST INFORMACIJSKO KOMUNIKACIJSKIH SUSTAVA 4
2.1.Informacijsko komunikacijski sustav 4
2.2.Sigurnost 6
2.3.Prijetnje informacijsko komunikacijskim sustavima 9
3.RAČUNALNA FORENZIKA 13
3.1.Povijest računalne forenzike 13
3.2.Računalni kriminalitet 14
3.2.1.Karakteristike računalnog kriminaliteta 15
3.2.2.Oblici i tipovi računalnog kriminaliteta 15
3.3.Digitalni dokaz 17
4.RAČUNALNA FORENZIČKA ANALIZA 20
4.1. Izrada postupka računalne forenzičke analize 20
4.2. Prikupljanje podataka i dokaza 21
4.2.1. Procjena dokaza 22
4.2.2. Ranjivost dokaza 23
4.2.3. Alati za prikupljanje ranjivih dokaza 24
4.2.4. Logičko i fizičko dohvaćanje podataka s diska 25
4.3. Prikupljanje dokaza na Linux operacijskim sustavima 26
4.3.1. Ispitivanje radne memorije 26
4.3.2. Ispitivanje sadržaja diska 27
4.4. Prikupljanje dokaza na Windows operacijskim sustavima 28
4.4.1. Rekonstrukcija sadržaja „*Recycle Bin*“ direktorija 28
4.4.2. Windows Forensics Toolchest 28
4.5. Analiza dokaznih materijala 29

4.5.1. Analiza vremenskog slijeda 30
4.5.2. Pronalaženje skrivenih podataka 30
4.5.3. Analiza aplikacija i datoteka 30
4.5.4. Analiza vlasništva nad datotekama 31
4.6. Dokumentiranje i izvještavanje 31
4.6.1. Vođenje bilježaka 31
4.6.2. Izvještaj 32
5.PROGRAMSKI ALATI RAČUNALNE FORENZIKE 34
5.1.Alati za analizu programa 35
5.2. Alati za analizu diska 37
5.3.PyFlag 37
5.3.1.Korištenje alata 38
5.3.2.Analiza log zapisa 39
5.3.3.Hash usporedba 41
5.3.4.Priprema tvrdog diska 41
5.3.5. Analiza učitanih podataka 42
5.3.6.Dodatne mogućnosti 43
5.4. The Coroner's Toolkit programski paket 44
5.4.1.Grave-robber 44
5.4.2.Mactime 45
5.4.3. Unrm 46
5.4.4.Lazarus 46
6.CERTIFIKACIJA FORENZIČKIH ISTRAŽITELJA 48
7.ZAKONSKA REGULATIVA I RAČUNALNA FORENZIKA 50
7.1.Konvencija o kibernetičkom kriminalitetu 51
7.2.Stanje u Republici Hrvatskoj 52

8.POSTUPCI RAČUNALNE FORENZIKE UPORABOM ODABRANOG FORENZIČKOG ALATA 54
8.1.Odabir forenzičkog alata – Helix 2009R1 54
8.2.Pokretanje na Windows operacijskim sustavima 56
8.3.Administracijsko sučelje za Windows sustave 57
8.4.Postupak forenzičke analize odabranim alatom 59
8.4.1. Priprema prije istrage 59
8.4.2.Prikupljanje podataka 60
8.4.2.1.Forenzika elektroničke pošte 61
8.4.2.2.Forenzika podataka 63
8.4.2.2.1.Obrisani podaci 65
8.4.2.2.2.Dohvat obrisanih dokumenata 65
8.4.2.2.3.Dohvat obrisanih podataka iz nealociranih prostora 66
8.4.2.2.4.Nepristupačan prostor 66
8.4.2.2.5.Dobava podataka 67
8.4.2.2.6.Analiza dobavljenih podataka 68
8.4.2.3.Forenzika dokumenata 68
8.4.2.3.1.Pronalazak dokaznog materijala u dokumentima: Metapodaci 69
8.4.2.3.2.Pregled CAM informacija 70
8.4.2.3.3.Otkrivanje dokumenata 71
8.4.2.3.4.Pronalazak poveznica i vanjskih medija za pohranu podataka 72
9.ZAKLJUČAK 73
10.LITERATURA 75
POPIS KRATICA 78
POPIS SLIKA 81

1.UVOD

Informacijsko komunikacijski sustavi jedan su od fundamentalnih stupova modernog društva, što znači da su zastupljeni u gotovo svim aspektima istoga, definiraju se kao skup ljudi, programa, metoda i drugih elemenata, organiziranih i povezanih radi obavljanja informacijske aktivnosti, a informacijsko komunikacijske tehnologije predstavljaju tehnološku okosnicu sustava. Informacijsko komunikacijska tehnologija (ICT) obuhvaća računala, komunikacijsku opremu i s njima povezane usluge. Uz sve prednosti koje se vežu uz uporabu informacijsko komunikacijski tehnologiji, postoje i nedostaci. Jedan od glavnih nedostataka je i zlouporaba istih u kriminalne svrhe.

Računalna forenzika je znanost koja se bavi otkrivanjem, sprječavanjem, analiziranjem i istraživanjem računalnih zločina. Područja istraživanja računalne forenzike uključuju web forenziku, forenziku podataka, forenziku dokumenata, mrežnu forenziku te forenziku mobilnih uređaja, odnosno, predmet elektroničke uređaje nad kojim je počinjena kriminalna radnja ili koji je bio alat za izvršenje takve radnje.

Tijekom ispitivanja računalnog sustava potrebno je minimizirati utjecaj na njegovo stanje. To znači da je potrebno izbjegavati njegovo gašenje, pohranu podataka na tvrdom disku, pokretanje aplikacija, mijenjanje mrežnih postavki i sl. Preporuča se korištenje programskih alata pokretanih s medija koji svojim radom ne utječu na ispitivani sustav. Također, prikupljanje dokaza potrebno je započeti dohvaćanjem sadržaja radne memorije te drugih ranjivih podataka.

Računalna forenzika relativno je mlada znanost, pogotovo u Republici Hrvatskoj, unatoč tome, razvija se velikom brzinom iz razloga da bi mogla pratiti suvremene tehnološke trendove koji se posljednjih desetak godina razvijaju i implementiraju.

Naravno, razvojem novih tehnologija, dolazi i do porasta računalnog kriminaliteta, kako u svijetu tako i u Republici Hrvatskoj. Prema podacima 2006. godine šteta prouzročena „cyber“ kriminalom je iznosila 1.45 milijardi USD i po prvi puta je bila veća od vrijednosti ukupnog ilegalnog tržišta droga, dok je 2010. godine iznosila čak 114 milijardi direktne, a 274 milijarde USD indirektne materijalne štete s time da i dalje raste. Nepoznavanje samog pojma digitalnog dokaza, neovisno od straha od novih tehnologija, veoma često je uzrok nesporazuma, nerazumijevanja, nepoznavanja pa u konačnici i pogrešno donošenih zaključaka koji su utjecali i na same presude.

Mnoštvo korisne literature nalazi se na Internetu, na stranicama specijaliziranih udruga i organizacija, kako svjetskih, tako i hrvatskih. Pa tako Bača, Ćosić i Protrka u više navrata pišu stručne članke na temu Računalnog kriminaliteta i prevencije istoga, a koji se objavljuju u časopisu Policija i sigurnost.

Svakako bih spomenuo udžbenik „Digitalna forenzika računarskog sistema“ (Milosavljević, M., Gojko, G. Univerizitet Singidunum, Beograd, 2009.), gdje je tematika računalne forenzike prikazana na iznimno detaljan i sistematičan način, što mi je omogućilo izvrstan uvid u problematiku teme.

Sam rad koncipira je kroz 9 cjelina:

1. Uvod
2. Sigurnost informacijsko komunikacijskih sustava
3. Računalna forenzika
4. Računalna forenzička analiza
5. Programski alati računalne forenzike
6. Certifikacija forenzičkih istražitelja
7. Zakonska regulativa i računalna forenzika
8. Postupci računalne forenzika uporabom odabranog forenzičkog alata
9. Zaključak

Drugo poglavlje pod naslovom „Sigurnost informacijsko komunikacijskog sustava“ objašnjava i prikazuje informacijsko komunikacijski sustav kao cjelinu, zatim je tu objašnjen pojam sigurnosti, te su prikazane i objašnjene prijetnje informacijsko komunikacijskom sustavu.

„Računalna forenzika“ naslov je treće cjeline, te je tu napravljen pregled povijesnog razvoja računalne forenzike, zatim je definiran pojam računalnog kriminaliteta uz neke karakteristike i podjele, te digitalni dokaz kao temelj računalne forenzike.

Četvrto poglavlje, pod naslovom „Računalna forenzička analiza“, logički je nastavak na prethodnu cjelinu. Pa je tako tu definiran postupak izrade računalne forenzičke analize, metodologija prikupljanja podatak i dokaza uz osvrt na dva operacijska sustava (Windows OS i Linux OS). Prikazan je i postupak analize dokaznih materijala, te način vođenja dokumentacije i bilježaka da bi dokazi bili valjani na sudu.

U petom poglavlju, pod nazivom „Programski alati računalne forenzike“, dat je pregled forenzičkih alata, podjela prema svojstvima, te su također ukratko opisana dva forenzička alata – PyFlag i The Coroner's Toolkit.

Šesto poglavlje (Certifikacija forenzičkih istražitelja) bavi se certifikacijom i školovanjem stručnjaka računalne forenzike u Hrvatskoj i svijetu, te važnosti školovanja i certifikacije za sudski proces.

U sedmom poglavlju pod naslovom „Zakonska regulativa i računalna forenzika“, napravljen je osvrt na „Konvenciju o kibernetičkom kriminalu“, te je napravljen prikaz staja računalne forenzike u RH s aspekta zakonodavstva.

Zadnje poglavlje razrade teme, odnosi se na postupak računalne forenzike uz uporabu Helix forenzičkog alata, te sa dodatnim alatima koji nadopunjuju ograničenu funkcionalnost Helixa na Windows 7 operacijskom sustavu.

Očekivani rezultati istraživanja su definicija računalnog kriminala, detaljan prikaz tematike računalne forenzike, njezine mogućnosti, evaluacija sadašnjeg stanja, kako u svijetu tako i u Republici Hrvatskoj, te budući razvoj, zakonski okvir (regulativa i smjernice) i certifikati (edukacija) čime bi se dobio uvid u važnost poštivanja procedure forenzičkih postupaka i edukaciju forenzičkih stručnjaka da bi se u što većoj mjeri spriječio računalni kriminalitet, te da bi se počinitelji uspješno sankcionirali. Zatim pregled nekih od najvažnijih alata za računalnu forenziku, metodologiju računalne forenzike. Želja je ukazati na važnosti koju računalna forenzika ima u otkrivanju i sprečavanju računalnog kriminala, a na kraju i prikaz i analiza praktične primjene pojedinih alata za prikupljanje i analizu dokaza.

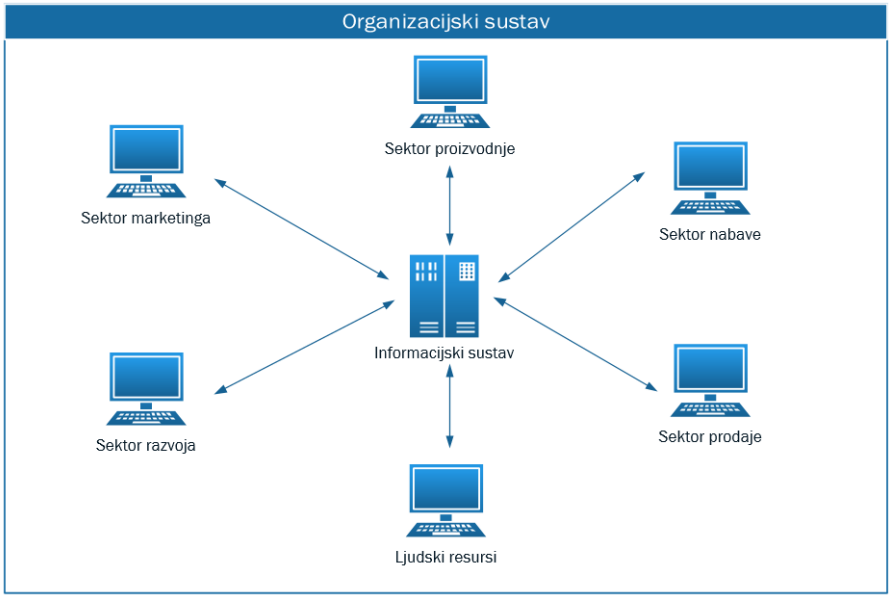
2.SIGURNOST INFORMACIJSKO KOMUNIKACIJSKIH SUSTAVA

2.1.Informacijsko komunikacijski sustav

Informacijsko komunikacijski sustav sastoji se od dva termina, informacijski sustav koji obuhvaća elemente potrebne za prikupljanje, pohranu i obradu podataka, i komunikacijski sustav koji obuhvaća elemente potrebne za prijenos podataka. Praktično gledano, koegzistencija dvaju sustava je nužna te se stoga i koristi jedinstveni naziv [1].

Moguće ga je promatrati i definirati iz dvije perspektive, tehničke i funkcionalne. Iz tehničke perspektive informacijsko komunikacijski sustav sastoji se od krajnjih uređaja, aktivne i pasivne mrežne opreme te podataka i informacija koje se u sklopu promatranog sustava prikupljaju, obrađuju, pohranjuju i prenose, dok definiranje informacijsko komunikacijskog sustava iz funkcionalne perspektive podrazumijeva njegovu ulogu i aktivnosti te zahtjeve u odnosu na organizacijski sustav [3].

Osnovna uloga informacijsko komunikacijskog sustava je povezivanje fizičkih elemenata organizacije (Slika 1.), te omogućavanje njihovog međusobnog komuniciranja u svrhu upravljanja organizacijskim sustavom ili nekim od njegovih podsustava, ali isto tako ima zadaću omogućiti komunikaciju organizacije sa okolinom. Krajnji cilj takvog sustava je dostaviti pravu informaciju na pravo mjesto u pravo vrijeme uz minimalne troškove [1].



Slika 1:Informacijsko komunikacijski sustav kao podsustav organizacijskog sustava [1]

Zbog međusobnog preklapanja u radu i funkcionalnostima, informacijski i komunikacijski sustav moguće je promatrati kroz iste elemente (Slika 2) [2].

Hardware predstavlja sklopovski element IK sustava, odnosno sve materijalne komponente zadužene za aktivnosti ulaza, obrade, pohrane i izlaza, što između ostalog uključuje i [3]:

a) računala,

b) računalne komponente (MBO[1], CPU[2], GPU[3], RAM[4], HDD[5], itd.),

c) računalnu ulazno-izlaznu opremu (miševi, tipkovnice, monitori, pisači, skeneri, itd.),

Software predstavlja nematerijalni element IK sustava u obliku programskih rješenja i operativnih sustava koji se izvršavaju povrh hardverskog elementa.

Lifeware obuhvaća sve osobe koji su ne određeni način povezane sa IK sustavom kao što su projektanti sustava, dizajneri, administratori i krajnji korisnici sustava.

Orgware podrazumijeva organizacijske metode, postupke, procedure i procese temeljem kojih se svi elementi IK sustava povezuju u jedinstvenu, svrsishodnu cjelinu.

Dataware – element IK sustava koji obuhvaća sve podatke koji se prikupljaju, pohranjuju, obrađuju i razmjenjuju unutar organizacijske strukture IK sustava ili sa okolinom.

Netware predstavlja komunikacijski element IK sustava, a obuhvaća aktivnu i pasivnu mrežnu opremu i komponente čiji je cilj omogućiti komunikaciju između uređaja. *Netware* element obuhvaća sljedeće:

a) računalna mrežna oprema (modemi, mrežne kartice, itd.),

b) usmjerivači (engl. *Router),*

c) preklopnici (engl. *Switch*) ,

[1]Eng. motherboard je matična ploča računala.
[2]Eng. central processing unit je centralna procesna jedinica ili procesor računala.
[3]Eng. Graphics processing unit je grafička procesna jedinica računala.
[4]Eng. random-access memory je radna memorija računala.
[5]Eng. hard disk drive je tvrdi disk računala.

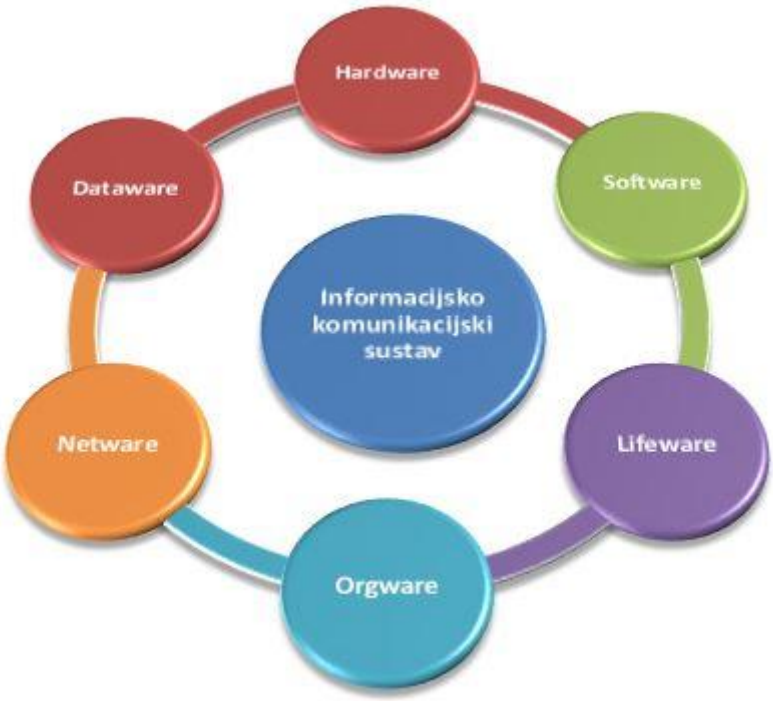
d) obnavljači (engl. *Repeater*),

e) koncentratori (engl. *Hub)*,

f) pristupne točke (engl. *Access Point*),

g) uređaji za zaštitu informacijsko komunikacijskog sustava (vatrozid, sustavi za detekciju i prevenciju napada),

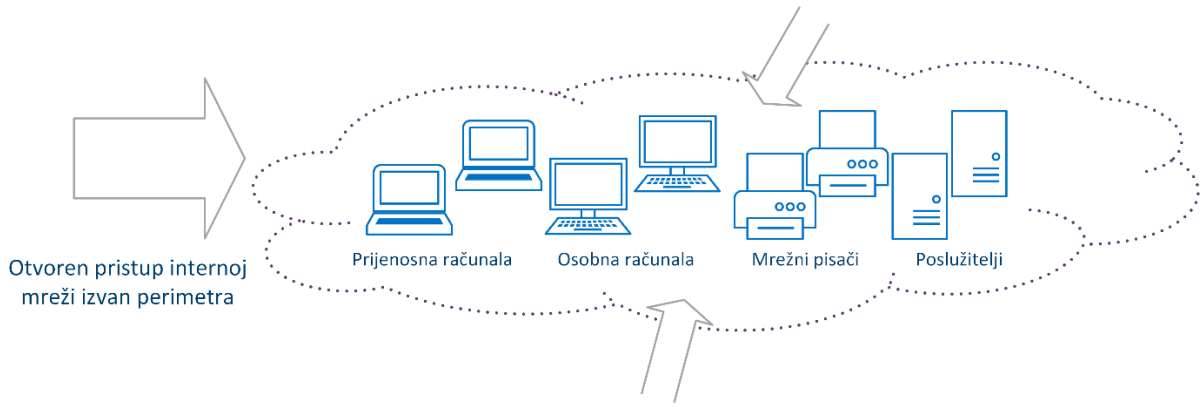
h) prijenosni mediji, itd.



Slika 2: Elementi informacijsko komunikacijskog sustava

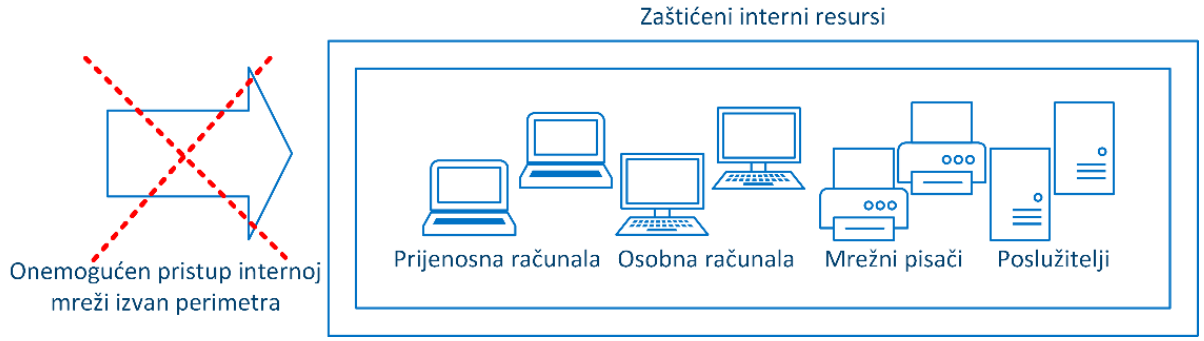
2.2.Sigurnost

Pojavom mrežne komunikacije, računala su bila povezana unutar akademskih ili vladinih okruženja te su mrežne tehnologije razvijane specifično za primjenu u navedenim okruženjima. Izvorno, akademski model sigurnosti (Slika 3.) bio je temeljen na otvorenom pristupu (*wide-open*) dok je model sigurnosti namijenjen vladinim institucijama (Slika 4.) temeljen na zatvorenom pristupu (*closed and lock*) [1].



Slika 3:Akademski otvoreni model informacijske sigurnosti[4]

Unutar okruženja vladinih institucija nastojalo se onemogućiti pristup računalima, ograničiti interni pristup povjerljivim podacima i spriječiti presretanje podataka (primjerice, zaštitom opreme s ciljem sprječavanja presretanja elektromagnetskih zračenja) [3].



Slika 4: Zatvoreni model informacijske sigurnosti [4]

Sigurnost je definirana kao „sposobnost ili mogućnost biti siguran – biti oslobođen od opasnosti“. Biti siguran znači biti zaštićen od protivnika ili drugih prijetnji. Sigurnost je često postignuta sredstvima nekoliko strategija obično pokrenutih istovremeno ili u kombinaciji jedne sa drugom [2].

Sigurnost informacijskih sustava obuhvaća primjenu mjera za zaštitu podataka koji su u obradi, ili su pohranjeni, ili je u tijeku njihov prijenos, od gubitka povjerljivosti, cjelovitosti i raspoloživosti, te radi sprječavanja gubitaka cjelovitosti ili raspoloživosti samih sustava. Sigurnost je moguće definirati i kao održavanje prihvatljive razine rizika, što znači da je sigurnost proces, ne konačno stanje, odnosno konačan proizvod.

Informacijska sigurnost podrazumijeva zaštitu imovine informacijsko komunikacijskog sustava, neovlašteno mijenjanje, brisanje ili otkrivanje osjetljivih informacija organizacije s ciljem očuvanja dostupnosti, integriteta i povjerljivosti informacija i imovine informacijsko komunikacijskog sustava u procesu njegovog planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada [3].

Sigurnosna politika je skup pravila i postupaka kojima se određuje razina sigurnosti nekog informacijskog sustava, istovremeno pridajući pažnju sigurnosti tehnologije i informacija koje informacijski sustav sadrži. Sigurnosnom politikom korisniku se nameću obvezna pravila ponašanja i odgovornosti kako bi se zaštitilo informacijski sustav, tj. informacije pohranjene u informacijskom sustavu, od vanjskih utjecaja (udaljenih napada, zlonamjernih programa, itd.), ali također i korisnika (neovlašteni pristup podacima, krađa podataka, izmjena podataka, itd.) [2].

