Usporedni prikaz forenzičke analize računala i mobilnih uređaja

Majić, Petar

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Petar Majić

USPOREDNI PRIKAZ FORENZIČKE ANALIZE RAČUNALA I MOBILNIH UREĐAJA

ZAVRŠNI RAD

Zagreb, 2018.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 24. travnja 2017.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Terminalni uređaji**

ZAVRŠNI ZADATAK br. 4030

Pristupnik: **Petar Majić (0135232891)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Usporedni prikaz forenzičke analize računala i mobilnih uređaja**

Opis zadatka:

Objasniti značajke forenzičke analize računala. Opisati karakteristike forenzičke analize mobilnih terminalnih uređaja. Usporediti mogućnosti forenzičke analize računala i mobilnih terminalnih uređaja. Ukazati na elemente zakonska regulative usmjerene forenzičkoj analizi računala i mobilnih terminalnih uređaja.

Zadatak uručen pristupniku: 28. travnja 2017.

Mentor:

dr. sc. Siniša Husnjak

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

USPOREDNI PRIKAZ FORENZIČKE ANALIZE RAČUNALA I MOBILNIH UREĐAJA

COMPARATIVE OVERVIEW OF FORENSIC ANALYSIS OF COMPUTERS AND MOBILE DEVICES

Mentor: dr. sc. Siniša Husnjak

Student: Petar Majić

JMBAG:0135232891

Zagreb, rujan 2018.

USPOREDNI PRIKAZ FORENZIČKE ANALIZE RAČUNALA I MOBILNIH UREĐAJA

SAŽETAK

Ovaj završni rad prikazuje značajke forenzičke analize računala i mobilnih uređaja. Također, opisane su osnove računalne tehnologije i jedna od metodologija forenzičke analize računala. Stalnim razvojem mobilnih uređaja, došlo je do pojave novih digitalnih dokaza, ali i potrebe za novom granom digitalne forenzike, mobilne forenzike. U ovom radu usporedno su prikazane mogućnosti forenzičkih alata za računala s forenzičkim alatima za mobilne uređaje, prikazane su prednosti i nedostatci jedne i druge strane. Usporedbom takvih alata, lako je izvedivo procijeniti mogućnosti pojedinog alata te utvrditi u kojim okruženjima je moguća njihova upotreba. Osim navedenih alata, postojeće su i metode antiforenzike čije mogućnosti su uspješne na jednoj razini, a to je u prikrivanju dokaza i stvaranju poteškoća tijekom provedbe forenzičke analize.

Ključne riječi**:** računalo; mobilni uređaj; digitalna forenzička analiza; ekstrakcija podataka

SUMMARY

In this bachelor's thesis, the beginning showed features of computer forensic analysis. The basis of computer technology is represented along with one of the methodologies for computer forensic analysis. With the emergence of mobile device, new digital evidence proved that there is a need for a new branch of forensic, mobile forensic. In this thesis, we compared the possibilities of forensic , tools for computers and mobile devices, together with their advantages and disadvantages. By comparing the tools, it is possible to evaluate the capabilities of each tool and in which environments it can be used. Apart from the tools, it is possible to see the possibilities of anti-forensics methods that are somewhat successful in concealing evidence and creating problems during implementation of forensic analysis**.**

Keywords: computer; mobile device; digital forensic analysis; data extraction

SADRŽAJ

1.Uvod

Digitalna forenzika relativno je mlada znanost koja se počela razvijati prije 30 godina, a u Republici Hrvatskoj u samim je začetcima. Jako je teško pratiti brzi razvoj tehnologije, a samim time i spriječiti nove kriminalne radnje učinjene uz pomoć računalne tehnologije. Postoji nekoliko grana digitalne forenzike, a one najzastupljenije su računalna forenzika i forenzika mobilnog uređaja. Zbog raznolikosti same arhitekture računala i mobilnog uređaja, postoje posebne metodologije kojima se provodi forenzička analiza uređaja. Na taj način razvijeni su i mnogi alati koji omogućavaju ekstrakciju i analizu podataka, a koji mogu biti korišteni kao dokazni materijali pred sudom.

Rad se sastoji od sedam poglavlja:

1. Uvod
2. Značajke forenzičke analize računala
3. Karakteristike forenzičke analize mobilnih uređaja
4. Usporedni prikaz forenzičke analize računala i mobilnih uređaja
5. Digitalna antiforenzika
6. Zakonska regulativa
7. Zaključak

U drugom poglavlju ovoga rada, opisane su osnove računalne tehnologije, izrada postupka računalne forenzičke analize te tijek forenzičke analize računala.