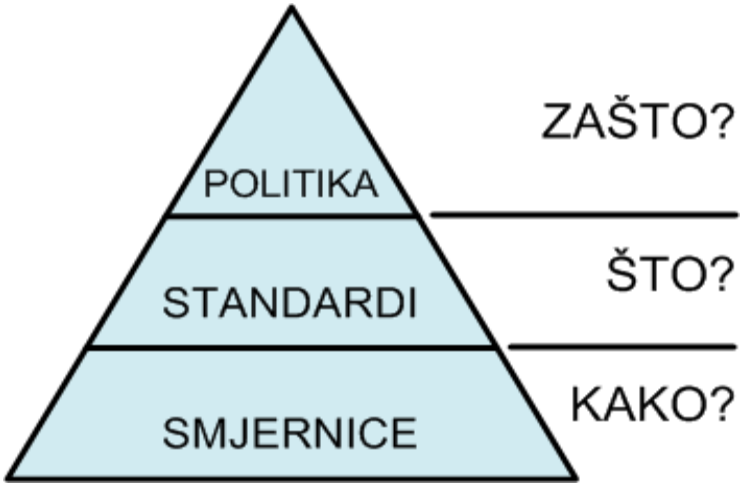
Sigurnosna politika tvrtke ili institucije prilagođava se potrebama, te nije jednaka za sve. Sigurnosnu politiku predstavlja službena izjava ili plan organizacije koji obuhvaća ciljeve, smjernice i prihvatljive postupke. Ona uključuje sljedeće zahtjeve:

- potrebno je poštovati pravila definirana sigurnosnom politikom,
- nepoštivanje pravila može rezultirati sankcijama ili kaznama nadležnih institucija,
- potrebno je usredotočiti se na rezultate, a ne na način provedbe sigurnosne politike i
- određivanje sigurnosne politike se temelji na unaprijed definiranim standardima i smjernicama.

Standard je obvezni postupak ili pravilo koje je izrađeno kako bi učinilo politiku suvislom i učinkovitom, a mora uključivati jedan ili više tehničkih opisa za komponente računala, programe i rukovanje istima. Smjernice su općenite izjave, preporuke ili administrativne upute koje daju okvirne upute za provođenje sigurnosne politike konstruirane kako bi se ostvarili ciljevi sigurnosne politike. Smjernice nisu obvezujuće, one služe više kao pomoć pri uspostavljanju sigurnosne politike.

Smjernice navode najbolje primjere *kako* izvesti nešto, npr. na koji način poboljšati sigurnost nekog informacijskog sustava. Standardi navode koji su osnovni zahtjevi za različite tehnologije i postavke, tj. *što* je potrebno kako bi se sustav postavio prema smjernicama. Sigurnosna politika opisuje kako i *zašto* je potrebno djelovati [4].

Pri oblikovanju sigurnosti nekog informacijskog sustava prvi je postupak uspostavljanje sigurnosne politike, potom slijedi odabir standarda prema kojem će se sigurnosna politika uspostaviti, te na kraju pronalazak smjernica koje će omogućiti učinkovit način provedbe sigurnosne politike. Na slici 5 je prikaz odnos između smjernica, standarda i sigurnosne politike [5].



Slika 5: Prikaz uklapanja smjernica, standarda i sigurnosne politike [5]

2.3.Prijetnje informacijsko komunikacijskim sustavima

Informacijsko komunikacijski sustavi izloženi su velikom broju sigurnosnih prijetnji koje mogu utjecati na integritet podataka i otuđivanje istih, ali jednako tako i financijsku štetu. Razmjeri štete nastale neželjenim aktivnostima mogu biti različitog opsega, od uništenja jedna datoteke, pa do nestajanja cijele baze podataka. Uzročnici neželjenih aktivnosti mogu biti napadači ili legitimni korisnici, zlonamjerni programi, itd.

Prijetnja sigurnosti nekog informacijskog sustava je svaki događaj koji može ishoditi narušavanjem integriteta, pouzdanosti i dostupnosti podataka. Također, važno je spomenuti da svaka prijetnja i neovlašteni pristup informacijskom sustavu, imaju različite posljedice, npr. Uništavanje podataka(točnosti, dostupnosti, itd.) ili narušavanje ispravnog rada cijelog informacijskog sustava [5].

Postoji nekoliko klasifikacija prijetnji informacijskim sustavima, međutim upitno je jedino da li svaka klasifikacija dovoljno detaljno razmatra sve uvjete i mogućnosti nastanka štete na informacijskom sustavu. Važnost detaljne klasifikacije je u pronalasku primjerenih

načina zaštite, te standardizaciji klasifikacije. Prema klasifikaciji NIST-a (***N**ational **I**nstitute of **S**tandards and **T**echnology*) prijetnje informacijskim sustavima se mogu podijeliti na [6]:

1. *Greške i kvarove* - ovu se vrstu prijetnji često podcjenjuje, ali mogu nanijeti značajnu štetu informacijskom sustavu. Najčešći uzrok greškama i kvarovima su ljudske radnje. Mogu ih uzrokovati zaposlenici, proizvođači programskih paketa ili administratori informacijskih sustava. Vjeruje se da je gotovo 65% napada uzrokovano greškama i kvarovima.
2. *Prijevare i krađe* - zlonamjerna aktivnost kojom napadač pokušava steći financijsku ili neki drugi oblik koristi. Prijevare i krađe se mogu dogoditi aktivnostima unutar (zaposlenik) ili izvan(udaljeni napad) organizacije. Međutim, češći su slučajevi aktivnosti prijevare i krađe unutar organizacije koji se događaju u čak 74% slučajeva. Primjerice, zaposlenik ima pristup određenim financijskim podacima i lako može upravljati iznosima koje je potrebno obraditi. Vrlo lako je navesti razloge zbog kojih se prijevare i krađe događaju češće od strane zaposlenika nego udaljenim napadima:
    - zaposlenici imaju pristup podacima i informacijskom sustavu,
    - zaposlenici znaju koje podatke sustav sadrži i koje su sigurnosne provjere i
    - zaposlenici znaju koje su prilike za prijevaru i krađu, te kolika je vrijednost mogućeg plijena.
3. *Sabotažu od strane zaposlenika* - koja je česta prijetnja sigurnosti i podacima informacijskog sustava. Kao što je već naglašeno, zaposlenici imaju pristup, te znaju u kojim dijelovima sustava je moguće prouzročiti najveću štetu. Ako je u pitanju nezadovoljstvo zaposlenika, sabotaža je vrlo čest slučaj, bilo da se radi o sadašnjem ili bivšem zaposleniku. Najčešći primjeri sabotaže su:
    - fizičko uništavanje dijelova informacijskog sustava,
    - postavljanje logičke bombe (*eng. Logicbomb*), tj. zlonamjernog programskog koda čija je namjena izbrisati, premjestiti ili izmijeniti podatke,
    - namjerni unos neispravnih podataka,
    - „rušenje“ informacijskih sustava,
    - brisanje i uništavanje podataka,
    - krađa podataka i ucjena pod prijetnjom otkrivanja tih podataka široj javnosti ili konkurenciji ili
    - namjerno mijenjanje podataka.

4. *Gubitak fizičke i infrastrukturne potpore* - je vrsta prijetnje koju nije moguće u potpunosti provjeriti, ponekad niti spriječiti, a može nanijeti veliku štetu sustavima. Takvi slučajevi mogu biti npr. prekid u opskrbi električnom energijom, prekid komunikacija, poplava, požar, potresi, itd.
5. *Hakere* (*eng. hackers*) - koje se smatra relativno novom vrstom prijetnje informacijskim sustavima koja se nameće kao najopasnija zbog razvoja Interneta i komunikacija, poslovanja i drugih aktivnosti putem Interneta. Napadačem se smatra osoba koja svoje računalno znanje koristi kako bi ugrozila sigurnost računala ili podataka na istom.
6. *Zlonamjerne programe (eng. malware)* - vrsta prijetnje koja narušava sigurnost informacijskog sustava zlonamjernim programima poput crva, virusa, trojanskih konja, logičkih bombi i drugih. Među najčešćim i najopasnijim prijetnjama su virusi, trojanski konji i crvi.
7. *Prijetnje privatnosti korisnika* - postaje vrlo česta prijetnja s obzirom da sve veći broj informacijskih sustava sadrži velik broj osobnih podataka korisnika. Primjeri takvih ustanova su banke, državne institucije i sve veći broj tvrtki.

Također, vrijedno je spomenuti i klasifikaciju prema ISO/IEC 27002:2013 standardu (*Code of Practice for Information Security Management*) koji definira ispravne i sigurne načine upravljanja nekim informacijskim sustavom. Prijetnje su podijeljene obzirom na uzroke nastanka [5]:

1. *prirodne katastrofe* - sve pojave koje su nepredvidive ili ih je nemoguće provjeriti, npr. potresi, poplave, oluje, zagađenja, požari, itd.
2. *tehnički uzroci* - tehničke greške, kvarovi, komunikacijske greške, različiti oblici zračenja, itd.
3. *nenamjerne ljudske radnje* - neposlušnost, kršenje pravila, upotreba neprimjerenih programa, itd.
4. *namjerne ljudske radnje* - uništavanje, sabotaža, špijunaža, ratna razaranja, prijevara, krađa, zlonamjerni programi, itd.

Cyber Security Institute (CSI) je naveo vrlo jednostavnu klasifikaciju prijetnji, obzirom na poziciju prijetnje u odnosu na poziciju informacijskog sustava, tj. prijetnje je podijelio na unutarnje ivanjske. Unutarnjim prijetnjama smatraju se sve namjerne i nenamjerne radnje korisnika koji imaju izravan pristup informacijskom sustavu. Vanjske prijetnje su definirane

kao svi pokušaji nanošenja bilo kakvog oblika štete udaljenim napadima ili ubacivanjem zlonamjernih programa u informacijski sustav sa udaljenih lokacija [7].

3.RAČUNALNA FORENZIKA

„Computer Forensics is simply the application of computer investigation and analysis techniques in the interest of determining potential legal evidence.“

Judd Robbinson

Računalna forenzika predstavlja relativno novo polje znanosti i tokom godina je dobivala razne nazive poput „digitalna forenzika“ i „analiza medija“. Tek prije nekoliko godina prepoznata je činjenica da svi digitalni uređaji ostavljaju fragmente informacija. Ovi fragmenti predstavljaju značajan dokaz u raznim vrstama istraga. Interes za ovu problematiku se prvo javio kod profesionalaca iz oblasti kaznenog prava i sigurnosno obavještajnih službi, dok su informatičari i civilno pravo sa entuzijazmom prihvatili ovaj novi izvor informacija [9].

Računalna forenzike, je dio forenzičke znanosti koji se odnosi na obradu legalnih dokaza pronađenih u računalu i digitalnim medijima za pohranu podataka. Sam pojam „forenzika“ je nastao od latinske riječi „*forensi“* što znači „*na otvorenom prostoru ili javno*“, a što dolazi od riječi „forum“ koja upućuje na lokaciju (javne površine koje su se upotrebljavale za suđenja ili neke druge javne poslove). Značenje je kasnije preraslo u „ znanstveni testovi i tehnike koje se upotrebljavaju za otkrivanje kriminala“ [8].

Računalna forenzika spada u forenzičke znanosti, a bavi se istraživanjem računalnih sustava, kao što su osobna i prijenosna računala, mobilni telefoni, digitalne kamere, vanjski diskovi, GPS uređaji, mrežni uređaji pa čak i uređaji za kopiranje ukoliko imaju internu memoriju. Standardno se dijeli na slijedeće grane [9]:

- forenzika podataka (eng. *data forensics*)
- forenzika dokumenata (eng. *document forensics*)
- mrežna forenzika (eng. *network forensics*)
- forenzika mobilnih uređaja (eng. *mobile forensics*)
- e-mail i web forenzika

3.1.Povijest računalne forenzike

Računalna forenzika se kao znanost razvila relativno kasno, te spada u mlađe znanstvene grane. Sama forenzika vuče korijene još iz Rimskog doba kada su kaznene prijave podrazumijevale javno iznošenje slučaja na Forumu, gdje bi osoba optuženo za kazneno djelo i podnositelj prijave javno raspravljali o tome, a osoba sa boljim argumentom bi pobijedila [8].

Prva škola forenzike je otvorena u Europi u *Lausanne* (Švicarska) i to od strane Rudolpha Archibalda Reissa. Što se tiče digitalne forenzike povijest je malo drugačija. Sama računala su se pojavili tek sredinom 20.stoljeća, te tada još uvijek nije postojao internet i digitalni kriminalitet, pa za forenzikom tog tipa nije bilo potrebe.

Početkom osamdesetih godina, kada osobna računala postaju sve pristupačnija, dolazi do njihove sve veće zloupotrebe, tj do povećanja upotrebe računala prilikom izvršenja kriminalnih radnji. Zbog toga je FBI (eng.*The Federal Bureau of Investigation*) 1984. godine oformio novu jedinicu *Computer Analysis and Response Team* (CART) koja je imala za cilj da se izbori sa sve većim brojem slučajeva koji su uključivali digitalne dokaze [10].

ASCLD – LAB (eng. *American Society of Crime Laboratory Directors / Laboratory Accreditation Bord***)** društvo je 2003 godine prihvatilo pojam digitalne forenzike i značaj digitalnog dokaza u rješavanju zločina. Kanada je prva zemlja koja je 1983. godine donijela zakon koji djelomično regulira digitalni zločin, nakon nje je slijedila Amerika 1986.godine, zatim Australija 1989.godine, a potom i Engleska 1990. godine. Danas u Sjedinjenim Američkim Državama postoji više desetaka kolegija na sveučilištima koji su specijalizirani za tematiku računalne forenzike [6].

Prvi zabilježen napad na digitalnu infrastrukturu se dogodio 1988.godine od strane Roberta Tappana Morrisa. Sjedinjene Američke Države i druge države uspostavile su specijalizirane grupe radi istrage računalnog kriminala na nacionalnom nivou, te 1992.godine termin digitalna forenzika se počinje koristi u stručnoj literaturi [9].

3.2.Računalni kriminalitet

Računalni kriminal predstavlja oblik kriminalnog ponašanja kod kojeg se korištenje računalne tehnologije i informacijskih sustava očituje kao način izvršenja kaznenog dijela ili se računalo upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka, u kazneno – pravnom smislu, relevantna posljedica [11].

Računalni kriminal se također odnosi na protupravnu povredu imovine, kod koje se računalni podaci s predumišljajem mijenjaju (manipuliranje računalom), razaraju (sabotaža) ili se koriste zajedno s hardverom (krađa vremena). U računalni kriminal isto tako spada svako kazneno djelo koje je počinjeno uz pomoć računala ili mreže [6].

Usporedno sa ubrzanom informatizacijom društva i ulaskom interneta u sve segmente društvenog i privatnog života ljudi, računalni kriminal postaje dominantan oblik zloupotrebe,

kršenja zakona i drugih normi ponašanja. Novi oblici napada na računala i računalne mreže javljaju se velikom brzinom, a novi tipovi računalnog kriminala praktično ovise samo o mašti malicioznih napadača [8].

3.2.1.Karakteristike računalnog kriminaliteta

Računalni kriminal ima svoje specifičnosti u odnosu na druge oblike kriminalnih djelovanja, a to su [8]:

- Velika dinamičnost
- Konstantno širenje na nove oblasti
- Težina posljedica koje nastupaju vršenjem računalnih kaznenih djela
- Otežano otkrivanje i dokazivanje
- Specifičan profil počinitelja
- Velike mogućnosti za prikrivanje izvršenog kriminalnog djela

Ove karakteristike posljedica su specifičnog okruženja u kojem se računalni kriminal vrši. To okruženje karakteriziraju sljedeće specifičnosti:

- Visoka koncentracija na malom prostoru
- Proširen prostor kriminalnog djelovanja, koji za razliku od tradicionalnih vidova kriminala ne zahtjeva prisutnost počinitelja na licu mjesta
- Skraćeno vrijeme kriminalnog djelovanja s obzirom na automatizirano okruženje, čija brzina sprečava nadzor i upravljanje
- Postojanje vještih tehnika i metoda koje se izvršavaju istim mehanizmima, ne ostavljajući tragove i ne ometajući redovan rad sistema
- Stabilnost rizika s obzirom da se jednom izgrađen modus može veoma dugo koristiti sa potpuno istim, niskim rizikom otkrivanja
- Jednostavnije mogućnosti upotrebe računalnih tehnologija od strane sve većeg broja korisnika.

3.2.2.Oblici i tipovi računalnog kriminaliteta

Na desetom kongresu Ujedinjenih naroda za prevenciju kriminala i tretman delikvenata, u okviru materijala za sekciju o kriminalu, zaključeno je da postoje dvije vrste pojavnog oblika kriminalnog ponašanja [9]:

- **Računalni kriminal u užem smislu –** predstavlja svako nezakonito ponašanje usmjereno na elektronske operacije sigurnosti računalnih sustav i podataka koji se u njima obrađuju
- **Računalni kriminal u širem smislu –** kao svako nezakonito ponašanje vezano za ili u odnosu na računalni sustav i mrežu, uključujući i nezakonito posjedovanje, nuđenje i distribuiranje informacija preko računalnih sustava i mreža.

Prema preporukama Vijeća Europe i listom OECD[6] –a iz 1989. odnosno 1985.godine računalni kriminal se dijeli na :

- Neautorizirani pristup računalnom sustavu ili mreži kršenjem mjera sigurnosti;
- Oštećenje računalnih podataka ili programa;
- Računalne sabotaže;
- Neovlašteno presretanje komunikacija od /u računalnim sustavima i mrežama;
- Računalna špijunaža.

Svaki od ovih oblika, može se ukrštavati sa svakim, jer gotovo da ne postoji "čisti" oblik. Od računalnog kriminala u širem smislu, najčešće se pojavljuju: računalni falsifikati, računalne krađe, tehničke manipulacije uređajima ili elektronskim komponentama uređaja, zloupotrebe sustava plaćanja (kao što su manipulacije i krađe elektronskih kreditnih kartica ili korištenje lažnih lozinki u nezakonitim financijskim aktivnostima [12].

Tipovi računalnog kriminala [8]**:**

- Krađa elektronskih usluga
- Komunikacija u cilju kaznene zavjere
- Piratstvo
- Elektronsko pranja novca
- Vandalizam i terorizam na Internetu
- Prodaja i investicija laži
- Ilegalno presretanje komunikacijskih kanala
- Transfer sredstava za on line prevare

U zavisnosti od tipa počinjenih djela računalni kriminal može biti :

[6]The Organisation for Economic Co-operation and Development je internacionalna ekonomska organizacija

- Politički
- Ekonomski
- Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja
- Manipulacija zabranjenim proizvodima, supstancama, robom
- Povreda Internet privatnosti

3.3.Digitalni dokaz

Dokaz je ono što razdvaja hipotezu od neosnovane tvrdnje. Dokazi mogu potvrditi ili oboriti hipotezu, pa je njihov integritet ključan u njihovom prihvaćanju, odnosno odbacivanju pred sudom. Postoji nekoliko specijalnih karakteristika digitalnog dokaza koje ih čine posebno izazovnim [8].

Prije svega potrebno je jasno i precizno definirati digitalni dokaz. Digitalni dokaz je informacija uskladištena ili prenošena u digitalnoj formi koja učestvuje u sudskom slučaju i može se koristiti na suđenju. Digitalna forma po svojoj prirodi podrazumijeva da se radi o nekom elektronskom ili magnetnom uređaju, pa to mogu biti podaci u radnoj memoriji, na tvrdom disku, *flash* karticama, ali i podaci koji se nalaze u transmisiji npr. radio valovi [12].

Digitalni dokaz nije nešto što ljudi mogu na prvi pogled protumačiti. U doslovnom smislu, digitalni dokaz predstavlja niz nula i jedinica koje neki elektronski uređaj prevodi u ljudima razumljivu formu, koju oni mogu koristiti kao potkrepljenje svojoj hipotezi u okviru nekog sudskog slučaja. Treba se osvrnuti na karakteristike i prirodu digitalnih dokaza.

1. *Veliki broj potencijalno inkriminiranih*: Kod tradicionalnih prestupa često se pojavljuje nešto što isti manifestira – postoji leš, otisci prstiju, vlasi kose – materijalni tragovi. Sa takvom početnom točkom, istražiteljima je lako započeti pretragu jer postoji neko usmjerenje i početna lista osumnjičenih. Provjerava se tko je poznavao žrtvu, čiji su otisci, radi se DNK test i sl. Internet, zbog svoje anonimnosti i nepostojanja standarda identifikacije može ponuditi veliki broj potencijalno osumnjičenih.
2. *Identifikacija prestupa*: Kod računalnog kriminala priroda prestupa je manje očigledna i neposredna. Na primjer, ako haker ukrade povjerljive informacije, žrtva ne mora primijetiti da je oštećena, sve dok ne bude obaviještena od strane sistem administratora, a to je obično kasno nakon samog upada. Krađa identiteta je jedan od prestupa, koji ima najveći faktor rasta na području računalnog kriminala, a može biti otkrivena tek nakon nekoliko godina.

3. *Previše potencijalnih dokaza*: Kod računalne forenzike, nekad je neophodno pokušati dati postojanu hipotezu koja je mnogo šira od finalne, da bise zatim ta ista hipoteza sužavala tokom istrage. Naravno da nije sve digitalni dokaz. Istražitelj mora znati što od nalaza može iskoristiti za sužavanja početne hipoteze, a da bi to uradio, mora znati prirodu prestupa. Kako je identifikacija prestupa teška sama po sebi, jasno je o kakvom se problemu radi.
4. *Podložnost kontaminaciji*: Tradicionalni dokazi se uglavnom šalju sa scene događaja na neko drugo mjesto, na kojima se vrši njihova obrada i na kome se čekaju rezultati. Kod računalne forenzike ne postoji takva neosjetljivost na promjenu stanja. Svi koraci u procesu istrage moraju osigurati što prije sve potrebne mjere za očuvanje početnog stanja. Provođenje takve metodologije moguće je samo ako se prati striktno određena procedura. Nitko ne želi da dođe do kontaminiranja dokaza, a koliko je to moguće govori činjenica da se ponovnim pokretanjem računala drastično mijenja početno stanje, a da dokazi mogu biti ne samo kontaminirani već i zauvijek izgubljeni.
5. *Lakoća gubitka dokaza*: Upravo posljednja rečenica prethodne karakteristike otvara novo pitanje, da li bez dokaza koji je izgubljen slučaj može opstati. Međutim nekada je gubitak dokaza posljedica neznanja da je dokaz zaista prisutan [9].

Kako je kompjuterska forenzika više zainteresirana za formu nego za funkciju izvora digitalnog dokaza izvori digitalnih dokaza su klasificirani prema skladištenju podataka na [8]:

1. ***Privremenu formu digitalnog dokaza***.

   Tipičan predstavnik ove forme je RAM memorija koja bez eksternog izvora napajanja briše.
2. ***Nestalnu formu***.

   Kod ove forme postoji neki interni izvor napajanja poput baterije. Kao i kad privremene forme ukoliko bismo izvadili bateriju informacije bi bile izgubljene. Primjer ove forme je CMOS ili RAM na prijenosnom računalu koji ima napajanje na bateriju.
3. ***Semipermanentna***(*polustalna*) ***forma***.

   Riječ je o čvrstom mediju koji se može promijeniti (npr. hard disk, disketa, CD, DVD, MMC i sl.)
4. ***Permanentna (stalna) forma***. ROM memorija.

Računalni forenzičar mora dobro poznavati svaku od gore navedenih formi kako bi izbjegao probleme koje smo naveli, a koji karakteriziraju digitalne dokaze. Istražitelj mora sa

takvim podacima postupati iterativno-dekrementalno, te početnu veliku količinu podataka svesti na optimalnu veličinu [12].

Svaka iteracija u forenzičkoj istrazi rezultira, za slučaj vrijednim podacima, a istovremeno smanjuje inicijalnu količinu podataka. Rezultirajući skup podataka se u sljedećoj iteraciji koristi za dublju analizu i tako se dolazi do neke optimalne veličine podataka. Finalni set dokaza bi trebao biti od velike koristi pravnicima u sudskom procesu protiv počinitelja prestupa [9].