U trećem poglavlju prikazane su razne metode koje su zastupljene tijekom ekstrakcije podataka iz mobilnih uređaja i metoda izolacije uređaja.

U četvrtom poglavlju uspoređene su mogućnosti forenzičkih alata, na osnovu čega je lako uvidjeti njihove prednosti. Također, opisani su dokazi koji se nalaze na računalima baziranim na Microsoft Windows operativnom sustavu te dokazi o mobilnim uređajima u ovisnosti o operativnim sustavima.

U petom poglavlju opisane su metode koje se primjenjuju kako bi se prikrili ili uklonili dokazi. Riječ je o antiforenzici koja je noćna mora svakog istražitelja.

U šestom poglavlju prikazane su zakonske regulative koje su nužne za poznavanje i rad, a strogo ih se mora poštovati.

U konačnici, cilj ovog rada je prikazati raznolikosti i mogućnosti primjene forenzičke znanosti na mobilnim uređajima i računalima što je prikazano različitim usporedbama. Uz navedeni cilj, važno je ukazati i na metode koje se primjenjuju kako bi se forenzička istraga ometala tijekom rada ili kako bi se postojeći dokazi uništili.

2. Značajke forenzičke analize računala

Računalna forenzika predstavlja sasvim novo područje znanosti i tijekom godina mijenjala je svoje nazive. Računalna forenzika dio je forenzičke znanosti koji se odnosi na obradu legalnih dokaza pronađenih na računalu i digitalnim medijima za pohranu podataka. Riječ *„forenzika“* potječe od latinske riječi *„forensis“* što u slobodnom prijevodu znači *„pred forumom, odnosno pred sudom“*, [1].

Računalna forenzika dio je forenzičkih znanosti koja se bavi istraživanjem računalnih sustava kao što su: osobna i prijenosna računala, digitalne kamere, vanjski diskovi, GPS uređaji, mrežni uređaji pa čak i uređaji za kopiranje ukoliko imaju internu memoriju. Standardno se dijeli na sljedeće grane, [2]:

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

Računalna forenzika prvi puta se pojavila 1984. godine kada je FBI osnovao posebnu jedinicu CART (engl. *Computer Analysis and Response Team*) čija djelatnost bila je analiza digitalnih dokaza, a pojavila se upravo zbog sve veće upotrebe računala za izvršavanje kriminalnih dijela.

2.1. Osnove računalne tehnologije

Iako digitalni istražitelji mogu koristiti sofisticirane softvere za oporavak izbrisanih datoteka i obavljati naprednu analizu tvrdog diska samog računala, jako je bitno poznavati što se događa iza scene.

Nedostatak razumijevanja rada računala i nepoznavanje procesa sofisticiranih alata, istražiteljima znatno otežavaju objašnjavanje njihovih otkrića sudu što može dovesti do krivih interpretacija digitalnih dokaza.

Primjerice, tijekom oporavka izbrisanih direktorija, postoji mogućnost da su dva obrisana direktorija zauzela isti prostor u različitom vremenu. Osim toga, svaki alat ima svoja ograničenja koja bi kompetentni digitalni istražitelj trebao prepoznati i riješiti.

Svaki put kada je računalo pokrenuto, ono se mora upoznati sa svojim unutarnjim komponentama i perifernim svijetom.

Taj početni proces naziva se *Boot proces*, a isti ima tri osnovne faze: ponovno pokretanje središnje procesorske jedince (CPU), automatsko testiranje (POST) i podizanje diska.

Središnja procesorska jedinca ili CPU (engl. *Central Processing Unit)* srž je svakog računala, odnosno logički sklop koji obrađuje osnovne upute koje pokreću računalo. Četiri osnovne funkcije procesora su dohvaćanje, dekodiranje, izvršavanje i upisivanje, [3].

BIOS (engl. *Basic Input Output System*) je softver koji se nalazi na malom memorijskom čipu na matičnoj ploči računala, te djeluje kao sučelje između hardvera računala i njegovog operativnog sustava. Zadaća BIOS-a je također prepoznavanje i konfiguriranje hardverskih komponenti na računalu kako što su tvrdi disk, optički pogon, CPU, memorija, itd., [4] .