4.RAČUNALNA FORENZIČKA ANALIZA

4.1. Izrada postupka računalne forenzičke analize

Računalna forenzička analiza (RFA) je zahtjevno područje djelatnosti koje iziskuje posebno obučeno osoblje, razrađenu logističku podršku i značajna financijska sredstva, a sve sa ciljem zadržavanja pravne vjerodostojnosti prikupljenih dokaza. Zbog toga je potrebno detaljno razraditi odgovarajuće postupke RFA [9].

- **Određivanje ciljeva RFA** Razvoj načela rada i postupaka je važan korak u stvaranju tima za RFA. Ovo je moguće učinkovito učiniti određivanjem ciljeva RFA koji obuhvaćaju osnovne funkcije tima bez obzira radilo se o istraživanju zločina na području visoke tehnologije, prikupljanju dokaza ili forenzičkoj analizi.
- **Ljudski resursi potrebni za provođenje RFA** Prilikom razrade postupaka RFA potrebno je posvetiti pažnju pitanjima vezanim uz ljudske resurse, kao što su: opis posla, potrebna stručna sprema, radno vrijeme, dežurstva te hijerarhija i struktura tima za provođenje RFA. Zbog dinamike ovog područja potrebno je neprestano održavati razinu stručnosti članova tima stalnim usavršavanjem djelatnika ili zapošljavanjem novih stručnjaka određenog profila.
- **Administrativne pripreme** Osnivanje i djelovanje tima za RFA zahtjeva znatna sredstva, a mnogi od potrebnih izdataka su periodički te je sredstva potrebno osiguravati na godišnjoj osnovi. Potrebno je osigurati radni prostor, opremu, programsku podršku s nužnim nadogradnjama te stalno školovanje osoblja. Korištena programska podrška obično treba biti licencirana, bilo na ime agencije ili članova tima koji ju koriste.
- **Zahtjevi za provedbom RFA te prihvaćanje dokaza** Potrebno je izraditi smjernice za predavanje zahtjeva za provedbom RFA te smjernice za prihvaćanje dokaza ako je takav zahtjev uvažen. Ove smjernice se odnose na: formulare sa zahtjevima, načine na koje se zahtjevi predaju, dokumentaciju koju treba priložiti zahtjevu, kriterije prihvaćanja zahtjeva i fizičkih dokaza.
- **Upravljanje slučajem** Jednom kada je zahtjev za provedbom RFA uvažen, potrebno je utvrditi kriterije za određivanje prioriteta pojedinih ispitivanja. Takvi se kriteriji mogu odnositi na vrstu zločina, rokove vezane uz sudski proces, potencijalne žrtve, pravna pitanja, postojanost dokaza i raspoloživa sredstva.
- **Određivanje postupaka rukovanja dokazima** Potrebno je izraditi smjernice za primanje, obradu, dokumentiranje i rukovanje dokazima i ostalim materijalima povezanim s istragom. Za prihvaćanje dokaza s ilegalnim sadržajima, npr. Dječjom

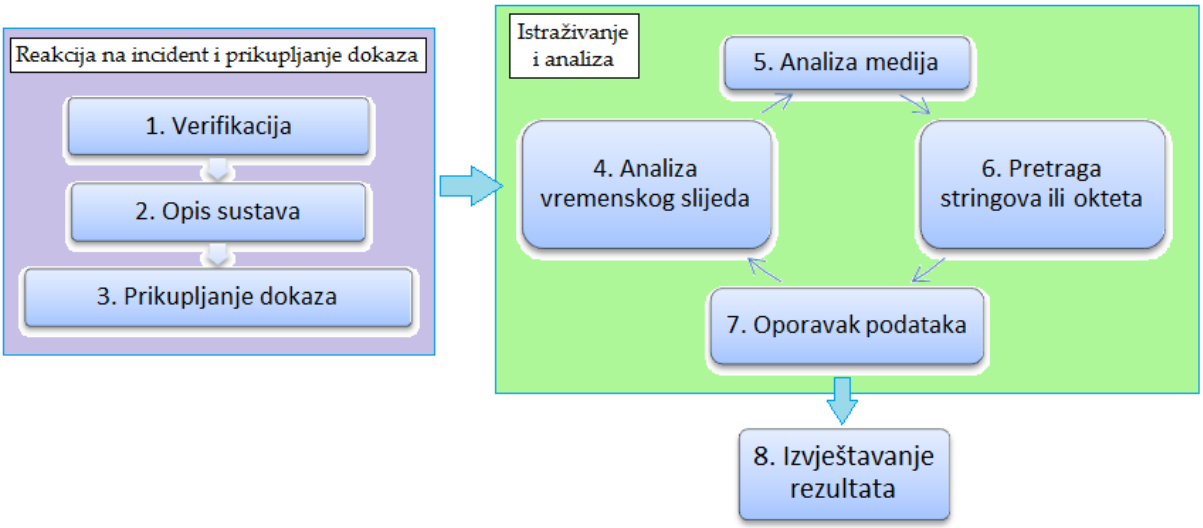
pornografijom, mogu biti potrebni posebni nalozi. Druge forenzičke discipline mogu pronaći dodatne dokaze, kao što su otisci prstiju na kućištu tvrdog diska, vlasi ili vlakna unutar tipkovnice te rukom pisane oznake ili tiskani materijali. Zbog toga je potrebno izraditi postupke za određivanje redoslijeda kojim će se vršiti ispitivanja, kako ne bi došlo do uništavanja dokaza. Sve tehničke postupke prikupljanja dokaza potrebno je ispitati kako bi se utvrdila njihova ponovljivosti valjanost dobivenih rezultata. Koraci razvoja i ispitivanja ovakvih postupaka trebaju biti dokumentirani i sadržavati:

- određivanje zadatka ili problema,
- prijedlog mogućih rješenja,
- ispitivanje svakog rješenja na poznatom uzorku,
- ocjenjivanje rezultata ispitivanja i
- oblikovanje postupka.

Uz prethodno navedeno, veoma je važno da se izvorni dokazi nikada ne koriste u procedurama testiranja postupaka [13].

4.2. Prikupljanje podataka i dokaza

Prikupljanje podataka i dokaza najosjetljiviji je korak RFA (Slika 6). Eventualne pogreške u ovom stupnju mogu značiti nepovratan gubitak dokaza, bilo zbog njihova oštećivanja ili zbog gubitka njihove vjerodostojnosti uslijed neprimjerenih metoda prikupljanja. Zbog toga je potrebno pažljivo isplanirati postupak prikupljanja dokaza, s posebnim naglaskom na ranjive dokaze, te koristiti odgovarajuće programske alate [13].



Slika 6: Reagiranje na incident [13]

4.2.1. Procjena dokaza

Prije prikupljanja dokaza potrebno je izvršiti temeljitu procjenu danog slučaja (Slika 7) i na temelju toga odrediti smjer daljnjeg djelovanja. U okvir takve procjene ulaze nalog za pretraživanje, detalji slučaja, vrsta ispitivanog sklopovlja i programske podrške, potencijalni dokazi koje se traži te uvjeti njihovog prikupljanja [9].

U razgovoru s voditeljem istrage potrebno je razmotriti:

- primjenu ostalih forenzičkih postupaka nad dokazima (DNA analiza, prikupljanje otisaka prstiju, traženje tragova mehaničke obrade i sl.),
- važnost opreme pronađene uz računalo (npr. kreditne kartice, skeneri, pisači ili digitalne kamere),
- ostale smjerove istrage (npr. traženje podataka od pružatelja Internet usluga, pronalaženje udaljenih spremišta podataka ili poruka elektroničke pošte),
- vrstu potencijalnih dokaza (fotografije, tablice, dokumenti, baze podataka, financijski podaci),
- ostale informacije vezane uz slučaj (korisnička imena, zaporke, računi elektroničke pošte, mrežne postavke, dnevnički zapisi) koje je možda moguće dobiti u razgovoru s administratorima, korisnicima ili zaposlenicima, te
- razinu informatičkog znanja korisnika čije se djelovanje ispituje.

Po dolasku na mjesto potencijalnog zločina potrebno je utvrditi:

- broj i vrste računala,
- prisutnost računalne mreže,
- vrstu i količinu medija za pohranu podataka te dokumentirati gdje su pronađeni,
- postojanje udaljenih spremišta podataka i/ili udaljenih računala,
- korištene komercijalne programske pakete,
- o kojim se operacijskim sustavima radi, te
- intervjuirati sistemske administratore i korisnike.

Prilikom skladištenja pronađenih dokaza potrebno je osigurati njihovu zaštitu od elektromagnetskih smetnji. Stalni izvori napajanja mogu biti potrebni ukoliko se radi o uređajima s baterijskim napajanjem.

Slika 7: Dijagram toka postupka RFA [vlastita izrada]

4.2.2. Ranjivost dokaza

Digitalni dokazi su mnogo ranjiviji od konvencionalnih fizičkih dokaza i zbog toga se prilikom rukovanja potrebno pridržavati određenih smjernica kako ih se ne bi uništilo ili oštetilo. Prvi korak u traženju dokaza na računalu često je njegovo gašenje i transport u laboratorij radi provođenja temeljite analize. Svi podaci nastali tijekom rada računala, koji nisu pohranjeni na tvrdi disk, time su nepovratno izgubljeni [13].

Ostavljanje računala uključenim ipak ne jamči očuvanje dokaza. Ako je računalo povezano na računalnu mrežu, napadač može s udaljene lokacije izbrisati dnevničke zapise ili, neovisno o vezi na mrežu, programirati njihovo automatsko brisanje. Jednako tako, dobronamjeran korisnik radom na računalu može nesvjesno uzrokovati prepisivanje dokaza. Uništenje nije jedina opasnost koja prijeti digitalnim dokazima [7].

Nestručnim rukovanjem oni mogu biti oštećeni i tako obezvrijeđeni u potencijalnom sudskom postupku. Ovo se najčešće događa zbog neinformiranosti korisnika koji, nakon što su uočili zločin, pokušavaju otkriti što se točno dogodilo, te tako utječu na sustav. Glavne vrste ranjivih dokaza su [13]:

- prijelazni podaci – oni koji se gube gašenjem računala i tu se ubrajaju aktivne mrežne veze ili aplikacije koje se izvode u radnoj memoriji,

- ranjivi podaci – iako pohranjeni na tvrdom disku, lako su izmjenjivi (primjer ovakvih dokaza su vremenske oznake posljednjeg pristupa datoteci ili direktoriju),
- privremeni podaci – podaci koji su pohranjeni na tvrdom disku, a moguće im je pristupiti samo u određenim vremenskim intervalima (primjer su datoteke kriptiranih datotečnih sustava).

Kako bi se ranjivi dokazi očuvali potrebno ih je što prije pohraniti na siguran medij. Tvrdi disk ispitivanog računala nije prikladan za to jer i sam može sadržavati dokaze koji bi na ovaj način mogli biti uništeni ili oštećeni. Prilikom pohrane ranjivih dokaza potrebno je koristiti što manje radne memorije kako bi se očuvao njezin sadržaj [9].

Diskete su dobar izbor za pohranu ranjivih dokaza zbog svoje raširenosti, niske cijene i jer ih je lako zaštititi od pisanja. Glavni im je nedostatak maleni kapacitet. Umetanje tvrdog diska u ispitivano računalo nije prihvatljivo jer zahtjeva njegovo gašenje. Ne preporuča se niti korištenje USB[7] ili *Firewire*[8] prijenosnih medija jer se njihovim spajanjem mijenja stanje ispitivanog sustava [12].

Najbolji način za prikupljanje ranjivih dokaza je uporaba računalne mreže. Kako bi se ispitivano računalo zaštitilo od daljnjih napada i kako bi se prikrila istraga, računalo je po otkriću napada potrebno isključiti sa mreže. Njegovim spajanjem na privatno čvorište (eng. *hub*) omogućuje se prijenos podataka. Pri tome drugo računalo, korišteno za prikupljanje dokaza, treba prilagoditi mrežnim postavkama ispitivanog računala [7].

Prije svega je potrebno dohvatiti i pohraniti sadržaj radne memorije ispitivanog računala i to umanjim paketima kako bi se izbjeglo prepisivanje ostatka radne memorije. Nakon što je sadržaj radne memorije pohranjen može se pristupiti dohvaćanju ostalih podataka, bez ograničenja na veličinu paketa [12].

4.2.3. Alati za prikupljanje ranjivih dokaza

Alat za prikupljanje ranjivih dokaza mora zadovoljavati sljedeće kriterije [9]:

1. Forenzički integritet ispitivanog sustava mora biti očuvan. To znači da na takvom sustavu nije dozvoljeno spremanje podataka niti izvođenje aplikacija.

[7]USB (eng. Universal Serial Bus) je naziv za računalnu sabirnicu koja služi za serijski prijenos podataka između osobnog računala i perifernih uređaja.

[8]IEEE 1394 je standard koji opisuje serijsku sabirnicu za prijenos podataka velikom brzinom i sa sposobnošću isokronog prijenosa podataka.

2. Alat autonomno izvodi cjelokupno rukovanje dokazima, bez interakcije korisnika. Ovo je potrebno kako bi se dokazi osigurali od nestručnog rukovanja. Time se ujedno osigurava i vjerodostojnost prikupljenih dokaza jer ih korisnik ne može mijenjati.
3. Alat sakuplja samo dokaze koji bi mogli biti oštećeni ili izgubljeni tijekom ispitivanja sustava ili njegova transporta.
4. Alat izvještava korisnika o otkrivenim tragovima napada. Rezultat razumljiv korisniku potaći će ga na korištenje alata.

Primjer ovakvog alata je FRED (Slika 8) (eng. *First Responder's Evidence Disk*) koga je razvila organizacija AFOSI (eng. *Air Force Office of Special Investigations*). Ovo je jednostavan i malen programski paket namijenjen pokretanju s diskete. Glavni zadatak FRED paketa je prikupljanje podataka potrebnih za otkrivanje napada, on bilježi osnovne sistemske veličine (npr. vrijeme i datum), mrežne veze, aktivne procese, aktivne DLL datoteke, otvorene priključke (eng. *port*) i MD5 (eng. *Message-Digest algorithm)*vrijednosti važnijih sistemskih datoteka.

Slika 8: Izgled FRED-a [14]

4.2.4. Logičko i fizičko dohvaćanje podataka s diska

Fizičko dohvaćanje podataka podrazumijeva dohvaćanje podataka na fizičkoj razini, bez obzira na datotečni sustav. Logičko dohvaćanje se odnosi na dohvaćanje podataka u ovisnosti o instaliranom operacijskom sustavu, o datotečnom sustavu i/ili prisutnim aplikacijama [15].

Fizičko dohvaćanje podataka obuhvaća sljedeće metode:

- ispitivanje particijske strukture (koristi se za identifikaciju prisutnih datotečnih sustava te određivanje veličine i sadržaja nezauzetog diskovnog prostora)

- traženje znakovnih nizova na fizičkom disku, čime se mogu pronaći podaci nevidljivi operacijskom i datotečnom sustavu.

Mogući koraci logičkog dohvaćanja podataka su [16]:

- dohvaćanje podataka o datotečnom sustavu kao što su struktura direktorija, imena, svojstva, veličine i položaji datoteka te vremenske oznake,
- eliminacija poznatih datoteka iz RFA na temelju identifikacijskih brojeva (eng. *Hash value*),
- identificiranje datoteka značajnih za RFA na temelju njihova imena, veličine, zaglavlja, sadržaja ili položaja na disku,
- obnavljanje izbrisanih datoteka,
- dohvaćanje komprimiranih, kriptiranih i zaporkama zaštićenih podataka,
- dohvaćanje neiskorištenog prostora iza kraja datoteka (eng. *file slack*),
- dohvaćanje nezauzetog diskovnog prostora.

4.3. Prikupljanje dokaza na Linux operacijskim sustavima

RFA analizu Linux operacijskih sustava moguće je provoditi alatima ugrađenim u operacijski sustav ili specijaliziranim aplikacijama.

4.3.1. Ispitivanje radne memorije

Prvi korak u ispitivanju radne memorije je pohrana njenog sadržaja (eng. *dump*) na neki trajni medij. Kako bi se smanjio utjecaj na ispitivano računalo pohranu je potrebno načiniti korištenjem samo jedne naredbe. Pritom sliku radne memorije nije uputno pohraniti na tvrdi disk ispitivanog računala. Sliku radne memorije moguće je dohvatiti pomoću *dd* naredbe, koja podatke kopira bit po bit, te ju je potom moguće korištenjem *netcat* alata spremiti na udaljeno računalo. Kod Linux operacijskih sustava radnu memoriju je moguće spremiti u dvije datoteke: /dev/mem i /proc/kcore. Slika radne memorije se u /proc/kcore datoteku sprema u „ELF core“ formatu, ali je pri tome slika nešto veća od same radne memorije zbog ELF zaglavlja. Radnu memoriju je moguće spremiti sljedećom naredbom: #mnt/cdrom/ddif=/dev/mem | /mnt/cdrom/nc <IP adresa> <broj porta> [17].

Nakon toga moguće je pristupiti pretraživanju spremljene slike radne memorije u potrazi za tragovima digitalnog zločina. Pri tome je nužno dobro poznavanje strukture radne memorije kod Linux operacijskih sustava [16].

4.3.2. Ispitivanje sadržaja diska

Linux operacijski sustavi imaju ugrađene brojne alate korisne u ispitivanju sadržaja diska. Neki od njih su [17]:

- *dd* – naredba za kopiranje podataka iz jedne datoteke ili uređaja u drugu datoteku ili uređaj
- *sfdisk* i *fdisk* – naredbe za određivanje strukture diska
- *grep* – naredba za traženje izraza ili uzoraka u jednoj ili više datoteka
- *loopdevice* – omogućuje dohvaćanje (eng. mount) slike diska bez snimanja na tvrdi disk
- *md5sum* i *sha1sum* – omogućavaju stvaranje MD5 ili SHA (eng. *Secure Hash Algorithm*) sigurnosnih suma datoteka ili lista datoteka
- *file* – čitanjem zaglavlja datoteke određuje njezin tip, bez obzira na ime
- *xxd* – preglednik binarnih datoteka
- *ghex* i *khexedit* – preglednici binarnih datoteka namijenjeni *Gnome* i *KDE* grafičkim okruženjima.

Značajan je korak svake RFA, utvrđivanje vjerodostojnosti prikupljenih podataka. To omogućuju naredbe *md5sum* i *sha1sum* koje za svaku datoteku ili disk stvaraju jedinstven digitalni potpis. Naredba *dd* stvara točnu kopiju zapisa na fizičkom uređaju s ne rezerviranim prostorom i neiskorištenim prostorom iza kraja datoteka [13].

Za razliku od drugih sličnih alata, *dd* u stvorenu sliku ne zapisuje dodatne podatke što ima višestruke prednosti sa stajališta RFA. Pretraživanjem ne rezerviranog prostora unutar slike ispitivanog diska pomoću *grep* naredbe moguće je pronaći fragmente teksta ili cijele izbrisane dokumente [16].

Kombiniranjem naredbe *dd* s naredbom *split*, sliku ispitivanog diska moguće je razložiti na dijelove proizvoljne veličine. To može biti korisno ukoliko sliku treba pohraniti na više CD ili DVD medija ili ako je potrebno ograničiti njezinu veličinu zbog specifičnosti alata korištenih za analizu. Ako je sadržaj ispitivanog tvrdog diska s više particija pohranjen unutar jedne slike može se javiti i potreba za stvaranjem pojedinačne slike za svaku particiju [17].

Izdvajanjem pojedinih particija olakšava se njihovo pregledavanje, jer je moguće koristiti *loopdevice* alate. Prije obnavljanja slike ispitivanog diska potrebno je „očistiti“ odredišni disk kako ostaci starih podataka ne bi otežali potragu za dokazima. Čišćenje je moguće izvesti prepisivanjem cijelog diska nulama. Provjeru uspješnog prepisivanja moguće je obaviti

naredbom *xxd* s „autoskip“ parametrom. Pored spomenutih alata namijenjenih tekstualnom korisničkom sučelju postoji niz grafičkih alata koji RFA čine bržom i jednostavnijom [15].

4.4. Prikupljanje dokaza na Windows operacijskim sustavima

Windows operacijski sustavi najčešće su korišteni operacijski sustavi među korisnicima. Stoga je u nastavku ovog poglavlja analizirana rekonstrukcija obrisanih datoteka te korištenje *Windows Forensics Toolchest* besplatnog alata [16].

4.4.1. Rekonstrukcija sadržaja „*Recycle Bin*“ direktorija

Brisanjem datoteka one nisu nepovratno izgubljene već se spremaju u „*Recycle Bin*“ direktorij kako bise umanjile posljedice slučajnog brisanja. Pri tome nastaje INFO2 datoteka s podacima potrebnim za obnavljanje izbrisanih datoteka od kojih neki mogu biti značajni za RFA. Datotekama premještenim u „Recycle Bin“ direktorij ime se mijenja u oblik „DC#.EXT“, gdje je #cjelobrojna jedinstvena oznaka izbrisane datoteke, a EXT izvorni format izbrisane datoteke, npr. brisanjem datoteke „DATOTEKA.TXT“ ona može u „Recycle Bin“ direktoriju biti spremljena kao„DC4.TXT“ [17].

Brisanjem sadržaja spomenutog direktorija briše se i sadržaj INFO2 datoteke te se brojač pobrisanih datoteka (#) postavlja u početno stanje. U INFO2 datoteku zapisuju se sljedeći podaci o svakoj izbrisanoj datoteci:

- puno ime izvorne datoteke (s položajem u datotečnom sustavu) u ASCII i UNICODE formatu,
- oznaka diska s kojeg je datoteka izbrisana (0x00 za „A:“ disk, 0x01 za „B:“ disk itd.),
- fizička veličina,
- datum i vrijeme brisanja i
- identifikacijski broj.

Analizu obrisanih datoteka moguće je automatizirati korištenjem nekog od specijaliziranih alata, kakav je npr. *Rifiuti* programski paket otvorenog koda [18].

4.4.2. Windows Forensics Toolchest

Ako se područje potrage za dokazima želi proširiti izvan „*Recycle Bin*“ direktorija potrebno je koristiti neki od alata koji to omogućuju. Jedan od njih je *Windows Forensics Toolchest* (WFT) besplatni programski paket koji omogućuje automatsko prikupljanje dokaza, a financiran je dobrovoljnim donacijama korisnika. WFT predstavlja forenzički unaprijeđenu

ljusku za automatsko pokretanje sigurnosnih alata (eng.*batch processing shell*) s mogućnošću stvaranja izvještaja u HTML[9] formatu. Uz pravilnu uporabu i u kombinaciji s odgovarajućim sigurnosnim alatima, ovaj paket omogućuje otkrivanje sigurnosnih incidenata te stvara izvještaj prikladan za uporabu tijekom sudskog procesa [17].

WFT bilježi sve svoje aktivnosti tijekom traženja dokaza i kontinuirano proračunava MD5 kontrolne zbrojeve, čime se osigurava vjerodostojnost njegovih izvještaja. Tijekom izvođenja sam WFT paket minimalno opterećuje ispitivani sustav(koristi dio radne memorije te čita nekoliko registara).Alati koje WFT poziva nisu nužno tako ne zahtjevni, pa je potreban pažljiv izbor postavki postupka traženja dokaza. Kako bi se osigurao forenzički integritet prikupljenih dokaza, potrebno je WFT pokretati sa CD ili USB diska na kojemu se, pored ovog paketa, nalaze kopije alata koje koristi u radu te sigurna kopija„cmd.exe“ datoteke, i to inačice jednake onoj na ispitivanom računalu. Konfiguracijska datoteka WFT alata mora sadržavati MD5 sigurnosne zbrojeve svih datoteka korištenih tijekom traženja dokaza. Tijekom ispitivanja računala u HTML izvještaj se, posebno za svaki od korištenih sigurnosnih alata, bilježi opis alata, MD5 sigurnosni zbroj pokrenute datoteke, korištene naredbe te rezultat i uz njega vezan MD5 sigurnosni zbroj [18].

4.5. Analiza dokaznih materijala

Poželjno je analizu dokaznih materijala provesti u kontroliranim uvjetima kakve pruža forenzički laboratorij ili neki drugi radni prostor takve namjene. Ako objektivne okolnosti nameću potrebu analize dokaza na mjestu pronalaska, prije pristupanja analizi, treba razmotriti vrijeme, materijalna sredstva i osoblje potrebno za takvu analizu te utjecaj na poslovanje ustanove u kojoj se provodi istraga. Kada je to moguće, analizu je potrebno provoditi nad kopijama dokaza kako bi se izbjeglo nenamjerno oštećivanje originala. Redoslijed ispitivanja dokaza može se utvrditi prema mjestu pronalaska ili stabilnosti medija na kojima su pohranjeni. Pri tome u obzir treba uzeti posljedice koje su na dokazima mogli ostaviti pakiranje, transport ili skladištenje [19].

U nastavku su navedene četiri skupine metoda analize prikupljenih dokaza. Rezultati svake od navedenih analiza sami za sebe ne moraju otkrivati puno i zbog toga ih je, u kontekstu istrage, potrebno sagledati kao cjelinu.

[9]HTML je kratica za Hyper Text Markup Language, što znači prezentacijski jezik za izradu web stranica.

4.5.1. Analiza vremenskog slijeda

Analizom vremenskog slijeda utvrđuje se redoslijed događaja na ispitivanom računalnom sustavu te se time oni povezuju s korisnicima. Ovu analizu moguće je provesti na dva načina. Prvi način se odnosi na analizu metapodataka[10] datotečnog sustava u kojima su zabilježena slijedeće oznake vremena:

- vrijeme stvaranja datoteka,
- vrijeme njihove posljednje promjene, te
- vrijeme posljednjeg pristupa i promjene statusa.

Druga metoda je analiza sistemskih dnevničkih zapisa koji mogu obuhvaćati zapise pogrešaka, instalacijske, mrežne, sigurnosne ili neke druge zapise [17].

4.5.2. Pronalaženje skrivenih podataka

Moguće je primijeniti nekoliko metoda za traženje skrivenih podataka:

- usporedbom zaglavlja datoteka i njihovih nastavaka moguće je otkriti nepodudaranja koja ukazuju na prikrivanje podataka,
- podatke je moguće prikriti kriptiranjem, komprimiranjem ili zaštitom zaporkama, pri čemu za RFA korištene zaporke mogu biti jednako značajne kao sadržaj datoteka koje štite,
- pohrana podataka u HPA (eng. *Host-Protected Area*) također može ukazivati na pokušaj njihova prikrivanja [16].

4.5.3. Analiza aplikacija i datoteka

Analizom aplikacija i datoteka prisutnih na računalu moguće je utvrditi njegove performanse te razinu informatičkog znanja korisnika. Takva saznanja mogu zatim ukazati na potrebu za dodatnim koracima RFA. Neki od primjera analize aplikacija i datoteka su [20]:

- uočavanje uzoraka u imenima datoteka,
- pretraživanje sadržaja datoteka,
- utvrđivanje broja i vrste prisutnih operacijskih sustava,
- utvrđivanje veza među datotekama i instaliranim aplikacijama,
- identificiranje nepoznatih vrsta datoteka i utvrđivanje njihove važnosti za RFA,

[10]Podaci o podacima – podaci koji opisuju karakteristike nekog izvora u digitalnom obliku. Korisni su kod pregledavanja, prijenosa i dokumentiranja informacijskog sadržaja. U digitalnom smislu to su „strukturirani podatci koji opisuju, objašnjavaju, lociraju ili na neki drugi način omogućavaju lakše upravljanje resursima.“

- utvrđivanje odnosa među datotekama, npr. povezivanje zapisa aktivnosti na Internetu s priručnim (eng. *cache*) datotekama ili povezivanje poruka elektroničke pošte s njihovim prilozima,
- ispitivanje korisničkih postavki,
- analiza metapodataka, npr. za tekstualni dokument to mogu biti podaci o autoru, vrijeme posljednje izmjene, broj izmjena te podaci o ispisu ili spremanju, itd.

4.5.4. Analiza vlasništva nad datotekama

Identificiranje korisnika koji je stvorio, izmijenio ili pristupio određenoj datoteci može biti ključno za istragu. To je moguće učiniti nekom od slijedećih metoda, koje pripadaju i prethodno navedenim skupinama:

- utvrđivanje točnog vremena kada je korisnik imao pristup računalu može omogućiti utvrđivanje vlasništva nad datotekama (analiza vremenskog slijeda),
- smještaj datoteka može otkriti njihova vlasnika (analiza aplikacija i datoteka),
- zaporke za pristup kriptiranim ili zaštićenim datotekama mogu, ukoliko su otkrivene, ukazati na vlasnika zaštićenih datoteka (pronalaženje skrivenih podataka),
- datoteke mogu sadržavati podatke karakteristične za pojedinog korisnika i tako otkriti svoga vlasnika (analiza aplikacija i datoteka) [21].

4.6. Dokumentiranje i izvještavanje

Istražitelj je odgovoran za potpunost i točnost izvještaja o RFA. Dokumentiranje je proces koji se treba provoditi usporedno s RFA, s preciznim bilježenjem svakog koraka. Dokumentacija mora biti potpuna, točna i sveobuhvatna.

4.6.1. Vođenje bilježaka

Tijekom cijele istrage potrebno je voditi bilješke u skladu s preporukama institucije u čije ime se istraga provodi. Slijedi nekoliko općenitih uputa koje u tome mogu pomoći istražitelju [20]:

- voditi bilješke tijekom konzultacija s voditeljem istrage ili tužiocem,
- sačuvati kopiju naloga za pretragu,
- sačuvati kopiju prvotnog zahtjeva za pokretanjem istrage,
- sačuvati kopiju dokumentacije o nadležnostima i odgovornostima sudionika istrage,
- voditi bilješke koje omogućuju ponavljanje svih provedenih postupaka,
- u bilješke unositi datum, točno vrijeme, opis i rezultate svakog provedenog postupka,
- dokumentirati neuobičajene okolnosti i u vezi njih poduzete akcije,

- bilježiti podatke kao što su: topologija računalne mreže, popis autoriziranih korisnika, korisničke zaporke i sl.,
- bilježiti sve promjene unesene u ispitivani sustav tijekom provođenja RFA,
- dokumentirati programsku podršku ispitivanog računala: operacijski sustav, instalirane aplikacije te zakrpe i nadogradnje,
- dokumentirati prisutnost udaljenih spremišta podataka, mogućnost pristupa udaljenih korisnika i sigurnosnih kopija, itd.

Ukoliko se tijekom pretrage pronađu materijali koji bi mogli biti značajni za RFA, ali nisu u nadležnosti istrage, to je potrebno dokumentirati, te zatražiti ovlasti potrebne za obradbu spomenutih materijala.

4.6.2. Izvještaj

Oblik i sadržaj izvještaja o RFA ovisi o zahtjevima tijela ili organizacije kojoj se izvještaj predaje. On može sadržavati [13]:

- podatke o organizaciji koja je provela RFA,
- jedinstvenu oznaku slučaja,
- podatke o istražiteljima i njihove potpise,
- datum početka istrage i predaje izvještaja,
- popis ispitanih predmeta s opisom koji uključuje serijski broj, naziv proizvođača i model,
- kratak opis poduzetih koraka RFA,
- rezultate RFA i zaključak.

Ponekada je potrebno izvještaj proširiti sažetkom pronalazaka, detaljnim opisom rezultata RFA te listom priloženih dokumenata i/ili kazalom. Sažetak pronalazaka sadrži kratak pregled rezultata svih ispitivanja provedenih u okviru RFA. Detaljan opis rezultata RFA se može sastojati od [21]:

- datoteka značajnih za RFA,
- ostalih datoteka koje potvrđuju rezultate analize, uključujući izbrisane datoteke,
- dokaza vezanih uz Internet kao što su analiza Web prometa, dnevnički zapisi, priručne datoteke, poruke elektroničke pošte, aktivnosti na tzv. *usenet* grupama,
- analize grafičkih datoteka,
- dokaza vlasništva koji mogu uključivati licence aplikacija,

- opisa za RFA značajnih programskih paketa pronađenih unutar ispitivanog sustava,
- opisa uočenih tehnika prikrivanja podataka kao što su enkripcija, sakrivanje atributa, sakrivanje particija, nepravilnosti imena datoteka, itd.

5.PROGRAMSKI ALATI RAČUNALNE FORENZIKE

Procjena i izbor alata za računalnu forenzičku analizu još uvijek predstavlja izazov, i nedovoljno je istražena tema u području digitalne forenzike. Izbor adekvatnog alata koji će biti korišten za računalnu forenzičku analizu u velikoj mjeri utječe na ishod u sudnici. Iako je cilj jasan – dobivanje valjanih digitalnih dokaza prihvatljivih na sudu, u praksi se pokazalo da do toga nije nimalo lako doći. Za dobivanje digitalnih dokaza u forenzičkom postupku postoji mnogo razvijenih tehnika i alata koji se danas koriste, a njihov velik značaj povezan je sa činjenicom da je danas preko 90 posto svih novih informacija proizvedeno u digitalnom obliku, i da se takvo bogatstvo mora na adekvatan način kontrolirati, nadgledati i čuvati. Razvoj forenzičkih alata usavršavao se kroz tri generacije [15].

Prvu generaciju su činili razni alati za: slike, dokumenta, pretraživanje i oporavak sustava; drugu generaciju su činili posebno dizajnirani i razvijeni profesionalni alati (*Encase*, SANS, *Helix* itd.), kao i veliki broj besplatnih alata otvorenog koda koji se mogu naći i preuzeti sa Interneta; treću generaciju čine inteligentni alati koji u realnom vremenu, sigurno i efikasno nadgledaju cjelokupan mrežni promet. Ono što je potrebno da bi se neki forenzički alat koristio u istrazi, je da bude certificiran i priznat od državnih sudskih organa, kako bi digitalni dokazi bili valjani u sudskom procesu [20].

Uobičajena je sljedeća podjela alata [17]:

Prema načinu implementacije:

- Hardverski alati
- Softverski alati

Prema tipu koda:

- Otvorenog koda
- Licencirani

Prema platformi na kojoj rade:

- Windows platforma
- Linux i druge platforme.

Prema području primjene:

- Forenzika računalnih mreža
- Forenzika računalnih sustava
- Analiza drugih digitalnih uređaja
- Forenzika softvera

Prema fazi procesa koji obavljaju u forenzičkoj istrazi:

- Formiranje sterilnih medija
- Formiranje fizičke kopije tvrdog diska
- Oporavak podataka
- Dešifriranje podataka
- Analiza digitalnog materijala
- Formiranje dokumentacije

5.1.Alati za analizu programa

Nakon obavljene istrage i predstavljanja njezinih rezultata, dokazi se temeljito proučavaju u sudskom procesu. Razvijeno je mnogo alata koji stručnjacima pomažu u pregledavanju, pretraživanju i analizi dokaza.

Programski alati za upravljanje podacima na čvrstom disku su [17]:

- *PD Block*– alat tvrtke *Digital Intelligence* koji sprječava pisanje po izvornom disku prilikom forenzičkog kopiranja diska,
- *DriveSpy*- alat temeljen na operacijskom sustavi DOS sa sučeljem sličnim istom, koji omogućuje stvaranje forenzičke kopije diska, obnavljanje obrisanih podataka i neiskorištenih dijelova sektora te analizu upotrebom kriptografskog sažetka,
- *ForensicReplicator* – alat tvrtke *Parben Forensics Tools* za forenzičko kopiranje različitih medija,
- *FTK Imager* – alat tvrtke Access Data Corporation za forenzičko kopiranje,
- *Snap Back Exact*– alat tvrtke Snap Back koji služi za forenzičko kopiranje diska,
- *DiskSig*– alat tvrtke NTI koji služi za provjeru autentičnosti forenzičke kopije diska i
- *GetFree*– alat tvrtke NTI koji služi za kopiranje oslobođenog prostora diska, spremanje tih podataka na drugi medij te njihovu analizu.

Alati za obnovu podataka su:

- *Ontrack* – program za obnavljanje podataka izbrisanih s diska,
- *AcoDisk* – program za obnovu podataka s optičkih medija i

- *Media Merge* - alat tvrtke *Computer Conversions* koji služi za obnavljanje podataka s optičkih medija i tvrdih diskova.

Preglednici binarnih datoteka:

- *010 Hex editor* – alat tvrtke Sweet Scape koji služi za pregledavanje binarnih datoteka
- *Hex Workshop* – programski paket tvrtke Break Point koji služi za pregledavanje i upravljanje datotekama, predviđen za rad na operacijskom sustavu Windows.

Višenamjenski programski paketi:

- *EnCase*– programski paket tvrtke Guidance Software, jedan od najpotpunijih forenzičkih programskih paketa,
- *Maresware*– alat tvrtke Maresand Company koji sadrži kolekciju korisnih alata za forenziku na mjestu zločina
- *Access Data*.

Besplatni forenzički alati [16]:

- *Sleuth Kit* – biblioteka i kolekcija komandno-linijskih alata koji omogućuju pretraživanje diska i datotečnog sustava,
- *Helix*[11]– skupina forenzičkih alata koja uključuje Sleuth Kit i mnoge druge aplikacije,
- *Foremost* – alat za pretraživanje slikovnih datoteka i različitih datotečnih sustava, kao što su Linuxext2/ext3, Linux swap, UFS, JFS, NTFS, FAT12, FAT16, FAT32,
- *F.I.R.E.* (eng. *Forensicand Incident Response Environment*) – samostalna skupina alata koja se pokreće kada se upali računalo,
- *Forensic Toolkit, Bin Text, Galleta, NT Last, Pasco, Patchit, Rifiuti, i ShoWin* – alati posebno namijenjeni operacijskom sustavu Windows,
- *Win Hex*– alat za upravljanje datotekama, diskovima i radnom memorijom u heksadekadskom formatu,
- *SMART Linux* – Linux distribucija posebno osmišljena za forenzičku analizu dokaza. Sadrži alate za analizu podataka, pretraživanje i odgovor na sigurnosni incident.,
- *Wireshark*– alat za analizu mrežnog prometa,
- *NTFSWalker*– alat za analizu NTFS datotečnog sustava

[11] Program korišten za prikaz slučaja u poglavlju

Iako postoji mnogo forenzičkih alata, besplatnih i komercijalnih, bez stručnog nadzora moguće je uništiti dokaze, a time i sudski proces. Potrebno je naglasiti da forenzičku istragu prema tome može kvalitetno i pravovaljano voditi isključivo forenzički stručnjak.

5.2. Alati za analizu diska

Čvrsti disk je sastavni dio računala i obično se na njemu nalazi operacijski sustav koji sadrži različite programske pakete. Većina forenzičkih alata može se pokrenuti s jednog takvog sustava, odnosno običnog računala. No, ukoliko je potrebno zasebno analizirati dijelove računala, kao što su čvrsti diskovi, optički mediji, USB memorijske kartice, mobilni uređaji i slično, potrebna je posebna oprema [22].

Postoji nekoliko proizvođača takvih forenzičkih uređaja za analizu dokaznog materijala (dijelova računala za pohranu podataka) i najvažniji među njima su *Digital Intelligence* i *Vogon International*.

Proizvodi tvrtke Digital Intelligence su [14]:

- forenzički sustavi - Fred, Freddie, Fred SR, Fred-M, Fred-C,
- uređaji za prikupljanje podataka - Forensic Talon Kit, Forensic Talon, Forensic MD5 Kit, Forensic MDP, Clone Card PRO, OmniPort,
- prijenosni uređaji - CellDEK, Mobile Response Kit, Wireless StrongholdBag, STE3000F RFEnclosure, RemoteCharger,
- uređaji za obradu optičkih medija (CD, DVD) - FAR LITE, FAR PRO i
- uređaji za kopiranje (kloniranje) podataka - Echo Plus, Sonix, OmniClone 2Xi, OmniClone 5Xi,OmniClone 10Xi, OmniSCSI 1, OmniSCSI 4, OmniWipe.

5.3.PyFlag

FLAG (engl. *Forensic and Log Analysis GUI*) je programski alat za forenzičku analizu i analizu log zapisa. Korisničko sučelje, koje je neizostavni dio ovog alata, namijenjeno je jednostavnijem i praktičnijem provođenju navedenih aktivnosti. Uobičajeno je da ovakve analize zahtijevaju provjeru i korelaciju velikih količina podataka, te stoga FLAG u pozadini koristi bazu podataka za lakšu i bržu manipulaciju podacima [22].

PyFlag je implementacija FLAG alata u *Python*[12] programskom jeziku, objektno-orijentiranom skriptnom jeziku koji je postao iznimno popularan zbog svoje jednostavnosti i

[12]**Python** je programski jezik opće namjene, interpretiran i visoke razine kojeg je stvorio Guido van Rossum 1990. godine (prva javna inačica objavljena je u veljači 1991. godine).

portabilnosti te brojnih naprednih karakteristika koji programerima olakšavaju izradu aplikacija. PyFlag programom upravlja se putem Web sučelja, što omogućuje njegovo pokretanje na poslužitelju, te istovremeni rad više korisnika. Također, integritet pojedinih aktivnosti unutar aplikacije je osiguran, budući da se različiti podaci pohranjuju u zasebne instance, zvane slučajevi (engl. *cases*)[22].

5.3.1.Korištenje alata

Glavni izbornik (Slika 9) nudi pet opcija koje se dalje mogu proširiti [23]:

1. ***Case Management*** – izbornik u kojem se upravlja pojedinim slučajevima. Moguće je otvoriti novi slučaj, ukloniti neki već postojeći ili samo izbrisati podatke iz nekog od slučajeva
2. ***Load Data*** – u ovom izborniku se za odabrani slučaj učitavaju ulazni podaci
3. ***Disk Forensics*** – glavni izbornik forenzičke analize u kojem se nude sve dostupne forenzičke metode koje PyFlag podržava.
4. ***Index Tools***– U sklopu PyFlaga dolazi i alat za indeksiranje. Putem ove opcije dolazi se do sučelja u kojem je moguće izgraditi rječnik ključnih rijeci, koji će naknadno biti korišten u forenzičkoj analizi
5. ***Log Analisys***– Kroz ovu opciju moguće je pregledati sadržaj odabranog log zapisa ili kreirati predložak koji će se koristiti za jasnije prikazivanje sadržaja nekog log zapisa. Kao dodatna opcija nudi se i WHOIS pretraživanje, međutim, za korištenje ove mogućnosti potrebno je dohvatiti *whois* bazu podataka. U sklopu alata dolazi i skripta čijim se pokretanjem sadržaj besplatne *whois* baze prebacuje u MySql tablice PyFlaga. Ukoliko se skripta ne izvrši, ovu opciju neće biti moguće koristiti, te će svi upiti biti razriješeni kao *unknown*

Slika 9: Glavni izbornik PyFlag alata [22]

5.3.2.Analiza log zapisa

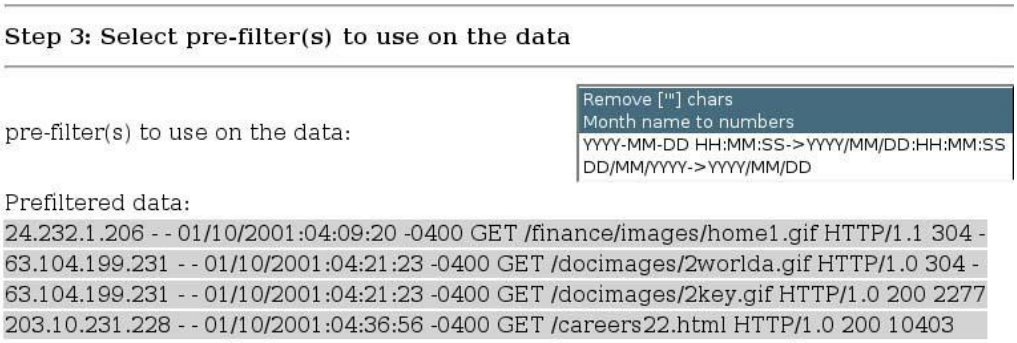
Analiza log zapisa jedna je od značajnijih forenzičkih metoda koja se, međutim, vrlo često koristi izvan forenzičkog konteksta. Prilikom analiziranja log datoteka javljaju se problemi kao što je nepostojanje njihovog standardnog formata, veličina log datoteka, vremenska razlika i sl. Različite aplikacije generiraju različite formate log datoteka, pa cak i iste aplikacije mogu generirati drukčije formate zbog različitih konfiguracijskih postavki. PyFlag pokušava razriješiti ove probleme slijedećim pristupom [24]:

- Postoje predlošci log datoteka. Ovime se log datoteka može učitati u unaprijed definirani format koji olakšava čitanje log zapisa. Predloške je moguće kreirati s obzirom na najpogodniji prikaz, mijenjati ih te pohraniti za buduću upotrebu.
- Svi podaci se pohranjuju u bazu podataka uz prikladno indeksiranje. Ovime se pretraživanje i grupiranje log podataka obavlja vrlo brzo.

Prvi korak u analiziranju novog formata log datoteke je kreiranje predloška kojim će se olakšati pregledavanje log zapisa. Ovime se PyFlag alatu definira format log datoteke, kako bi se moglo izvršiti izdvajanje i indeksiranje dijelova zapisa korištenjem prikladnih tipova podataka. Nakon ove procedure, u analizi je dostupno sučelje za brzo pretraživanje, grupiranje, sortiranje itd.Za kreiranje log predloška potrebna je log datoteka koja će poslužiti kao ogledni primjerak [21].

Na stranicama PyFlag projekta moguće je dohvatiti neke standardne datoteke koje mogu poslužiti kao ulazni podaci za testiranje PyFlaga. U prezentiranom primjeru korištena je *access* log datoteka Apache poslužitelja. Pod opcijom ***Log Analysis*** odabere se ***Create Log Preset***, te se u prvom koraku traži učitavanje ulazne datoteke. PyFlag vidi samo one datoteke koje su smještene u *Upload* direktoriju definiranom pri prvom pokretanju PyFlaga, tako da je bitno da se željeni ulazni podaci smjeste u odabrani direktorij. Nakon što se podaci učitaju, nudi se mogućnost podešavanja pojedinih parametara. Moguć je odabir separatora polja (Slika 10.), te podešavanje filtara koji će biti korišteni nad ulaznim podacima (Slika11.) [24].

Slika 10: Odabir separatora polja[22]



Slika 11: Podešavanje filtera [22]

5.3.3.Hash usporedba

Hash usporedba datoteka, odnosno usporedba sažetaka, je jedna od tehnika koja se primjenjuje u postupcima forenzičke analize. Da bi se ova tehnika koristila u sklopu PyFlag alata potrebno je dohvatiti *hash* bazu podataka za brzo klasificiranje datoteka.

NIST institut održava najveću javno dostupnu bazu sažetaka. NSRL (engl. *The National Software Reference Library*) je ostvaren od strane NIST-a s ciljem prikupljanja programskih paketa iz različitih izvora, te ugradnju njihovih sažetaka u skup referentnih podataka nazvan RDS (engl. *Reference Data Set*) [17].

Posljednja inačica ove kolekcije digitalnih potpisa poznatih programskih paketa sadrži 10 533 722 jedinstvenih SHA-1, MD5 i CRC32 vrijednosti. U sklopu PyFlag alata dolazi skripta koja izvršava punjenje NSRL baze u PyFlag MySQL bazu podataka [18]:

```
/pyflag# ./utilities/nsrl_load.sh
Usage: nsrl_load.py path_to_nsrl_directory
An NSRL directoryis one oftheCDs, andusuallyhasinit
NSRLFile.txt,NSRLProd.txt.
```

Da bi se iskoristila ova skripta potrebno je dohvatiti RDS datoteku u ISO formatu sa stranica NIST instituta, te uputiti skriptu na lokaciju gdje je datoteka pohranjena. Ove datoteke su podijeljene na 4 kategorije, te ih je moguće dohvatiti odvojeno, ovisno o potrebi.