BIOS sadrži program pod nazivom POST (engl. *Power-On Self-Test)* koji ispituje osnovne komponente računala. POST program se pokreće nakon što CPU aktivira BIOS. Prvi test provjerava integritet CPU-a i samog POST programa, a ostatak POST-a potvrđuje funkcioniraju li sve komponente računala ispravno, uključujući diskove, monitor, RAM (engl. *Random Access Memory*) memoriju i tipkovnicu. Tijekom istrage, odnosno prikupljanja digitalnih podataka s računala, često je potrebno ometati proces podizanja sustava i ispitati CMOS (engl. *Complementary Metal Oxide Semiconductor)* postavke, poput vremena i datuma, konfiguracije tvrdog diska i slijed podizanja sustava.

Iako mediji za pohranu dolaze u mnogim oblicima, tvrdi diskovi su najbogatiji izvor digitalnih dokaza na računalu. Razumijevanje kako tvrdi disk radi, kako se podaci skladište i kako se podaci mogu sakriti jako su bitni za istražitelje. Tvrdi disk sastoji se od nekoliko ploča i glave koja upisuje podatak na određenom mjestu na ploči (sektor) tako da mijenja njegovu magnetsku polarizaciju, a čitanje se vrši postupkom mjerenja magnetske polarizacije. Podaci na ploči bilježe se u koncentričnim krugovima, tj. putanjama.

U posljednjih nekoliko godina umjesto tvrdih diskova sve više se koristi SSD (engl. *Solide State Drive)*, koji umjesto ploča koriste flash memoriju. Pojavom računala sa SSD-om postavljeni su izazovi za forenzičke istražitelje. Jedan od izazova predstavlja opasnost brisanja svih izbrisanih podataka prilikom uključivanja SSD-a.

Prednost za forenzičke istražitelje je što SSD ima mehanizam koji nivelira trošenje, tj. distribuira korištenje flash memorije kako bi spriječio nejednako trošenje jednog područja u odnosu na ostala. Svi podaci koji se nalaze na mediju mogu se sakriti od istražitelja, odnosno samog alata i na taj način ometati tijek istrage. Primjerice, pojedinac može označiti dijelove na tvrdom disku kao loše sektore i samim time sakriti podatke od operativnog sustava.

2.2. Izrada postupka računalne forenzičke analize

RFA (*Računalna forenzička analiza*) zahtjevno je područje djelatnosti koje iziskuje posebno obučeno osoblje, razrađenu logističku podršku i značajna financijska sredstva, a sve to s ciljem zadržavanja pravne vjerodostojnosti prikupljenih dokaza.

Zbog toga je potrebno detaljno razraditi odgovarajuće postupke RFA, [5]:

- *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 određenih profila.

- *Administrativne pripreme*

  Osnivanje i djelovanje tima za RFA zahtijeva znatna sredstva, a mnogi od potrebnih izdataka su periodički te je sredstva potrebno osiguravati na godišnjoj razini. Potrebno je osigurati: radni prostor, opremu, programsku podršku s nužnim nadogradnjama te stalno educiranje osoblja. Korištena programska podrška obično treba biti licencirana, bilo na ime agencije ili članova tima koji je 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 te 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 ponovljivost i valjanost dobivenih rezultata.

Koraci razvoja i ispitivanja ovakvih postupaka trebaju biti dokumentirani i sadržavati, [5]:

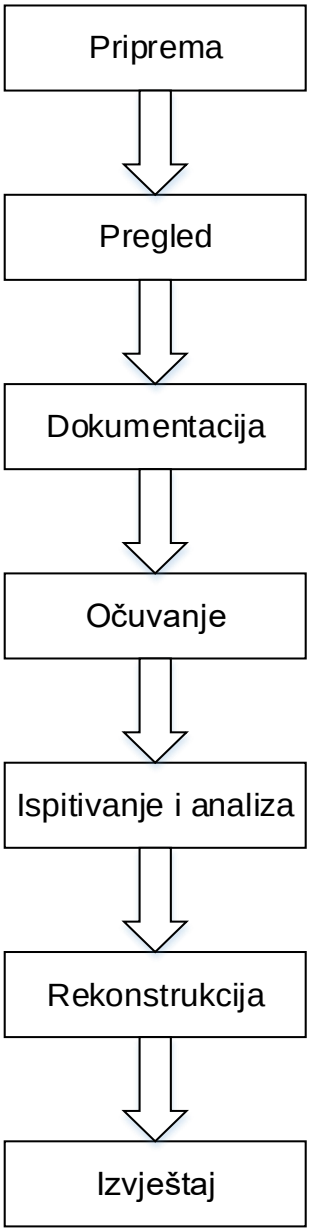
- određivanje zadatka ili problema
- prijedlog mogućih rješenja
- ispitivanje svakog rješenja na poznatom uzorku
- ocjenjivanje rezultata
- oblikovanje postupka.