S obzirom na sadržaj ovih datoteka njihove veličine variraju od 200 do 500 MB-a, te stoga dohvaćanje ovih datoteka može predstavljati problem. Ova je opcija PyFlaga zato samo opcionalna. Alat će raditi i bez učitavanja NSRL baze sažetaka, međutim ova tehnika u tom slučaju neće biti dostupna prilikom provođenja postupka forenzičke analize [17].

5.3.4.Priprema tvrdog diska

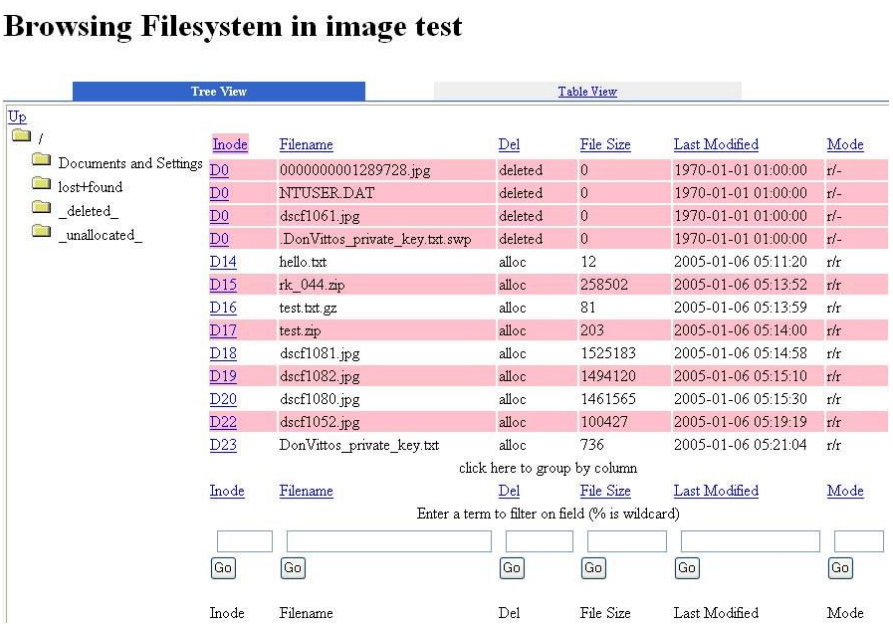
Do preslike tvrdog diska (engl. *hard disk image*) se uobičajeno dolazi u fazi analize incidenta, najčešće korištenjem distribucije Linux operacijskog sustava koju je moguće pokrenuti sa CD-a (npr.Knoppix) na kompromitiranom računalu. Operacijski sustav će prepoznati tvrdi disk te ga učiniti dostupnim putem/dev/ direktorija. Rad sa velikim količinama podataka koje se očekuju prilikom analize tvrdih diskova može biti vrlo nepraktičan, pogotovo jer velika količina dostupnog prostora ostaje neiskorištena. Iz ovog razloga većina forenzičkih alata osigurava i neku vrstu kompresije. Standardni programi za kompresiju, poput *zip-a* i *gzip-*

a nisu pogodni za ovakvu vrstu posla, jer svako novo pretraživanje u ovim formatima zahtjeva dekompresiju cijelog niza podataka [22].

Forenzička kompresija se uglavnom obavlja u formatu koji komprimira manje blokove podataka, cime se osigurava brže pretraživanje. Jedan od popularnijih formata nosi naziv *sgzip*. Ovo je format koji se bazira na *gzip* kompresiji, ali omogućava pretraživanje(engl. *seekable gzip*).

5.3.5. Analiza učitanih podataka

U VFS-u (engl. *Virtual File System*) je moguće pregledati sve zapisane direktorije i datoteke. Na slici 12 se može vidjeti da su osim direktorija koji su postojali u originalnom datotečnom sustavu dodani i virtualni direktoriji *_deleted_*za rekonstruirane obrisane datoteke, te *_unallocated_* za datoteke pronađene u nelociranom prostoru diska. Obrisane datoteku su one o kojima je informacija, odnosno *inod*[13]struktura, ostala sačuvana [25].



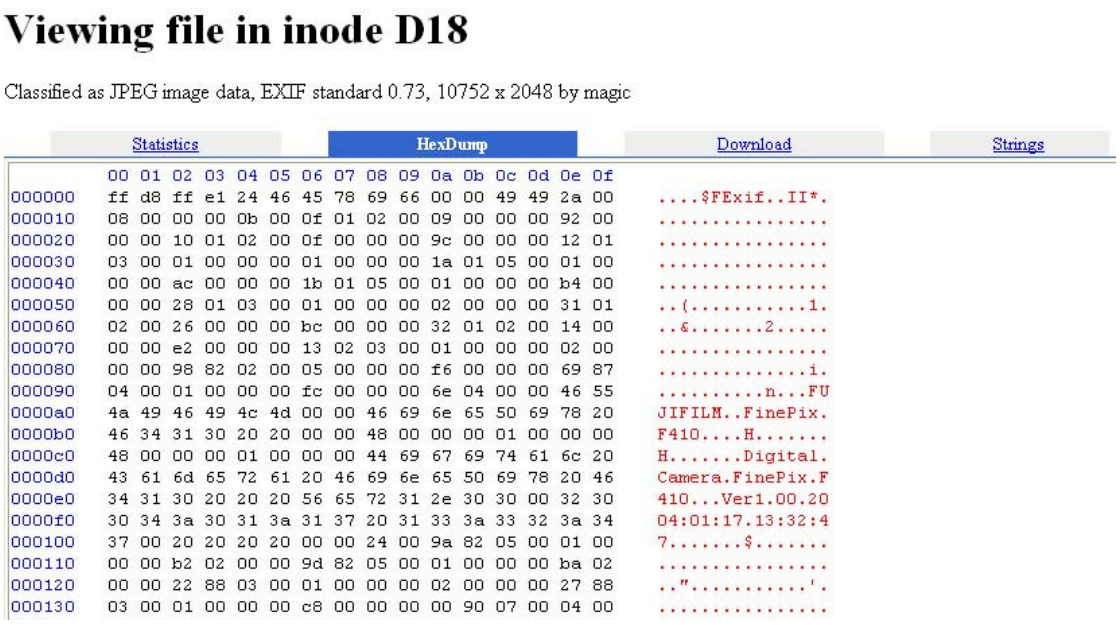
Slika 12: Virtualni datotečni sustav [25]

Iz ovih informacija je poznata lokacija njihovih alociranih blokova, te ih je moguće rekonstruirati. Originalno ime datoteke nije moguće saznati jer informacije direktorija, gdje se pohranjuju imena datoteka, ne spominju ove obrisane datoteke. Za pobliže ispitivanje određene

[13]*Inode je* osnovni gradivni blok ext2 sistema

datoteke, moguće joj je direktno pristupiti, pri ćemo se otvara sučelje za datoteke, koje sadrži više načina prikaza datoteka.

Datoteku je moguće pregledati u heksadecimalnom i ASCII zapisu, a moguće je pregledati i statistiku odabrane datoteke, te je dohvatiti na lokalno računalo. Na slici 13. je prikazan heksadecimalni zapis jedne od slika pronađenih na disku.



Viewing file in inode D18

Classified as JPEG image data, EXIF standard 0.73, 10752 x 2048 by magic

Statistics | HexDump | Download | Strings

```
        00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
000000  ff d8 ff e1 24 46 45 78 69 66 00 00 49 49 2a 00  ....$FExif..II*.
000010  08 00 00 00 0b 00 0f 01 02 00 09 00 00 00 92 00  ................
000020  00 00 10 01 02 00 0f 00 00 00 9c 00 00 00 12 01  ................
000030  03 00 01 00 00 00 01 00 00 00 1a 01 05 00 01 00  ................
000040  00 00 ac 00 00 00 1b 01 05 00 01 00 00 00 b4 00  ................
000050  00 00 28 01 03 00 01 00 00 00 02 00 00 00 31 01  ..(...........1.
000060  02 00 26 00 00 00 bc 00 00 00 32 01 02 00 14 00  ..&.......2.....
000070  00 00 e2 00 00 00 13 02 03 00 01 00 00 00 02 00  ................
000080  00 00 98 82 02 00 05 00 00 00 f6 00 00 00 69 87  ..............i.
000090  04 00 01 00 00 00 fc 00 00 00 6e 04 00 00 46 55  ..........n...FU
0000a0  4a 49 46 49 4c 4d 00 00 46 69 6e 65 50 69 78 20  JIFILM..FinePix.
0000b0  46 34 31 30 20 20 00 00 48 00 00 00 01 00 00 00  F410....H.......
0000c0  48 00 00 00 01 00 00 00 44 69 67 69 74 61 6c 20  H.......Digital.
0000d0  43 61 6d 65 72 61 20 46 69 6e 65 50 69 78 20 46  Camera.FinePix.F
0000e0  34 31 30 20 20 20 56 65 72 31 2e 30 30 00 32 30  410...Ver1.00.20
0000f0  30 34 3a 30 31 3a 31 37 20 31 33 3a 33 32 3a 34  04:01:17.13:32:4
000100  37 00 20 20 20 20 00 00 24 00 9a 82 05 00 01 00  7.......$.......
000110  00 00 b2 02 00 00 9d 82 05 00 01 00 00 00 ba 02  ................
000120  00 00 22 88 03 00 01 00 00 00 02 00 00 00 27 88  ..".........'.
000130  03 00 01 00 00 00 c8 00 00 00 00 00 90 07 00 04 00  ................
```

Slika 13: Heksadecimalni zapis datoteke [22]

5.3.6.Dodatne mogućnosti

Osim navedenih mogućnosti koje su analizirane u dosadašnjem dijelu dokumenta, PyFlag posjeduje i brojne dodatne mogućnosti koje ne treba zanemariti. Prije svega, treba naglasiti mogućnost rekonstrukcije RAID polja. Pri forenzičkim analizama i analizama incidenata, vrlo cesto se susreću računalni sustavi koji koriste RAID sustave.

Stvaranje preslika ovakvih diskova je vrlo komplicirano jer je rekonstrukcija RAID polja bez identičnog kontrolora koji je korišten za stvaranje polja ili identične konfiguracije izuzetno teška. Moguće je i da RAID kontrolor ne prihvaća diskove zbog oštećenih ili prepisanih zaglavlja, te je stoga nemoguće rekonstruirati logičke dijelove standardnom metodom. U ovom dokumentu neće biti rijeci o rekonstrukciji RAID polja upotrebom PyFlag alata, ali je bitno napomenuti da PyFlag posjeduje tu mogućnost, te je detalje o slijedu postupaka moguće pronaći u PyFlag dokumentaciji dostupnoj na stranici alata [26].

Uz PyFlag je moguće koristiti i *Fuse* programski paket. *Fuse* je projekt koji omogućuje zapis datotečnog sustava u korisnički prostor. Zapisom datotečnog sustava u korisnički prostor, umjesto u prostor jezgre, omogućuje se korištenje zbirki datoteka (engl. *library*) i jezika više razine. U PyFlagu programski paket *Fuse* služi za proširenje mogućnosti ovog alata, kao što je montiranje većeg broja virtualnih datotečnih sustava koji potom omogućuju montiranje komprimiranih preslika preko standardnog *loopback drivera* jezgre, ili mogućnost korištenja grep i find naredbi u montiranom datotečnom sustavu [27].

5.4. The Coroner's Toolkit programski paket

TCT programski paket sastoji se od skupa alata, od kojih su neki pisani u *Perl*, a neki u *C* programskom jeziku. Osnovna im je namjena prikupljanje i analiza podataka sa kompromitiranih sustava. Program nije vezan uz točno određeni zadatak ili funkciju, tako da je teško u jednoj rečenici opisati sve njegove mogućnosti i kvalitete.

Ugrađene funkcionalnosti korisnicima omogućuju automatizirano prikupljanje informacija sa kompromitiranih sustava te jednostavniju rekonstrukciju prethodnih događaja. Važno je napomenuti da je TCT alat namijenjen statičkoj analizi sustava, što znači da se analizira stanje računala u trenutku pokretanja programa. Sve aktivnosti koje se u tom trenutku odvijaju na sustavu (kopiranje datoteka, mrežne konekcije, stanja procesa) TCT program neće zabilježiti. Osnovne komponente koje čine program su [28]:

- *Grave-robber,*
- *Mactime,*
- *Unrm,*
- *Lazarus*.

5.4.1.Grave-robber

Grave-robber program predstavlja jezgru TCT programskog paketa i njegova je primarna namjena **prikupljanje** informacija s kompromitiranog računala. Program je realiziran kao *Perl* skripta koja pokreće ostale potprograme zadužene za pojedine zadatke, od kojih je većina napravljena u obliku *Perl* modula smještenih u *lib* poddirektoriju TCT programskog paketa. Način rada programa, tip i količina podataka koji se žele prikupljati, zajedno s njihovom lokacijom, može se kontrolirati uređivanjem konfiguracijske datoteke programa (*$TCT_HOME/conf/grave-robber.conf* i *coroner.conf*) ili prosljeđivanjem odgovarajućih opcija programu [29].

Program je realiziran tako da prvo prikuplja one podatke za koje je poznato da imaju kraći "vijek trajanja" u odnosu na ostale podatke. Naime, dobro je poznato da na računalu postoje različite kategorije podataka s obzirom na njihovu postojanost (npr. radna memorija u odnosu na tvrdi disk), a *grave-robber* program ovu činjenicu uzima u obzir. Program prvo prikuplja informacije iz radne memorije kao što su podaci o pokrenutim procesima, stanjima mrežnih konekcija i sl., nakon čega slijedi postupak prikupljanja podataka s tvrdog diska. Inicijalni direktorij pregledavanja datotečnog sustava moguće je zadati navođenjem njegovog imena prilikom pokretanja programa. Bez eksplicitno navedenog imena direktorija, program prikuplja podatke u odnosu na *root* (/) direktorij, što je ujedno i preporučljiv način njegova korištenja. Iako je program moguće pokrenuti pod bilo kojim korisničkim računom, najbolje ga je pokretati pod ovlastima *root* korisnika, budući da većina aktivnosti programa zahtijeva najviše ovlasti na sustavu [28].

5.4.2.Mactime

Mactime je vrlo jednostavan i moćan program koji omogućuje prikupljanje i analizu informacija o MAC vremenima pojedinih datoteka i direktorija. Program se može pokretati ili zasebno ili u kombinaciji s *grave-robber* programom, odnosno sa *body* i *body*. *Mactime* program za dolazak do odgovarajućih vremena pristupa koristi *stat()* i *lstat()*pozive sustava. Osim općenitih parametara kojima je moguće preciznije definirati način rada programa, program dodatno prima i parametre *time1* i*time2* kojima se određuje vremenski period za koji se provodi analiza [29].

Neke od općenitih opcija *mactime* programa navedene su u nastavku [28]:

-b – alternativna lokacija *body* datoteke koja se koristi kao izvor podataka (bez ove opcije koristi se inicijalna lokacija definirana coroner.cf konfiguracijskom datotekom).

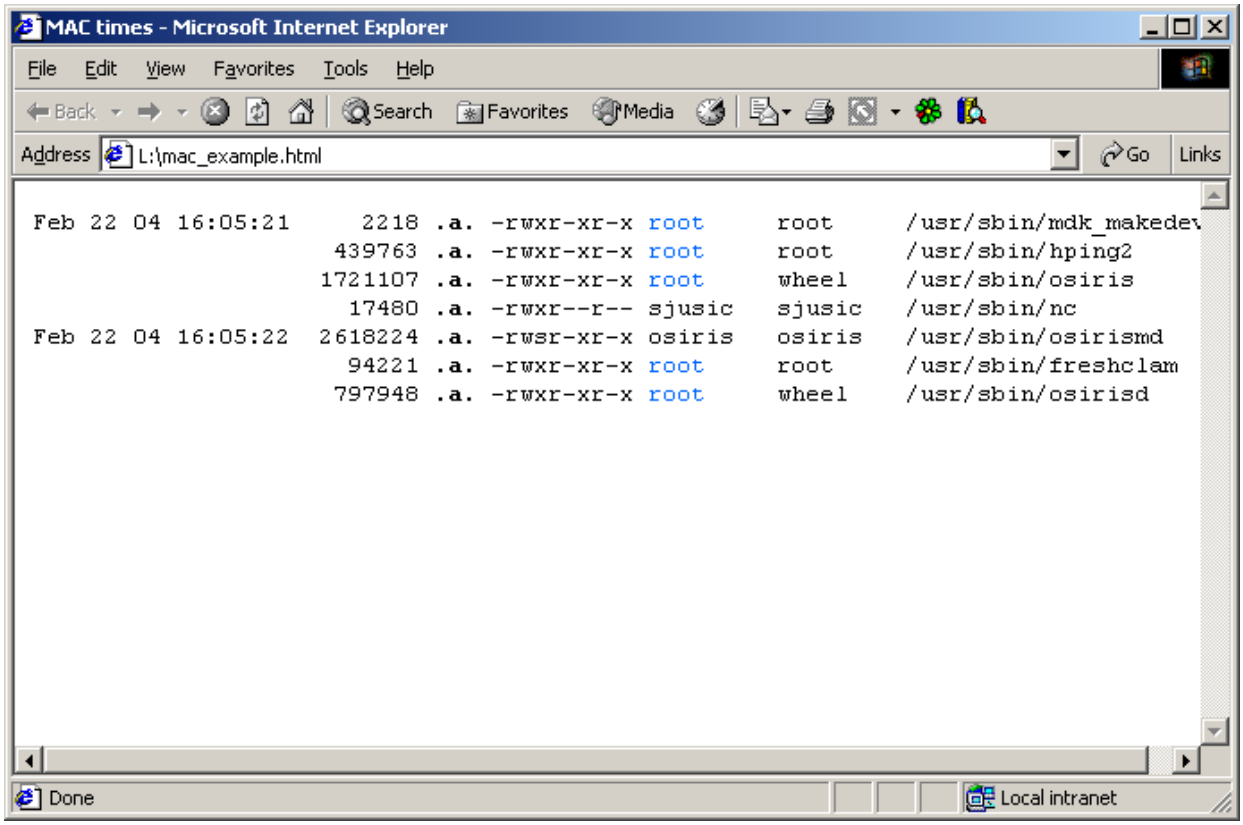
-d – prikupljane i analiza MAC vremena provodi se u odnosu na zadani direktorij, a ne na temelju *body* datoteke generirane od strane *grave-robber* programskog paketa. Ova opcija koristi se u slučajevima kada se *mactime* program koristi neovisno od *grave-robber* programa.

-R – rekurzivno pregledavanje u odnosu na direktorij zadan opcijom –R.

-h – ispis u HTML formatu (Slika 14).

-u – datoteke u vlasništvu navedenog korisnika obilježit će se drugom bojom (Slika 3).

-D – debug opcija; program ispisuje vrlo detaljne poruke o radu.



Slika 14:Ispis mactime programa u HTML formatu [28]

5.4.3. Unrm

Unrm program omogućuje rekonstrukciju podataka iz ne alociranog područja datotečnog sustava. Podaci prikupljeni *Unrm* programom tipično se koriste u kombinaciji s *Lazarus* programom, koji prikupljene podatke pokušava organizirati u smislene cjeline. Prilikom korištenja *Unrm* alata potrebno je u obzir uzeti veličinu datotečnog sustava s kojeg se obnavljaju podaci kao i veličinu nezauzetog prostora. Također je vrlo važno da se prikupljeni podaci ne pohranjuju na isti datotečni sustav koji se analizira, budući da će to gotovo uvijek rezultirati prepisivanjem podataka koji se žele obnoviti. Veličina nezauzetog prostora posebno je važan parametar, budući da je istu količinu prostora potrebno osigurati na mediju na kojeg se vrši pohrana prikupljenih podataka [28].

5.4.4.Lazarus

Kako je već ranije spomenuto, *Lazarus* programski paket namijenjen je obnavljanju izbrisanih podataka sa sustava, najčešće iz ne alociranog područja na tvrdom disku, iako je moguće prikupljanje podataka i iz drugih izvora (radna memorija, *swap* i sl.). Program je pisan u *Perl* programskom jeziku. Iako *Lazarus* može raditi na podacima iz različitih izvora (npr. sliku

datoteka dobivena d.d. programom), program daje najbolje rezultate u kombinaciji sa *Unrm* programom spomenutom u prethodnom poglavlju [29].

6.CERTIFIKACIJA FORENZIČKIH ISTRAŽITELJA

Forenzika je multidisciplinarno i interdisciplinarno područje. U razvijenim zemljama, naročito SAD-u, postojanje diplomskih studija forenzike dovelo je do kvalitetnog i učinkovitog rada pravosuđa.

U Hrvatskoj je 2009. osnovan *Studij forenzičkih znanosti* na Sveučilištu u Splitu. Do tada nije postojala jedinstvena škola ili fakultet na kojem je bilo moguće izučiti forenzičku znanost. U Hrvatskoj postoje sljedeći forenzički laboratoriji:

- Zavod za sudsku medicinu zagrebačkog Medicinskog fakulteta,
- Laboratorij za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava, Fakultet prometnih znanosti u Zagrebu
- MUP-ov Centar za kriminalistička vještačenja Ivan Vučetić te
- Splitski forenzički laboratorij.

U SAD-u postoji nekoliko forenzičkih certifikata koje istražitelji moraju imati kako bi mogli svjedočiti na sudu. Jedan od certifikata koji nije vezan uz proizvođača programskih alata je GIAC (eng. *Global Information Assurance Certification*), a forenzičar koji posjeduje taj certifikat postaje certificirani GIAC forenzički analitičar (eng. *GIAC Certified Forensic Analyst - GCFA*). U siječnju 2010. spomenuti certifikat je akreditiran po programu ANSI/ISO/IEC 17024 za certifikaciju osoblja. Organizacija IACRB (eng. *Information Assurance Certification Review Board*) sponzorira CCFE (eng. *Certified Computer Forensics Examiner*) certifikaciju. Kandidati moraju proći pismeni ispit na kojem moraju imati 70% ili više točnih odgovora. Kandidati koji prođu spomenuti ispit dobivaju dokazne datoteke u obliku kopije čvrstog diska. Datoteke moraju analizirati i predati na ocjenjivanje [30].

IACIS (eng. *International Association of Computer Investigative Specialists*) nudi obavljanje certifikacije računalnih forenzičara od 1994. godine. U početku je to bio „MS-DOS Processing Certificate“ (DPC), a kasnije CFCE (eng. *Certified Forensic Computer Examiner*) koji osposobljava kandidate za rad s forenzičkim kopijama te rješavanje problema koji se javljaju pri analizi digitalnog dokaznog materijala [31].

Različite računalne tvrtke nude certifikate posebno namijenjene za rad s njihovim programskim paketima. Na primjer, za rad s alatom EnCase izdaje se EnCE certifikat (eng. *Encase Certified Examiner*), a za alat Access Dana ACE certifikat. EnCE certifikacija se obavlja od 2001. godine [32].

Forenzički istražitelji obično počinju svoju karijeru u policiji i sličnim vladinim organizacijama ili u tvrtkama koje se bave računalnom sigurnošću. U današnje vrijeme za forenzičke stručnjake se zahtjeva, da imaju barem završeni preddiplomski ili diplomski studijski program iz područja društvenih i humanističkih znanosti, medicine, biomedicine i zdravstva, biotehnologije, tehničkih znanosti ili prirodnih znanosti.

7.ZAKONSKA REGULATIVA I RAČUNALNA FORENZIKA

Zakon ima presudan utjecaj na računalnu forenziku jer ima stroga pravila o prihvaćanju prikupljenih podataka kao dokaza. Da bi se prikupljene informacije uistinu smatrale dokaznim materijalom, mora se održati visoka razina formalnosti u postupanju s računalom i njegovim spremnicima.

Posebna briga se mora voditi kada se pristupa podacima osumnjičenika, virusima, elektromagnetskim i mehaničkim oštećenjima, a ponekad i računalnim zamkama (eng. *Booby-traps*). Postoji nekoliko pravila kojih se treba pridržavati kako se ne bi ugrozila pravna upotrebljivost dokaza [6]:

- koristiti samo alate i metode koje su prethodno ispitane i ocjenjene. Ispitivanje alata provode institucije poput proizvođača programskih paketa, vladinih organizacija (na primjer *Defense Cyber Crime Institute* iz SAD-a) i druge,
- originalne dokaze treba što manje mijenjati i odložiti na sigurno mjesto,
- zapisivati sve što je napravljeno jer je dokumentacija na kraju dio izvještaja,
- istražitelj treba poštovati vlastito znanje ili neznanje, tj. raditi samo ono u što je siguran da zna.

Također, potrebno je paziti na osjetljivost informacija do kojih se došlo pretragom, a koje nisu vezane za one podatke koji nas zanimaju. Zakoni nisu isti u svim državama, ali su im namjene i namjere jednake. U istragama kod kojih vlasnik digitalne opreme nije dao pristanak za inspekciju, a to su krivične istražne radnje, posebno se mora paziti da stručnjak za računalnu forenziku ima sve dozvole i zakonski autoritet za pregledavanje, kopiranje, otuđivanje i korištenje svih uređaja i njihovog sadržaja (odgovarajući sudski nalog).

Ako to nije slučaj, osim odbacivanja dokaza na sudu, teško je očekivati izbjegavanje pravne tužbe. Koliko god da je forenzička obrada bila vođena ispravnim principima, uvijek je moguće doći u situaciju u kojoj će dokaz biti odbačen. Isto tako, ponekad izostanak stvaranja forenzičke kopije čvrstog diska neće biti otežavajuća okolnost pri prezentaciji dokaza.

Digitalna forenzika je relativno nova znanstvena disciplina i zakoni koji su temelj za priznavanje elektroničkih dokaza na sudovima još su uvijek u stanju nedorečenosti. Konstantan napredak tehnologije dovodi do većeg broja dokaza i alata, a time i dokaznog materijala, što u nekim slučajevima može biti i loše jer dokazi nisu jasni. Ipak, računalna forenzika se ne koristi

samo u svrhe kriminalističke istrage. Alati i metode specifične za digitalnu forenziku koriste se i u svrhu povratka izgubljenih podataka kod običnih korisnika računala.

Također, koriste se i u velikim tvrtkama za zaštitu računalnih mreža. Novije zakonske legislative u zapadnim državama drže odgovornim tvrtke koje ne uspiju spriječiti otkrivanje i zlouporabu osobnih podataka svojih klijenata pa je bavljenje računalnom forenzikom ponekad način da se tvrtki sačuva ugled i novac.

Uzimajući za cilj usuglašavanje međunarodnih zakona iz područja „cyber – zločina“ , Vijeće Europe je, kao najstarije tijelo Europske Unije, postavilo temelje dokumenta nazvanog „Konvencija o kibernetičkom kriminalu“ (eng. *Convention on cybercrime*).

7.1.Konvencija o kibernetičkom kriminalitetu

Konvencija potpisana u studenom 2001., dokument je kojim je Vijeće Europe pokušalo dati smjernice u borbi protiv računalnog kriminala, pogotovo onog vezanog uz Internet. Konvenciju je potpisalo preko trideset zemalja [6].

Konvencija definira po grupama inkriminacije vezane uz Internet, pa redom imamo [11]:

- grupu djela protiv tajnosti, nepovredivosti i dostupnosti podataka spremljenih na računalima i samih sustava (ovdje spadaju takve povrede kao što su neovlašten pristup računalu, neovlašteno presretanje podataka, neovlašteno mijenjanje i uništavanje podataka, zloupotreba računala i programa radi počinjenja kažnjivih djela, ometanje nesmetanog rada računala itd.)
- kaznena djela poput prijevare i krivotvorenja uz pomoć računala
- kaznena djela vezana uz sadržaj podataka na računalima, prvenstveno uz distribuciju i širenje dječje pornografije
- djela vezana uz kršenje autorskih i srodnih prava

Nakon samih kaznenih djela slijede i odredbe o:

- sankcioniranju pomaganja i prikrivanja pri izvršenju gore navedenih kaznenih djela (čl. 11)
- kaznenoj odgovornosti pravnih osoba za navedena kaznena djela (čl. 12)
- dužnosti zemalja potpisnica da u svoj kaznenopravni sustav unesu odredbe koje će osigurati da kaznena djela mogu biti kažnjavana sa efektnim kaznama, uključivši i kaznu zatvora.

Na nekoliko mjesta u Konvenciji spominje se obveza zemalja potpisnica da u svoj pravni poredak unesu i odredbe koje će omogućiti i pristup i pretragu podataka na računalima korisnika osumnjičenih za počinjenje neke od inkriminacija gore opisanih, a koje su sadržane u odredbama članaka 2. do 10. Poseban je naglasak stavljen i na omogućavanje suradnje između zemalja potpisnica u vezi s istražnim radnjama. To je pogotovo očito u odredbama čl. 35 koji određuje dužnost zemalja potpisnica da osnuju službu koja će biti 24 sata na raspolaganju ako se pojavi potreba za suradnjom glede nadgledanja prometa na dijelu mreže u nadležnosti neke od zemalja potpisnica.

7.2.Stanje u Republici Hrvatskoj

U kazneno zakonodavstvo Republike Hrvatske preuzete su odredbe koje proizlaze iz obveza utvrđenih Konvencijom o kibernetičkom kriminalu VE i Direktivom EU-a o napadima na informacijske sustave. Međutim, način na koji su preuzete pravno-tehnički slabi njihovu uporabnu vrijednost. Temeljni pojmovi, kao što su računalni podaci, programi, mreža, u bitnim dijelovima različito su prevedeni, protumačeni i kroz zakonski tekst međusobno različito postavljeni [11].

Većina kaznenih djela kibernetičkog kriminala postavljena je šire od minimalnih okvira spomenutih međunarodnih izvora, dok su pojedina kaznena djela ostala nedorađena. Iako takva u radu opisana rješenja nisu zabranjena niti nepoznata na međunarodnoj razini, postavlja se pitanje njihove kriminalno-političke opravdanosti, poštivanja načela zakonitosti, prekomjerne kriminalizacije i standarda pravne zaštite i sigurnosti. S druge pak strane, uočljive su pravne praznine kad su u pitanju djela neovlaštenog ostajanja u računalnom sustavu i neovlaštenog pribavljanja računalnih podataka.

Takva rješenja nisu usamljena i preslika su stvarnog stanja na području kriminalizacija napada na informacijske sustave na međunarodnoj razini. S obzirom na ogroman doprinos informacijsko-komunikacijskih tehnologija razvoju društva, potrebno je slobode i prava koje ljudi imaju izvan kibernetičkog prostora osigurati i unutar kibernetičkog prostora, sa svim raspoloživim sredstvima, a kriminalizaciji napada pribjeći tek kao krajnjem sredstvu suzbijanja najtežih od njih [6].

U tom pogledu kao prikladnije rješenje kod blažih oblika napada bilo bi uvođenje i prekršajne odgovornosti po uzoru na druga posebna područja, čime bi se otvorio prostor za

detaljniju razradu složene terminologije i sveukupne problematike. Kod najtežih pojavnih oblika bit će potrebno popuniti ranije spomenute pravne praznine.

Za kraj, može se zaključiti da, bez obzira na pravni kontinuitet zaštite informacijskih sustava, programa i podataka u kaznenom zakonodavstvu Republike Hrvatske, i dalje ostaju otvorena pojedina pitanja koja su od važnosti za sveobuhvatno uređenje područja.

8.POSTUPCI RAČUNALNE FORENZIKE UPORABOM ODABRANOG FORENZIČKOG ALATA

8.1.Odabir forenzičkog alata – Helix 2009R1

Helix operacijski sustav spada u grupu sustava namijenjenih podizanju sa CD-ROM medija. To je posebna inačica poznate *Knoppix Linux* distribucije, koja je za razliku od drugih preinaka prilagođena za forenzičku analizu i reagiranje na incidentne (izvanredne) situacije. U tu svrhu, *Helix* je modificiran na način da nikad ne koristi *swap* particiju te da prepoznaje iste datotečne sustave koji su podržani i u *Knoppix* distribuciji (ext2, ext3, vfat, ntfs), ali također i *xfs, reiser, jfs* te mnoge druge datotečne sustave [34].

Važna funkcionalnost Helix distribucije je i mogućnost pokretanja u obliku samostalne aplikacije na Windows operacijskim sustavima (najbolje radi na Windows XP i nižim distribucijama). Pri tome su raspoloživi različiti alati namijenjeni za forenzičke svrhe u opsegu od 90MB. Tom funkcionalnošću Helix je razdijeljen u program koji analizira podignute Windows sustave te u Linux operacijski sustav koji se samostalno podiže. Zbog spomenute ograničene funkcionalnosti na novijim Windows operacijskim sustavima (*Windows Vista, Windows 7, Windows 8*), u samoj izradi forenzičke analize korišteni su i neki alati van *Helix* distribucije.

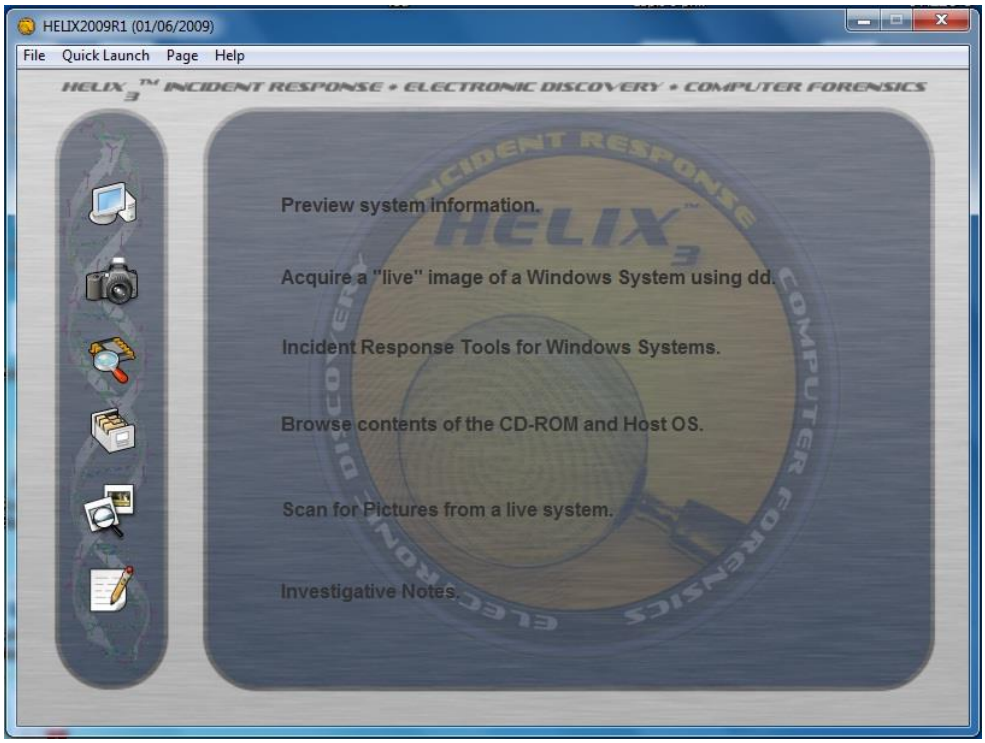
Helix distribuciju (Slika 15) je moguće preuzeti na stranici proizvođača. Samu distribuciju moguće je koristiti na dva načina: kao Linux operacijski sustav kojim se analizira isključeni sustav, te kao aplikaciju pokrenutu pod Windows operacijskim sustavom pomoću koje se analizira rad uključenog sustava.

Helix sadrži statične binarne datoteke za *Linux, Solaris* i *Windows* operacijske sustave, koristeći GNU i Cygwin alate. Također su dostupni i mnogi drugi forenzički alati. Iako je mnogo alata dostupno preko grafičkog sučelja, velik je broj i onih koji su dostupni samo iz komandne linije.

Slika 15: Distribucija Helix forenzičkog programa

8.2.Pokretanje na Windows operacijskim sustavima

Pri radu u Windows okruženju moguće je samo umetnuti *Helix* CD te kretanjem kroz njegov sadržaj pokrenuti potrebne forenzičke aplikacije (Slika 16). Sve binarne datoteke koje se koriste su statične tj. Pokreću se isključivo sa CD medija i ne koriste nikakve dodatne biblioteke ili datoteke sustava na kojem su pokrenute.



Slika 16: Grafičko sučelje forenzičkog programa Helix

Druga mogućnost pri radu na Windows operacijskim sustavima je korištenje *Helix.exe* aplikacije. Ukoliko je na računalu omogućeno automatsko pokretanje (eng. autorun), nakon umetanja CD-a, *Helix* aplikacija se automatski pokreće. U slučaju kada je automatsko pokretanje isključeno, aplikaciju je potrebno pokrenuti ručno. Nakon što se pokrene *Helix.exe*, korisniku je dostupno grafičko sučelje koje olakšava rad s dostupnim alatima.

Helix je na Windows operacijskim sustavima moguće koristiti na tri načina. Jedan je pokretanjem grafičkog sučelja pomoću Helix.exe izvršne datoteke, drugi je korištenjem komandne linije Helixa,a treći je izravno pokretanjem pojedinih programa koji su sadržani u Helix distribuciji korištenjem Windows Explorer programa. Preduvjet za pokretanje na zadnji način je da ti programi moraju imati grafičko sučelje.

Kao što je prethodno spomenuto, Helix se na Windows operacijskim sustavima izvršava kao zasebna aplikacija. Pri tome se prati aktivno stanje Windows sustava, tj. aktivni procesi,

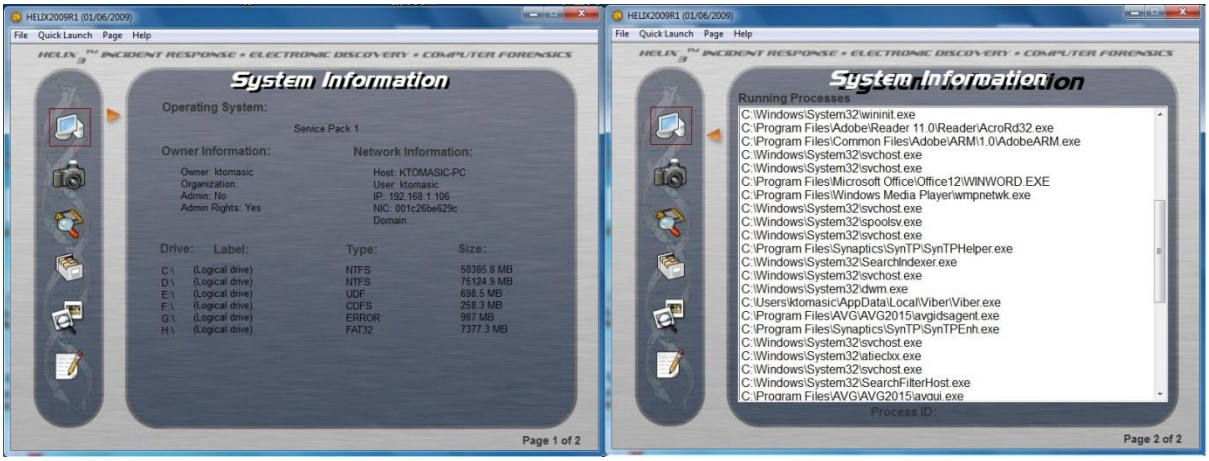
koji se kontinuirano mijenjaju, a tome dodatno doprinose i alati koji se pokreću s Helix CD-a. Ipak, pošto se gašenjem sustava mogu izgubiti važni forenzički podaci, mogućnost pokretanja forenzičkih alata tijekom rada sustava je veoma korisna.

Helix za Windows sustave se može koristiti za prikupljanje informacija sa sustava koji se ne smiju gasiti, a to su uglavnom poslužitelji. Svi pokrenuti alati pokreću se s privilegijama korisnika koji je trenutno prijavljen na sustavu. Ukoliko trenutni korisnik ima ograničena prava, na sustavu postoji mogućnost nepravilnog izvršavanja nekih alata. Iz tog se je razloga ponekad potrebno prijaviti na sustav s ovlastima administratora kako bi se osigurao nesmetan rad i potpuna funkcionalnost [35].

8.3.Administracijsko sučelje za Windows sustave

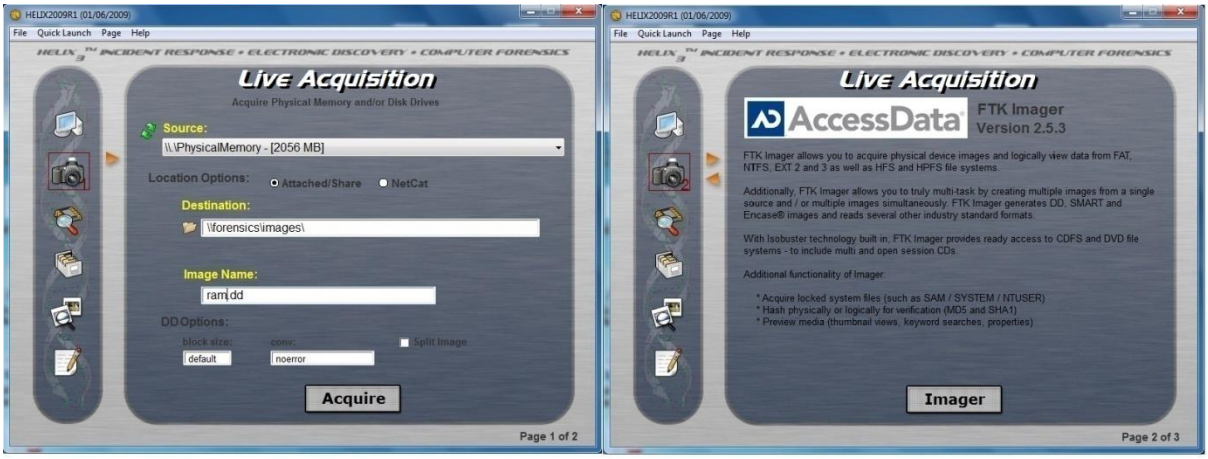
Važno je napomenuti da se za pokretanje grafičkog sučelja (Slika 16) koriste neke DLL datoteke sustava na kojem se pokreće Helix pokreće. Potrebne DLL datoteke nije moguće uključiti u Helix CD zbog različitosti između pojedinih inačica samih Windows operacijskih sustava. Samo grafičko sučelje podijeljeno je u više dijelova [34]:

- Preview System Information (Slika 17) – prikazuje se verzija operacijskog sustava te sažete informacije o diskovima i mrežnim sučeljima. Također je dostupan i popis svih aktivnih procesa na sustavu.



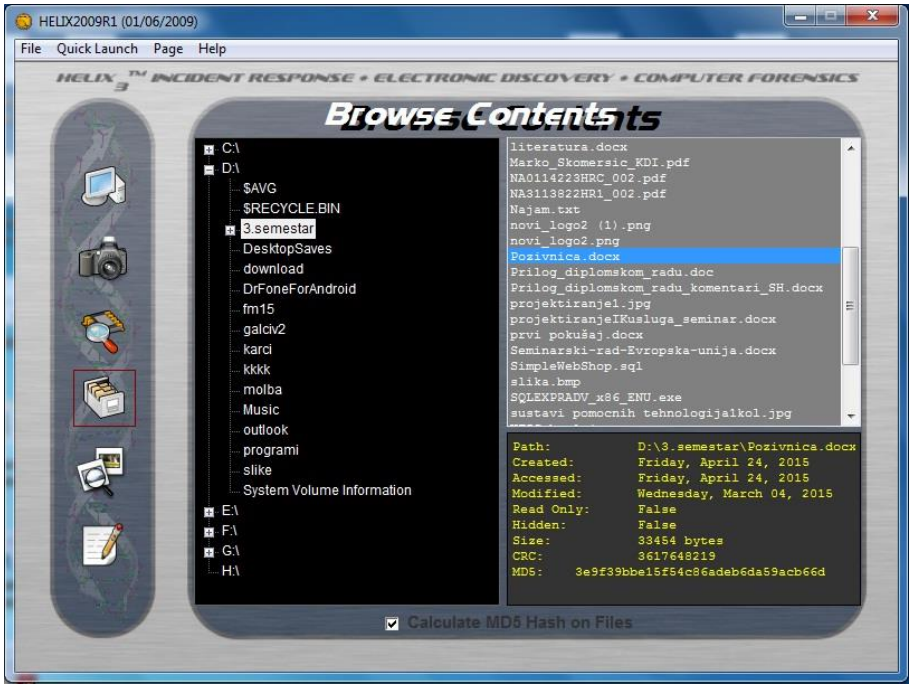
Slika 17: Izgled Preview System Information sučelja

- Acquire a „live“ image of a Windows System using d.d. (Slika 18) – služi za izradu kopija čvrstih diskova, disketa ili sadržaja memorije te za spremanje istih na CD, DVD ili drugo računalo na mreži, korištenjem dd (eng. Disk Duplicator) alata.



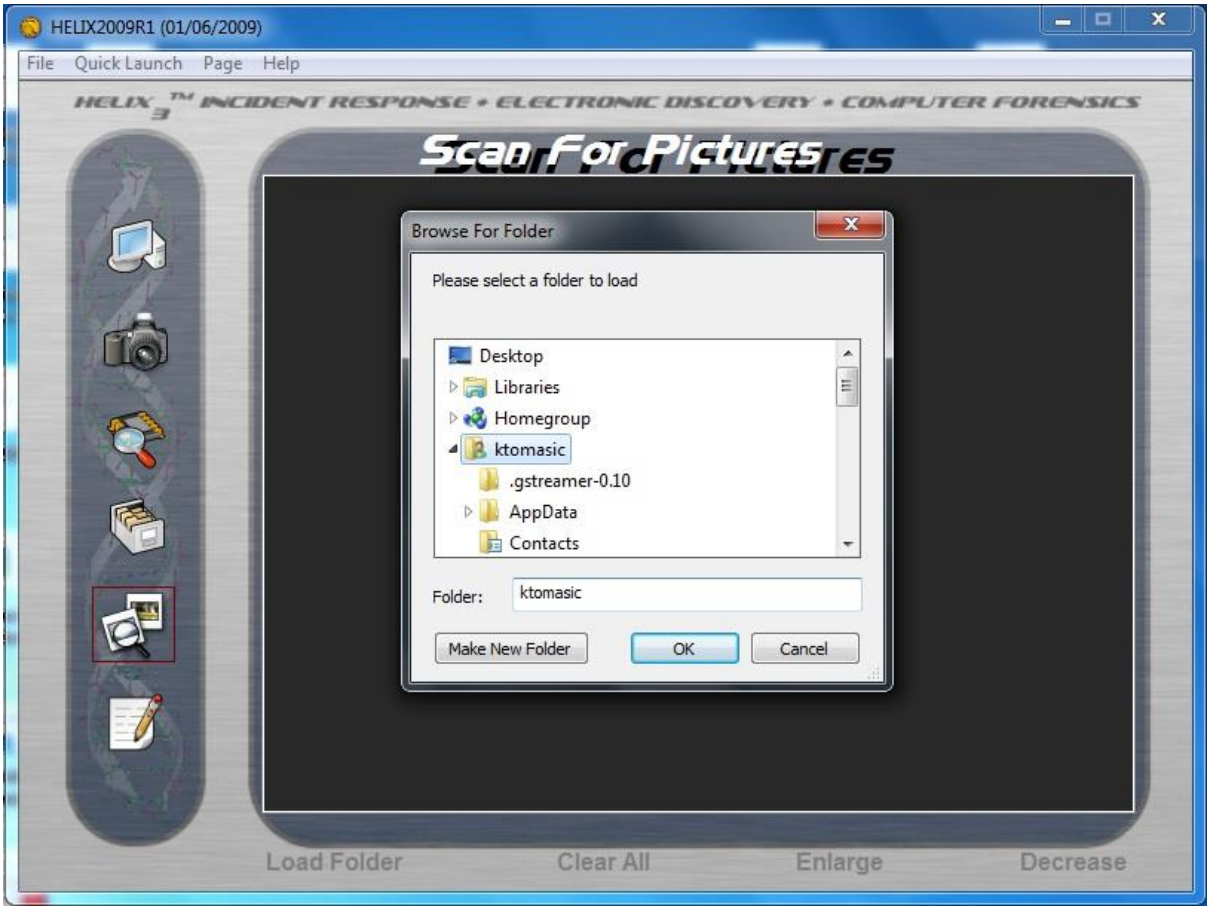
Slika 18: Izgled Acquire a „live“ image of a Windows System using dd sučelja

- Incindent Response tools for Windows System– u ovom djelu je dostupno 20 alata koji se pokreću izravno sa CD medija u svrhu forenzičke analize.
- Browse contents of the CD-ROM and Host OS (Slika 19) – jednostavni preglednik sadržaja diskova koji prikazuje osnovne podatke za svaku odabranu datoteku (ime datoteke, datum kreiranja, datum zadnje izmjene, datum zadnjeg pristupa, CRC, MD5 i veličinu datoteke).