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

2.3. Forenzička analiza računala

Digitalni istražitelji često obavljaju sve potrebne zadatke; od prikupljanja, dokumentiranja, čuvanja digitalnih dokaza do izdvajanja korisnih podataka kako bi se kreirala jasnija slika istrage kao cjeline. Istražiteljima je potrebna metodologija koja im pomaže obavljati sve zadatke ispravno, a kako bi oni došli do znanstvene istine koje će iskoristiti kao dokaze na sudu. Pravosuđe je jedno od područja gdje je forenzička znanost korisna, nudeći pažljivo provjerene metode za obradu i analizu dokaza te dolaženje do zaključka koji se može reproducirati.

Danas postoji nekoliko različitih metodologija koje se primjenjuju prilikom procesa forenzičke analize računala, a razlikuju se uvelike. U ovom poglavlju opisani su uobičajeni koraci forenzičkih metodologija koje se koriste za računalo koje nije povezano s mrežom. Proces forenzičke istrage računala je opisan dijagramom (slika 1), [6].



Slika 1. Proces digitalne forenzičke istrage računala

Navedene faze služe konačnom cilju, odnosno otkrivanju istine i prezentiranju dokaza. Dokaze je vrlo važno prezentirati na takav način da je njihova svrha olakšati donositeljima odluke proces razmatranja ispravnosti presude.

U stvarnosti, zbog tvrdih diskova koji su velikih kapaciteta i često ograničenog vremena trajanja istrage, istražitelji rijetko pronađu sve relevantne digitalne dokaze na jednom računalu, stoga moraju odlučiti jesu li prikupili dovoljno podataka za navedeni slučaj.

2.3.1. Priprema

Problemi i poteškoće događaju se u svakom poslu pa tako i u ovome. Kako to obično i biva nikada se ne pojavljuju u prikladnom vremenu stoga je poželjno uvijek biti spreman. Vrijeme potrebno za reagirati na određeni incident vrlo je važno kako bi se što brže prikupili potrebni digitalni dokazi.

Kreiranjem kontrolnog popisa osigurava se ispravan pristup prikupljanju potrebnih dokaza i dokumentiranju.

Kontrolni popis treba biti fokusiran na osnovna pitanja, *tko, što, kada i gdje*. Uobičajeni kontrolni popis se sastoji od, [7]:

- datum i vrijeme
- ime i prezime, kontakt osobe koja je pristupila incidentu
- opis otkrića incidenta
- ugrožene stavke sustava (hardver, operativni sustav, lokacija uređaja, mrežne informacije)
- poduzete radnje
- ostala razmatranja, poput pravnih i regulatornih aspekta incidenta.

Proces pripreme sastoji se od niza manjih koraka koji uključuju: pred-pripremu, pripremu detaljnog izgleda slučaja, pripremu plana pretraživanja i određivanje potrebnih resursa, [8].

Pred-priprema obuhvaća otkrivanje i prepoznavanje incidenta, izvođenje procjena rizika i prijetnji, uspostavljanje zapovjedništva za komunikaciju i odlučivanje te dodjeljivanje zadataka odgovornim osobama i priprema dokumentacije.

U *pripremi detaljnog izgleda slučaja* nastaje opći pregled za istraživanje slučaja u kojemu su pripremljeni detaljni koraci uzimajući u obzir procjenu vremena, resursa i novca.

Priprema plana pretraživanja obuhvaća izradu plana na licu mjesta koji sadržava pravila, postupke, dodjeljivanje osoblja i tehničke zahtjeve.

Osim navedenog potrebno je unaprijed definirati korake za provjeru dokaza i nalaza i razviti strategiju pristupa prikupljanja i očuvanja dokaza. Određivanje potrebnih resursa obuhvaća određivanje vrste softvera i hardvera za istragu prema radu sustava i prikupljanje dokaza i materijala za pakiranje i opremu, [8].

Kako bi forenzički istražitelji mogli provoditi istragu prijeko su im potrebni alati o kojima je potrebno pravovaljano brinuti.

Oštećeni alati mogu se popraviti i korigirati kako bi se vratili u upotrebu, a ukoliko to nije moguće potrebno ih je zamijeniti novima kako bi se osigurala kvalitetna i vjerodostojna istraga.