Slika 19: Izgled Browse contents of the CD-ROM and Host OS sučelja

- *Scan for Pictures from a live system* (Slika 20) – pretražuje zadani disk ili direktorij i prikazuje sve pronađene slike. Ova opcija podržava velik broj grafičkih formata.



Slika 20: Izgled Scan for Pictures from a live system sučelja

- *Investigative Notes*– omogućuje zapisivanje bilježaka vezanih za slučaj.

8.4.Postupak forenzičke analize odabranim alatom

8.4.1. Priprema prije istrage

Četvrto poglavlje ovog rada (Slika 7), govori da je prvi korak u računalnoj forenzičkoj istrazi priprema prije same istrage, a ona se sastoji od sljedećih koraka [13]:

- Prilikom provedbe istraga, uvijek je korisno razgovarati s IT djelatnicima, te doznati način i lokacije skladištenja podataka. Loša strana ovog pristupa je naravno moguće otkrivanje provedbe istrage neautoriziranim osobama.

- Određivanje vremenskog razdoblja važnog za istragu, te obujam podataka koje treba pretražiti kako bi se izbjegla analiza nepotrebno velike količine podataka, kao i preskakanje moguće važnih.
- Određivanje tipova informacija važnih za istragu, kako bi se skratilo vrijeme i smanjio obujam pregledanih informacija.
- Određivanje riječi, imena, jedinstvenih fraza pomoću kojih je moguće filtrirati podatke, te pronaći one važne
- Prikupljanje korisničkih imena i zaporki mrežnih i računa elektroničke pošte.
- Utvrditi broj računala te ostalih medija, kao i internet promet koji bi mogao sadržavati važne dokaze.

8.4.2.Prikupljanje podataka

Jedno od pravila digitalne forenzike, kao što je već spomenuto, je kako se nad originalnim podatcima ne smiju provoditi analize već se stvara identična kopija kako se ne bi uništilo originalne podatke. Stvaranje forenzičke kopije naziva se dobavljanje ili akvizicija (eng. *acquisition*). Na slici 21, prikazano je grafičko sučelje forenzičkog programa Helix za stvaranje forenzičke slike. U konkretnom slučaju, program *dd* (sastavni dio Helix forenzičkog alata) nudi stvaranje forenzičke slike radne memorije (osjetljivi dokazi), što je i odabrano, ali isto tako nudi i mogućnost stvaranja forenzičke slike kompletnog tvrdog diska [35].

Slika 21: Pokretanje dd programa kroz Helix grafičko sučelje

Vidljivo je da alat također nudi mogućnost odabira lokacije pohrane slike, pa se odabirom opcije „Attached/Share“ može odabrati pohrana na neki fizički medij odabirom lokacije u prozoru „Destination“, dok se odabirom opcije NetCat omogućuje izravno slanje kopije na Netcat poslužitelj koji se nalazi na mreži, a kao preduvjet potrebno je specificirati IP adresu poslužitelja.

Nakon unosa svih željenih parametara pritiskom na opciju „*Acquire*“ otvorit će se komandna linija u koju je potrebno zalijepiti naredbu te pritisnuti tipku Enter kako bi se ona izvršila. Nakon uspješnog izvršenja naredbe kreiraju se 3 datoteke:

1. `ime_datoteke.dd` – datoteka koja sadrži kopiju diska,
2. `ime_datoteke.dd.md5` – datoteka s MD5 kodom kopije i
3. `Audit.log` – datoteka sa zapisom naredbe i njezinog ispisa.

Forenzička kopija naziv je za završni produkt forenzičkog prikupljanja informacija s tvrdog diska ili drugih medija za pohranu informacija istraživanog računala. Forenzička kopija naziva se i *bitstream* kopija, ili *bitstream* slika (eng. *bitstream image*), zbog toga što predstavlja identičnu bit-po-bit kopiju originalnog dokumenta, datoteke, particije, slike, fotografije, ili diska, te je znatno naprednija slika sustav od tkz. zrcalne kopije, koja može, ali ne mora predstavljati identičnu kopiju originala.

8.4.2.1.Forenzika elektroničke pošte

Elektronička se pošta kao dokazni materijal pojavljuje u većini civilnih kao i kriminalnih forenzičkih istraga. Elektronička pošta i elektronička pošta zasnovana na internet poslužiteljima (eng. *Web based e-mail*, kratica *Web mail*) širi se veoma brzo, te jednostavno može završiti na računalu korisnika kojem nije namijenjena.

Elektronička pošta zasnovana na internet poslužiteljima veoma je korisna prilikom istrage. Na primjer ako osumnjičenik ima račun na Google mail poslužitelju, postoji mogućnost da se uz odgovarajuća dopuštenja pronađu čak i obrisane poruke, jer Google svojom politikom o privatnosti korisnika ne garantira brisanje poruka na rezervnim *backup* sustavima.

Svaka elektronička poruka šalje se kao niz paketa veličine bajta. Prilikom transporta na mreži, svaki od tih paketa sadrži sljedeće elemente:

- Izvorišnu adresu: IP adresu računala pošiljatelja, osim u slučaju kada je ta IP adresa prikrivena.

- Odredišnu adresu: IP adresu računala.
- Payload: podatke ili poruku.

Usmjerivači prosljeđuju pakete prema svojim tablicama usmjeravanja sve do krajnjeg odredišta. S forenzičkog stajališta, klijent/poslužitelj sustavi e-pošte najbolji su za traženje informacija zbog toga što se poruke skidaju na korisnikovo lokalno računalo, tj tvrdi disk, što olakšava istragu, jer forenzičar već ima pristup mediju za pohranu. Pristupa se i poslužitelju zbog njegovih dnevnika aktivnosti e-pošte, te mogućih novih poruka. Produkcijski poslužitelji elektroničke pošte nije moguće isključiti radi istrage, stoga se prvo pregledavaju sigurnosne kopije, te se jedino kao zadnjoj mogućnosti pristupa isključenju poslužitelja

Analiza elektroničke pošte

Elektronička poruka sastoji se od dva dijela: zaglavlja i tijela poruke. Iz zaglavlja je moguće saznati izvorišnu i odredišnu adresu, tj pošiljaoca i namijenjenog primaoca, a tijelo poruke sadrži tekst poruke [34].

Većina klijenata e-pošte po originalnim postavkama prikazuju samo osnovne informacije u zaglavlju:

- Od: pošiljateljeva adresa. Ovo polje može biti zamaskirano, tj kao pošiljatelj može bit naveden netko drugi, dok je prava pošiljateljeva IP adresa prikrivena.
- Za: primateljeva adresa, koja također može biti prikrivena, odnosno zamaskirana
- Tema: ponekad je ovo polje prazno, ili sadrži zavaravajuće informacije.
- Datum: zabilježeno s računala pošiljatelja, no može biti pogrešno, ukoliko je sat na njegovom računalu pogrešno postavljeno

Kako istražitelj zapravo ne može vjerovati osnovnim informacijama u zaglavlju, mora proširiti informacije koje se prikazuju u njemu. Prošireno zaglavlje sadrži mnogo više informacija nego što je usmjerivačima zapravo potrebno da dostave poruku do svog odredišta. Najkorisnija informacija u proširenom zaglavlju zasigurno je IP adresa izvora, odnosno domene. Pomoću ove informacije moguće je ući u trag pošiljaocu poruke.

Prvi poslužitelj elektroničke pošte kroz koji e-poruka prođe, dodijeli joj jedinstveni identifikacijski broj, te ukoliko istražitelj pristupi dnevnicima poslužitelja prije nego li se tražene informacije prebrišu, moguće je pratiti stvarno vrijeme i smjer prolaska poruke kroz

mrežu. Osim pregleda zaglavlja i tijela poruke, potrebno je provjeriti i ostale potencijalne izvore informacija:

- Privitke s ekstenzijama kao što su .doc, .xls, ili slike.
- Ljude koji su navedeni u cc (eng. *Carbon copie,* Skrać cc.) ili bcc poljima.
- Ljude kojima je poruka proslijeđena.
- Originalnu poruku ili niz poruka na koje je ova odgovor, ili odgovor na istraživanu poruku.

Ne smije se pretpostaviti kako je prijavljeni korisnik poslao sve poruke; u mnogim radnim okruženjima suradnici dijele računala i lozinke, tako da mnogi imaju pristup istraživanom računalu.

Proces forenzičkog izvlačenja e-poruka u okolini klijent/poslužitelj slijedi općenite korake. Većina sustava za elektroničku poštu koriste SMTP *Simple Mail Transfer Protocol*, POP *Post Office Protocol*, ili IMAP *Internet Message Access Protocol*. Korištenjem ovih protokola transport e-poruka postaje standardiziran. Izazov jest izvući e-poruke iz raznih klijentskih aplikacija za e-poštu pomoću forenzičkih alata. Dva najčešće korištena klijentska softvera:

Outlook: izuzev uobičajenih mogućnosti aplikacije za e-poštu, sadrži kalendar, listu zadataka (eng. *Task list*), te upravitelja kontaktima (eng. *Contact menager*). Samim time pruža detaljan uvid u svakodnevnu rutinu osumnjičenika. Za razliku od Outlook Expressa, Outlook sprema sve podatke unutar jednog korisničkog identiteta, u dokumentu s ekstenzijom .pst kojem je moguće pristupiti korištenjem forenzičkih alata kao što su FTK, i EnCase.

U Outlook Expressu, Outlooku, AOL, Eudori i Thunderbirdu, e-poruke se pohranjuju lokalno na istraživanom računalu, što znatno olakšava pregled i pretragu. Unatoč tome, pregledom dnevnika mail poslužitelja dolazimo do informacija koje povezuju poslužitelj i e-poruku, pregledom identifikacijske poruke [34].

8.4.2.2.Forenzika podataka

Osnovni medij za pohranu podataka kod većine je računala magnetni disk. Osnovni dizajn diskova nije se mijenjao desetljećima; oni koriste magnetski materijal koji se polarizira pozitivnim ili negativnim nabojem. Ova dva tipa polarizacije magneta omogućuju pohranu binarnih podataka nula i jedinica kao magnetske naboje, te predstavljaju jednostavan način

pohrane velike količine podataka na relativno stabilnoj fizičkoj platformi. Tvrdi diskovi ovog tipa sastavljeni su od istih osnovnih elemenata strukture [22]:

- Glava za čitanje: fizički element tvrdog diska koji čita i zapisuje magnetski materijal lociran na metalnim pločama. Većina današnjih tvrdih diskova posjeduje dvije glave, za istodobno čitanje gornje i donje površine ploče.
- Staza: kružno područje na ploči koje sadržava informacije.
- Cilindar: staze više ploča poslagane jedna iznad druge.
- Sektor: najmanja jedinica pohrane na mediju za pohranu podataka. Staze su podijeljene na sektore, njihova veličina obično iznosi 512 bajta.

Veličine tvrdih diskova variraju, ovisno o kombinaciji cilindara, glava i sektora (eng. *Cyilinders, heads, sectors,* kratica CHS). *Basic Input Output System* (BIOS) sam očitava standardne postavke proizvođača za BIOS s tvrdog diska, te se korisnik ne mora manualno pobrinuti za njih, no moguće je namjestiti nestandardne postavke samostalno.

U slučaju da računalo iz nekog razloga izgubi specijalne postavke uređaja za pohranu, korisno je imati digitalni zapis pohranjen na nekom mediju van računala. Kada istražitelj analizira računalo čije su postavke tvrdog diska nestandardne, takav zapis izvor je informacija koji pomaže pri prikupljanju potencijalno korisnih podataka.

Najraširenij i najpopularniji OS današnjice. Windowsi organiziraju podatke na tvrdom disku koristeći sljedeće fizičke elemente [1]:

- Klaster (eng. *Cluster*): Grupacija sektora kojom se smanjuje broj zapisa potrebnih za praćenje smještaja datoteka na tvrdom disku. Što je veći disk, u klasteru će biti smješten veći broj sektora, kako alokacijske tablice ne bi prerasle razumnu veličinu. Danas uobičajena veličina klastera iznosi 32KB. Kako su sektori definirani na sklopovskoj razini nazivaju se i fizički adresni prostor, a klasteri koji su definirani na razini operacijskog sustava logički adresni prostor.
- Particija ili logički *volume*: Logički odjeljak fizičkog uređaja za pohranu podataka. Ovisno o operacijskom sustavu, fizički medij za pohranu podataka razdijeljen je na manje logičke jedinice kako bi OS mogao funkcionirati ispravno, no u današnje vrijeme particioniranje je više korisnikova metoda organizacije datoteka, nego limitacija od strane operacijskog sustava. Kada se tijekom istrage naiđe na velik dio

neparticioniranog prostora na disku, preporučuje se detaljniji pregled jer neki korisnici znaju privremeno obrisati podatke s diska kako bi ih prikrili.

- Glavni *boot* zapis (eng. *Master Boot Record*, kratica MBR): područje na uređaju za pohranu podataka koje OS koristi kada traži medij za boot prilikom uključivanja. Iako MBR ima nekoliko primjena, glavna mu je zadaća pohrana informacija o particijama definiranim na fizičkom tvrdom disku. MBR je smješten ispred prve particije na disku u glavnom području boot zapisa (eng. *Main boot record area*, kratica MBRA). MBR sadrži i *bootstrap* informacije, te jedinstvene identifikatore medija za pohranu koji se mogu koristiti za praćenje prijenosnih memorija priključenih na računalu.

8.4.2.2.1.Obrisani podaci

Kada korisnik obriše dokument, datotečni sustav postavi marker u sustav za upravljanje datotekama, kako bi OS znao kako taj dokument više nije u tom klasteru ili bloku. Ovim postupkom sustav logički obriše podatak iz svojih zapisa, ali nije fizički obrisao binarne podatke s medija za pohranu. Ne obavljanjem fizičkog brisanja OS ostavlja virtualno binarno arheološko nalazište, veoma korisno forenzičkim istražiteljima.

Što su tvrdi diskovi veći, količina podataka preostalih od prijašnjih zapisa povećava se, jer je sustavu na raspolaganju više prostora za pohranu, i više mu vremena treba da ponovo dođe do mjesta na disku gdje je već nešto bilo zapisano. Datotečni sustav nealocirani prostor smatra praznim i spremnim za daljnju uporabu, a u njemu se mogu nalaziti i *cached* podatci.

Ovaj proces ima neželjen efekt čuvanja internetske stranice koju je korisnik posjetio čak i nakon brisanja *cache* dokumenta. U starijim datotečni sustavima kao što je DOS, nealocirani prostor sadrži obrisane podatke, dok se u novijim verzijama operacijskih sustava koristi dvostupanjski proces koji uključuje *Recycle Bin*. Stoga se prije provjere nealociranog područja preporučuje pregled Recycle Bina[35].

8.4.2.2.2.Dohvat obrisanih dokumenata

Forenzički alati (Slika 22) nakon pregleda diska sastavljaju listu obrisanih dokumenata. Na primjer u listi se mogu nalaziti izbrisane slike, koje se još uvijek nalaze na mediju za pohranu zajedno sa svim važnim metapodacima i oznakama datuma i vremena. Najbolji se rezultati postižu ako je dokument još uvijek čitav sadržan na disku ili je bio zapisan u FAT ili MFT tablicama.

Slika 22:Izgled PC Inspektor alata za dohvat izbrisanih podataka

8.4.2.2.3.Dohvat obrisanih podataka iz nealociranih prostora

Prilikom pretraživanja oštećenih dokumenata ili fragmenata dokumenata iz nealociranih područja, nije moguće provoditi standardnu pretragu jer bi se neki dokumenti preskočili zbog na primjer nepotpunih zaglavlja, nedostatka dijela dokumenta ili ekstenzije. Nadalje takvi podatci obično nemaju očuvane metapodatke zbog načina na koje aplikacije hvataju podatke. Nekada se metapodaci mogu pronaći ugrađeni u samom dokumentu.

Na primjer, pretraga ključnim riječima može izgledati ovako; traži se Microsoft Word dokument, a kao ključne riječi koristi se sekvenca zaglavlja MS Worda, i tema dokumenta npr. kompanija za ekspresnu dostavu pošte. Metapodaci mogu biti nepovratno izgubljeni na sustavskoj razini, ali moguće je da još uvijek postoje na aplikacijskoj razini.

8.4.2.2.4.Nepristupačan prostor

Podaci se mogu sakriti i u dijelove diska do kojih OS nema pristupa. Razlozi zbog kojih OS nema pristupa nekim dijelovima diska mogu biti oštećenje ili limitacija datotečnog sustava. *Hex* editorom moguće je pristupiti i promijeniti konfiguracijske dokumente datotečnog sustava u dijelu koji kontrolira označavanje oštećenih dijelova diska. Informacije se tada mogu

pohraniti i sakriti u dio diska koji je datotečni sustav prozvao oštećenim. Informacije je moguće sakriti u dijelove medija za pohranu koje OS ne prepoznaje, veličine i do 1GB.

Ova su područje najčešće locirana na fizičkom kraju medija, i podatci sačuvani na tom dijelu dostupni su jedino *hex* editorom. Informacije koje se želi sakriti dovoljno je kopirati u *hex* editor i sačuvati u nedostupan dio diska. Iako se ove metode skrivanja podataka i dalje koriste, jednostavnije je i učinkovitije informacije kriptirati, nego modificirati medij za pohranu i podatke.

8.4.2.2.5.Dobava podataka

Računalni forenzički softver omogućuje relativno jednostavno izvlačenje podataka iz medija za pohranu zbog nekoliko razloga:

- Većina procesa pretrage i izvlačenja podataka je automatizirana.
- Prosječni korisnici ne razumiju kako funkcionira računalo, niti načine pohrane podataka na računalo.
- Tehnički sposobniji korisnici ponekad nemaju pristup svim dijelovima računala ili mreže na kojem ostavljaju digitalne otiske prstiju.
- Većina osumnjičenika ne skriva podatke, već ih samo kriptira, ili sakriva koristeći steganografiju[14].

Osnovno izvlačenje podataka koristeći softver kao što je *Helix* relativno je jednostavno nakon što se na radno računalo dobavi forenzička kopija, slika originalnog medija za pohranu. Tada se koriste automatizirani procesi izvlačenja podataka i generacije izvještaja. Sljedeći koraci prikazuju izvlačenje obrisanih dokumenata [34]:

- Dobava forenzičke kopije i popisivanje cijelog sadržaja medija za pohranu, izdvajanje samo obrisanih podataka.
- Identifikacija obrisanog dokumenta koji sadrži informacije vezane uz istragu, analiza i pretraga dokumenta za metapodacima kao što su zaglavlja i vremenske oznake.
- Ispitati internu strukturu podataka: ako podatak treba biti grafički, otvara ga se s prikladnim preglednikom iz softverskog paketa forenzičkih alata, biti će ga moguće otvoriti ukoliko interna struktura podataka odgovara zaglavlju.

[14] Steganografija je umjetnost i znanost o pisanju skrivenih poruka na takav način da nitko, osim pošiljaoca i primaoca, posumnja u postojanje poruke.

- Označiti ili uključiti dokaz u izvještaj: izvještaji trebaju sadržavati što je više moguće dokaznih dokumenata i njihovih metapodataka.
- Izvlačenje podataka i analiza, traženje skrivenih podataka, metapodataka ili informacija specifičnih za istraživani slučaj
- Izrada radne kopije koja će se koristiti za daljnje analize

8.4.2.2.6.Analiza dobavljenih podataka

Nakon izvlačenja podataka, slijedi njihova analiza. Tehnički dio forenzičke istrage uglavnom je jednostavniji jer su alati za pronalazak podataka prilično efikasni. Pravi izazov leži u povezivanju i pronalasku dokaza. Kod analize podataka treba uzeti u obzir sljedeće :

- Vremenski slijed događaja: kao se dokaz uklapa u vremenski slijed događaja
- Poveznica s osumnjičenikom: kako je dokaz povezan s osumnjičenikom, je li ta poveznica potvrđena drugim činjenicama ili dokazima.
- Trag dokaza: kako je dokaz dospio na mjesto gdje je pronađen, može li se pratiti digitalni trag dokaza koji se uklapa u vremenski slijed događaja
- Integritet dokaza: Jeli dokaz ili dokument zbilja ono za što se predstavlja, postoje li skriveni podatci u njemu, može li biti krivotvorina, ili podmetnut.
- Zašto: Zbog čega je podatak lociran tamo gdje je, zbog čega su dokazi u tom formatu.

8.4.2.3.Forenzika dokumenata

Što dokument govori o osobi koja ga je stvorila gotovo je jednako važno namjeni tog dokumenta. Kada istražitelj pronađe dokument s inkriminirajućim dokazima, mora dokazati tko ga je napisao i kada. Nekako mora povezati dokaz s osumnjičenikom, tada u igru ulazi forenzika dokumenata i metapodaci.

Metapodaci su podatci o podatcima. Razlikuju se za različite tipove podataka i domena, na primjer metapodaci o dokumentima razlikuju se od metapodataka o internetskim stranicama, no oboje opisuju u nekom obliku karakteristike podataka koje predstavljaju. Dio metapodataka za sliku na primjer sadržava vremensku oznaku koja prikazuje kada je fotografija nastala. Računalna forenzika, asocijacijom i forenzika dokumenata imaju isti cilj kao i klasična forenzika: sastaviti istinitu verziju događaja potkrijepljenu dokazima [35].

8.4.2.3.1.Pronalazak dokaznog materijala u dokumentima: Metapodaci

Dokumenti predstavljaju najvažnije mjesto pronalaska metapodataka. Sljedeća lista opisuje osnovne tipove metapodataka za tipičan tekstualni dokument [22]:

- Autor: Nebitno dolazi li informacija od operacijskog sustava ili instalacije softvera za obradu riječi, u dokument se ugrađuje ime;
- Organizacija: Dobavlja se iz istog izvora kao i informacija o autoru;
- Revizije: Kao dio stvaranja revizijskog zapisa pohranjuje se ime prethodnih autora i putanja do mjesta na kojem je dokument pohranjen;
- Prethodni autori;
- Predložak: Ova informacija prikazuje koji je predložak ugrađen u dokument;
- Ime računala: ova informacija povezuje dokument s računalom na kojem je nastao;
- Tvrdi disk: ime diska i putanja do mjesta na kojem je pohranjen podatak;
- Mrežni poslužitelj: Nastavak informacija o tvrdom disku, ukoliko je dokument pohranjen na mrežnom poslužitelju, metapodatak sadrži ime mrežne putanje
- Vrijeme: ovaj informacija ukazuje na to koliko je dokument vremena bio otvoren prilikom uređivanja;
- Izbrisani tekst: neki metapodaci sadrže i izbrisani tekst;
- Vremenske oznake: datum i vrijeme stvaranja, pristupa, i modifikacije (eng *created, accessed, and modified* - CAM.);
- Ispis: Metapodaci sadrže i informacije je li i kada je dokument ispisan.

Iako se većina metapodataka izvlači iz Microsoft-ovih alata i aplikacija, metapodatke se može pronaći u gotovo svim aplikacijskim softverima; u Adobe PDF dokumentima, multimedijalnim zapisima, internetskim stranicama, bazama podataka, čak i geografskim softverskim aplikacijama.

Tip i količina pronađenih metapodataka ovisi o aplikaciji i koliko je korisnik sklon unošenju osobnih informacija na računalu. Metapodaci locirani unutar dokumenta mogu se svrstati u dvije kategorije: metapodaci kojima korisnik može pristupiti, i oni kojima ne može. Ukoliko metapodaci nisu vidljivi, potrebno ih je izvući. Lista opisuje informacije koje se može pronaći pregledavajući metapodatke dostupne korisnicima:

- Osnovne informacije o korisniku

- Statistika dokumenta: broj stranica, paragrafa, vremenske oznake

Prilikom izvlačenja metapodataka potrebno je koristit specijalne softverske alate kao što su Metadata Analyzer ili iScrub. Ovi alati analiziraju dokumente na binarnoj razini pri analizi dnevnika revizije, Objekata Visual Basic-a ili izbrisanog teksta koji bi se još mogao nalaziti u podatcima.

8.4.2.3.2.Pregled CAM informacija

Korištenjem CAM (eng.*Create, Access, Modify*) vremenskih oznaka često je moguće odrediti vremenski tijek događaja. Lokacija CAM informacija ovisi o OS-u. Korištenjem CAM metapodataka moguće je rekreirati osumnjičenikov tijek kretanja, povijest dokumenta ili pratiti putanju dokumenta kroz mrežu. Vremenske oznake u CAM metapodacima znače [34]:

- Stvaranje (eng. *create*): prikazuje vrijeme i datum kada je dokument stvoren na tom mediju za pohranu. Ova se vremenska oznaka mijenja svaki puta kada se dokument kopira na novi medij, čak i unutar istog uređaja za pohranu.
- Pristup(eng. *acess*): specificira zadnji puta kada je dokument otvoren, ili pregledan ali ne i mijenjan
- Modificiranje(eng. *modify*): sadrži datum i vrijeme mijenjanja dokumenta. Na dokumentima koji su kopirani na nove medije, vremenska oznaka modificiraj može biti starija od vremenske oznake stvaranja.

Datumi i vremena asocirana s CAM informacijama dobivaju se od sustavskog sata, stoga u slučaju da je on krivo postavljen, vremenske su oznake također pogrešne. Pitanje koje ostaje prilikom pregleda vremenskih oznaka jest jeli korišteno lokalno računanje vremena ili Zulu. Svijet je podijeljen na 24 vremenske zone, koje se označavaju po slovima engleske abecede; vremenska zona Z (Zulu), predstavlja vrijeme u Greenwich-u, Engleska.

Zulu se računanje vremena u avijaciji koristi kao standardno, tako se bez obzira na vremensku zonu zna koliko je sati. Problem koji se javlja prilikom pregleda vremenskih oznaka je taj da je dokument možda stvoren u Hong Kongu, poslan u London, te kopiran u New Yorku, sve unutar nekoliko sekundi. Ovaj raspon lokalnih vremena može zbuniti istražitelje, i postaje veoma teško odrediti vremenski tijek događaja dokumenta. Za većinu je ljudi korištenje lokalnog ili *Zulu* računanja vremena semantičko pitanje, ali za istražitelje znači točnost preciznost, i pouzdanost vremenskih oznaka.

Kako su CAM informacije postale ključne u rješavanju računalnih forenzičkih slučajeva, stvoreni su softverski paketi koji mogu poremetiti CAM informacije, te popuniti polja vremenskih oznaka sa slučajnim nizom vremena i datuma., ili ih jednostavno obrišu, te se forenzičari moraju pouzdati u vremenske oznake sekundarnih izvora kao što su poslužitelji elektroničke pošte.

8.4.2.3.3.Otkrivanje dokumenata

Na žalost forenzičkih računalnih istražitelja, dokumenti mogu biti skriveni na mnogo mjesta, prikriveni, prerušeni kriptirani. Prvo mjesto gdje treba tražiti dokumente jest naravno u aplikacijama u kojima su stvoreni. Većina softverskih aplikacija pohranjuje listu dokumenata koji su nedavno bili otvarani, mijenjani, stvoreni, te gdje su sačuvani. Ova metoda pretrage prikladna je iz razloga jer upućuje na vanjske uređaje za pohranu podataka kao što su prijenosne memorije.

Sljedeći korak u otkrivanju dokumenata jest korištenje forenzičkog softvera kao što je FTK, te otvaranje svih dokumenata određenog traženog tipa. Ovaj pristup može doprinijeti preskakanju dokumenata ukoliko ih je korisnik zamaskirao u neki drugi tip dokumenata promjenom zaglavlja ili ekstenzije. Aplikacijski programi općenito prepoznaju dokumente po ekstenziji ili po zaglavlju, dok se OS općenito oslanja na ekstenziju kako bi utvrdio tip dokumenta.

Zaglavlje se sastoji od niza znakova, na samom početku dokumenta koji označavaju kojem tipu dokumenta pripada. Postoje tisuće tipova dokumenata, te pronalazak zaglavlja dokumenta stvorenog nekom manje poznatom aplikacijom može biti izazovno. Na sreću većina dokumenata pripada tipovima podataka koje stvaraju popularni softverski i dobro poznati paketi.

Promjenom ekstenzije dokumenta, niz znakova na početku zaglavlja se ne mijenja, te aplikacija koja je originalno stvorila dokument, bez problema ga i otvara. Većina forenzičkog softverskog alata provodi analizu potpisa kako bi utvrdili odgovaraju li ekstenzije tipu dokumenta deklariranom u zaglavlju, te sastavljaju popis sumnjivih datoteka i dokumenata. Ukoliko se zapisi poklapaju, dokument je vjerojatno ono za što se predstavlja, ukoliko se ne poklapaju, dokument je zamaskiran kao nešto drugo, kako bi se prikrili podatci, ili zavaralo istražitelje [36].

8.4.2.3.4.Pronalazak poveznica i vanjskih medija za pohranu podataka

Kada se dokument kopira ili sačuva na lokalnom računalu, generira se dokument poveznica (eng. *Link file*), kako bi OS znao gdje je dokument lociran. Ovi *link* dokumenti često su jedini dokaz kako je neka vanjska jedinica spajana na računalo. Forenzičkim je softverom moguće pronaći čak i obrisane dokumente poveznice.

Ovisno o korištenom forenzičkom softveru, koraci rekonstrukcije dokumenata poveznica variraju, no cilj im je isti; utvrđivanje traga ili poveznice s jednog uređaja na drugi. Utvrđivanje traga važan je proces jer se njime povezuje na primjer uređaj na kojem je pronađen dokument s računalom na kojem je nastao. Uz dokumente poveznice, tragove o mogućim vanjskim medijima moguće je pronaći i u Windows Registru.

Ako dokument poveznica upućuje na mrežnu putanju kao što je na primjer \\poslužitelj\test.doc, istražitelji imaju malo vremena za njihovo praćenje jer se informacije na usmjerivačima i poslužiteljima relativno brzo prepisuju novim podatcima. Dokumenti poveznice pružaju veliku količinu informacija, moguće jednake važnosti kao i sam dokument do kojeg vode zbog vremenskih i lokacijskih oznaka koje sadrže.

Većina kompanija i organizacija posjeduje određeni oblik sigurnosnih kopija svojih baza podataka te ostalih važnih informacija. Forenzičkim istražiteljima ove kopije pružaju uvid u sranje računalnog sustav kroz vrijeme, i čuvaju se dugo nakon što su originalna računala zamijenjena. Malo ljudi zna za njihovo postojanje ili imaju pristup sigurnosnim kopijama. Čak ako uspiju obrisati sve svoje digitalne tragove na računalu, ne mogu i na sigurnosnim kopijama.

9.ZAKLJUČAK

Zadnjih dvadesetak godina vidljiv je nevjerojatna napredak u razvoju tehnoloških rješenja za poboljšanje kvalitete življenja, a još se veći napredak vidi kroz razvoj terminalne opreme telekomunikacijske mreže, koja danas postaje nezaobilazni faktor modernog doba.

Razvoj tehnike, prati i sve veća mogućnost zlouporabe iste od strane kriminalnih grupa ili zlonamjernih pojedinaca, radi pribavljanje ilegalnih sredstava. Time se javlja i potreba za zaštitom sustava, ali i za legalnim pribavljanjem digitalnih dokaza i tragova neovlaštenih pristupa i kriminalnih radnji.

Računalna forenzika je mlada, a nadasve dinamička grana forenzičke analize, jer zahtijeva konstantnu edukaciju, pronalazak novih i boljih hardverskih i softverskih rješenja za poboljšanje kvalitete pronalazaka digitalnih dokaza.

Oprema za računalnu forenziku je izrazito sofisticirana i napredan jer mora omogućiti kompleksna pretraživanje terminalne opreme uz minimalnu ili gotovo nikakvo narušavanje digitalnih tragova, te mogućnost pronalaska najmanjih tragova koji bi mogli pomoći u istrazi, što u krajnjoj liniji znači i visoku cijenu takve opreme, te potrebu za stručnim rukovanjem.

Vezano uz gore navedenu literaturu, vidljivo je da je računalna forenzika znanost u konstantnoj evoluciji, te je u današnje doba, od krucijalne važnosti da računalna forenzika prati trendove razvoja tehnologija, a računalni forenzičari metodologiju forenzičke analize, da bi se uspješno mogli boriti protiv računalnog kriminala.

U svijetu postoje organizacije koje izdaju certifikate za pojedina područja računalne forenzike. Ispitni postupak za dobivanje certifikata se standardno sastoji od pitanja vezana uz hardware, software te zakone u državi u kojoj se polaže ispit. U Hrvatskoj se obrazovanjem budućih forenzičara bavi samo INsig2 u Zagrebu, ovlašteni forenzički centar za regiju bivše Jugoslavije.

Neki od dostupnih certifikata u svijetu su GIAC certificiran forenzički analitičar (GCFA, The GIAC (Global Information Assurance Certification) Certified Forensics Analyst), ANSI/ISO/IEC 17024 akreditiran certifikat, ISFCE CCE (The International Society of Forensic Computer Examiners Certified Computer Examiner), IACRB CCFE (Information

Assurance Certification Review Board Certified Computer Forensics Examiner), IACIS CFCE (The International Association for Computer Information Systems Certified Forensic Computer Examiner), te certifikati pojedinih tvrtki, npr. EnCE Certification Program softverskog alata EnCase.

Na području Republike Hrvatske djeluje Croatian national computer emergancy response team (CERT) te u okviru svog djelovanja provodi proaktivne i reakativne mjere.

Važan aspekt informacijsko komunikacijskog sustava je i sigurnost istoga, koja se definira kao skup pravila i postupaka kojima se određuje razina sigurnosti nekog informacijskog sustava. Istovremeno je bitno pridodati pažnju sigurnosti tehnologije i informacija koje informacijski sustav sadrži.

Sigurnosnom politikom korisniku se nameću obvezna pravila ponašanja i odgovornosti kako bi se zaštitilo informacijski sustav, tj. informacije pohranjene u informacijskom sustavu, od vanjskih utjecaja (udaljenih napada, zlonamjernih programa, itd.), ali također i korisnika.

10.LITERATURA

1. Dragičević, D**.** *Kompjutorski kriminalitet i informacijski sustavi*. Zagreb. Informer. 1999.
2. Hadjina, N**.** *Zaštita i sigurnost informacijskih sustava*. Zagreb. Sveučilište u Zagrebu. Fakultet elektrotehnike i računarstva. 2009.
3. Vacca, J.A. *Network and system security*. SAD. Elsevier. 2010.
4. Peraković, D., Cvitić, I**.** Autorizirana predavanja za predmet „Sigurnost i zaštita informacijsko komunikacijskog sustava“. Zagreb. Fakultet prometnih znanosti u Zagrebu. 2014.
5. Information Security Policy Templates [Online]. 2015. Dostupno na http://www.sans.org/security-resources/policies [25.05.2015.]
6. Računalna forenzika. Nacionalno središte za sigurnost računalnih mreža i sustava. [Online]. 2010. Dostupno na: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-05-301.pdf .[25.05.2015.].
7. Hailey, S. What is computer forensic? [Online]. 2002. Dostupno na: http://www.csisite.net/ [25.05.2015.]
8. Bača, M., Ćosić, J. Prevencija računalnog kriminaliteta. Policija i sigurnost. 2013. Vol.22 No1.
9. Grubor, G., Milosavljević, M. Digitalna forenzika računarskog sistema. Beograd. Univerzitet Singidunum. 2009.
10. Ćosić, J. Druga strana socijalnih mreža. CUC 2010 – CarNET korisnička konferencija. Split-Croatia. 2010.
11. Zakon o informacijskoj sigurnosti - NN79/07. Narodne novine. Zagreb. 2007.
12. Bača, M., Ćosić, J. Računalna forenzika – široki aspekti primjene. Jahorina. INFOTEH. Vol.9 str. 857-860
13. Tijek forenzičke istrage. [Online] 2015. Dostupno na: http://www.cis.hr/WikiIS/ [25.05.2015.]
14. https://www.digitalintelligence.com/products/fred/ [10.06.2015.]
15. Horvat, A. Forenzička analiza računalnog sustva. Diplomski rad. Zagreb: Sveučilište u Zagrebu. Fakultet elektrotehnike i računarstva. 2007. http://os2.zemris.fer.hr/ostalo/2007_horvat/Forenzika.htm [10.06.2015.]
16. Burdach, M. Digital forenzics of the physical memory, Varšava, 2005.

17. Marčeta, M. Digitalna forenzika slika. Fakultet elektrotehnike i računarstva. [Online] 2010. Dostupno na: http://os2.zemris.fer.hr/ostalo/2010_marceta/Diplomski.htm#_Toc261209063 [10.06.2015.]
18. Computer forensic analysis class. [Online]. Dostupno na: http://www.porcupine.org/forensics/handouts.html [10.06.2015.]
19. Računalna forenzika. [Online]. Dostupno na: http://www.cis.hr/wiki/wiki.html [15.06.2015.]
20. Federal bureau of investigation. Handbook of forensic services. [Online] Sjedinjene američke države. 2007. Dostupno na: https://www2.fbi.gov/hq/lab/handbook/forensics.pdf [10.06.2015.]
21. Radić, B. Osnove računalne forenzike. Sveučilišni računski centar. [Online]. 2008. Dostupno na: http://sistemac.srce.unizg.hr/fileadmin/user_root/seminari/Srce-Sys-Seminari-Osnove_racunalne_forenzike.pdf [25.05.2015.]
22. PyFlag Tutorials [Online]. Dostupno na: http://pyflag.sourceforge.net/Documentation/tutorials/samples/ [25.05.2015.]
23. PyFlag Tutorials [Online]. Dostupno na: http://pyflag.sourceforge.net/Documentation/tutorials/index.html [25.05.2015.]
24. PyFlag Tutorials Log Analysis [Online]. Dostupno na: http://pyflag.sourceforge.net/Documentation/tutorials/loganalysis.html [25.05.2015.]
25. PyFlag Tutorials Disk Forensics [Online]. Dostupno na: http://pyflag.sourceforge.net/Documentation/tutorials/forensics.html [25.05.2015.]
26. PyFlag Tutorials RAID Reassembly - A forensic Challenge [Online]. Dostupno na: http://pyflag.sourceforge.net/Documentation/articles/raid/reconstruction.html [25.05.2015.]
27. PyFlag Forensics ND Log Analysis GUI [Online]. Dostupno na: http://pyflag.sourceforge.net/Presentations/PyFlag_Auscert2007/ [25.05.2015.]
28. CARNet CERT. Primjena TCT programskog paketa u postupcima forenzičke analize. [Online]. Zagreb. 2004. Dostupno na: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-01-56.pdf [15.06.2015.]
29. Frequently Asked Questions about The Coroner's Toolkit [Online] Dostupno na: http://www.fish2.com/tct/FAQ.html [15.06.2015.]
30. Cyber security institute. [Online]. Dostupno na: http://www.csisite.net/ [15.06.2015.]

31. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls *(second edition)* [Online]. Dostupno na: http://www.iso27001security.com/html/27002.html [15.06.2015.]
32. EnCE® Certification Program. [Online]. Dostupno na: https://www.guidancesoftware.com/training/Pages/ence-certification-program.aspx[15.06.2015.]
33. What is KNOPPIX®? [Online]. Dostupno na: http://www.knopper.net/knoppix/ [15.06.2015.]
34. E-fense. Helix 3: user manual. [Online]. 2009. Dostupno na: http://www.sdp-tech.com/sdp-tech/pub/helix/Helix_Opensource_User_Manual.pdf [15.06.2015.]
35. Gleason, BJ., Fahey, D. Helix 1.7 for Beginners. [Online]. 2005. Dostupno na: http://www.thecybercrimeinvestigator.com/crj455/Helix-for-Beginners.pdf [15.06.2015.]
36. http://www.nsrl.nist.gov/Downloads.htm [15.06.2015.]

POPIS KRATICA

IK sustav – informacijsko komunikacijski sustav

MBO – (eng. motherboard) matična ploča računala

CPU – (eng. central processing unit) centralna procesna jedinica ili procesor računala

GPU – (enggraphicsprocessorunit) grafička procesna jedinica računala

RAM – (eng. random-accessmemory) radna memorija računala

HDD – (eng.hard disk drive) tvrdi disk računala

NIST – (eng. ***N****ational* ***I****nstitute of****S****tandardsand****T****echnology)* Nacionalni institut za standarde i tehnologiju

ISO – (eng. International Organization for Standardization) Međunarodna organizacija za standardizaciju

IEC – (eng. The International Electrotechnical Commission) Internacionalna elktrotehnička komisija

CSI – (eng.*Cyber Security Institute)* Institut za kibernetičku sigurnost

FBI – (eng. *The FederalBureauofInvestigation*) Federalni ured za istrage

CART – eng. *Computer Analysisand Response Team*

ASCLD-LAB – eng. *American Society of Crime Laboratory Directors / LaboratoryAccreditation Bord*

OECD–(eng. TheOrganisation for Economic Co-operationand Development) Međunarodan organizacija za ekonomsku suradnju i razvoj

DNK – deoksiribonukleinska kiselina

CMOS - (engl. Complementary Metal Oxide Semiconductor) je tehnologija za izradu digitalnih i analognih mikroelektroničkih sklopova

MMC – (eng memory card) memorijska kartica

RFA – računalna forenzička analiza

USB - (eng. Universal Serial Bus) je naziv za računalnu sabirnicu koja služi za serijski prijenos podataka između osobnog računala i perifernih uređaja

IEEE – (eng. Institute of Electrical and Electronics Engineers) neprofitna, tehnička, profesionalna organizacija s više od 400,000 pojedinačnih članova u oko 175 zemalja

FRED – (eng. *First Responder's Evidence Disk)* forenzički alata

AFOSI – (eng. *Air Force Office of Special Investigations)* ured za specijalne istrage američkih zračnih snaga

DLL – (eng. dynamic-link library)

MD5 – (eng.message-digest algorithm) kriptografski algoritam

SHA – (eng. Secure Hash Algorithm) sigurnosni algoritam

KDE – (eng. ***K D****esktop* ***E****nvironment*) grafičko sučelje za UNIX operacijske sustave

ASCII – (eng. American Standard Code for Information Interchange) Američki standardni kod za razmjenu informacija

UNICODE - standard za razmjenu podataka usmjeren na prikaz slova na način neovisan o jeziku

WFT – (eng. Windows Forensic Toolchest) forenzički alat

HTML – (eng. Hyper Text Markup Language) prezentacijski jezik za izradu web stranica

HPA – (eng. *Host-Protected Area*)

UFS – (eng. The Unix file system) datotečni sustav

JFS– (eng. Journaled File System) datotečni sustav

NTFS – (eng. New Technology File System) datotečni sustav

FAT – (eng. **F**ile **A**llocation **T**able) datotečni sustav

FLAG – (engl. *Forensic and Log Analysis GUI*) forenzički alat

CRC32 – (eng. cyclic redundancy check) algoritam za provjeru zalihosti

NSRL – (engl. *The National Software Reference Library*)

RDS – (engl. *Reference Data Set*) skup referentnih podataka

NSRL – (engl. *TheNational Software Reference Library)*

VFS - (engl. *Virtual File System*) virtualni datotečni sustav

RAID – (eng. redundant array of independent disks)

GIAC - (eng. *Global Information Assurance Certification*) cerifikat

GCFA - eng. *GIAC Certified Forensic Analyst*) GIAC certificirani forenzičar

ANSI – (eng. *American National Standards Institute*) Američki institut za standardizaciju

IACRB – (eng. *InformationAssuranceCertificationReviewBoard)*

CCFE - (eng. *Certified Computer Forensics Examiner*) certifikat

IACIS - (eng. *International Association of Computer Investigative Specialists*) Internacionalno udruženje računalnih forenzički specijalista

DOS – (eng.Disk Operating System) je opći naziv za operacijske sustave koji su se počeli pojavljivati krajem 70ih godina 20. stoljeća i u slobodnom prijevodu DOS znači *operacijski sustav za diskove*

DPC - (eng. MS-DOS Processing Certificate) certifikat

CFCE – (eng. *CertifiedForensic Computer Examiner)*

GNU - Unixu sličan računalni operacijski sustav

POPIS SLIKA

Slika 1:Informacijsko komunikacijski sustav kao podsustav organizacijskog sustava 4
Slika 2: Elementi informacijsko komunikacijskog sustava 6
Slika 3:Akademski otvoreni model informacijske sigurnosti 7
Slika 4: Zatvoreni model informacijske sigurnosti 7
Slika 5: Prikaz uklapanja smjernica, standarda i sigurnosne politike 9
Slika 6: Reagiranje na incident 21
Slika 7: Dijagram toka postupka RFA 23
Slika 8: Izgled FRED-a 25
Slika 9: Glavni izbornik PyFlag alata 39
Slika 10: Odabir separatora polja 40
Slika 11: Podešavanje filtera 40
Slika 12: Virtualni datotečni sustav 42
Slika 13: Heksadecimalni zapis datoteke 43
Slika 14:Ispis mactime programa u HTML formatu 46
Slika 15: Distribucija Helix forenzičkog programa 55
Slika 16: Grafičko sučelje forenzičkog programa Helix 56
Slika 17: Izgled Preview System Information sučelja 57
Slika 18: Izgled Acquire a „live“ image of a Windows System using dd sučelja 58
Slika 19: Izgled Browse contents of the CD-ROM and Host OS sučelja 58
Slika 20: Izgled Scan for Pictures from a live system sučelja 59
Slika 21: Pokretanje dd programa kroz Helix grafičko sučelje 60
Slika 22:Izgled PC Inspektor alata za dohvat izbrisanih podataka 66

METAPODACI

Naslov rada: Mogućnosti primjene računalne forenzike kao element sigurnosti informacijsko komunikacijskih sustava

Autor: Karlo Tomašić

Mentor: Prof. dr. sc. Dragan Peraković

Naslov na drugom jeziku (engleski):

Capabilities of Application of Computer Forensics as Security Issue of the Information and Communication Systems

Povjerenstvo za obranu:

- Prof. dr. sc. Slavko Šarić, predsjednik
- Prof. dr.sc. Dragan Peraković, mentor
- Dr.sc. Marko Periša, član
- Prof. dr. sc. Štefica Mrvelj, zamjena

Ustanova koja je dodijelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu

Zavod: Zavod za informacijsko komunikacijski promet

Vrsta studija: Diplomski studij

Naziv studijskog programa: Promet

Stupanj: VSS

Akademski naziv: Magistar inženjer prometa

Datum obrane diplomskog rada: 24.09.2015.

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Mogućnosti primjene računalne forenzike kao element sigurnosti informacijsko komunikacijskih sustava, na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student

U Zagrebu, 24.09.2015. _____

(*potpis*)