Nužni alati i materijali koje forenzički istražitelj mora posjedovati tijekom provedbe forenzičke analize:

- forenzička radna stanica (slika 2)
- vrećice za dokazne materijale
- antistatička vrećica
- digitalna kamera
- medij za pohranu podataka (tvrdi disk, USB memorija, CD, DVD)
- razni softverski alati
- mrežni i računalni kablovi
- razni alati poput odvijača, svjetiljke, kliješta.

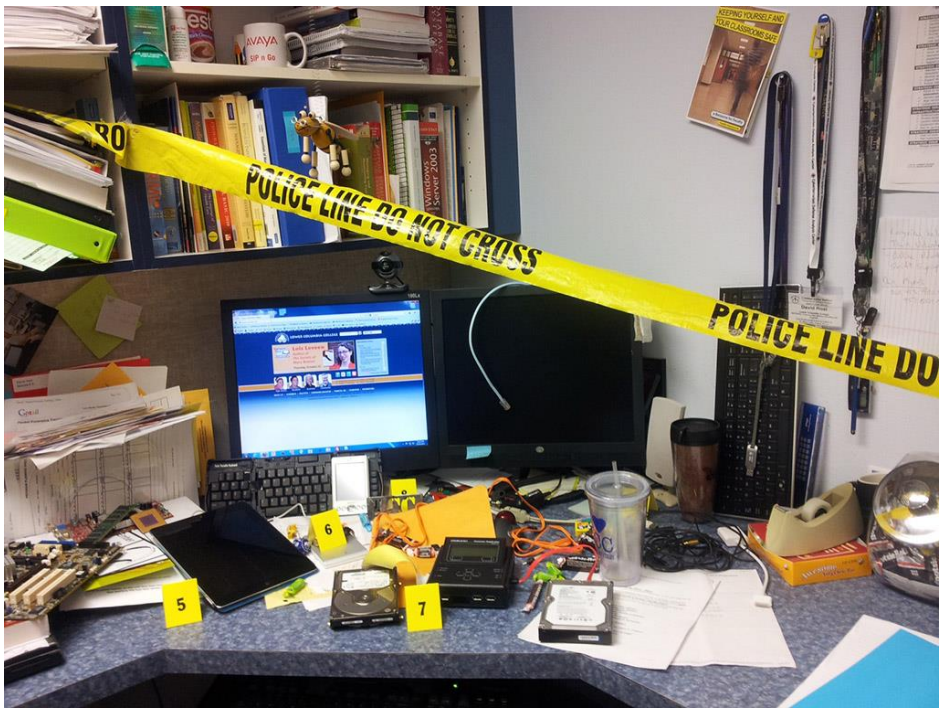
Slika 2. Forenzička radna stanica TALINO KA-Nano, [9]

Kako bi forenzički stručnjaci izvršili svoje zadaće i ispitali mobilne uređaje, razne medije za pohranu, oni koriste forenzičku radnu stanicu. Forenzička radna stanica je posebno dizajnirano računalo za ispitivanje i analizu digitalnih dokaza. Većina radnih stanica posjeduje vrhunske performanse, zahvaljujući višejezgrenim procesorima, količini radne memorije i velikog prostora za pohranu (SSD i HDD).

2.3.2. Pregled

Pregled mjesta istrage metodičan je proces koji uključuje pronalaženje svih potencijalnih izvora digitalnih dokaza te donošenje odluke o tome koji digitalni dokaz je potrebno sačuvati.

Jedini učinkoviti pristup provođenja metodičkog pregleda jest onaj kada se područje istrage razdijeli na mrežu, a svaki segment mreže zasebno se pregleda. Dijeljenjem mreže na ovakve manje segmente bitno umanjuje propuste kao što je npr. neki bitan dokaz: mala memorijska kartica ili skriveni dio medija.



Slika 3. Pregled dokaza na mjestu istrage, [10]

Općenito gledano, pregled mjesta istrage u svrhu pronalaska digitalnih dokaza je dvostruki proces. U prvom dijelu, digitalni istražitelj mora prepoznati hardver koji sadrži digitalne informacije, dok u drugom dijelu digitalni istražitelji moraju prepoznati razlike između nevažnih informacija koje mogu upućivati na počinjeno djelo, ili mogu osigurati poveznicu između žrtve i zločinca (slika 3).

Tijekom pregleda, upute i kutije povezane s hardverom i softverom mogu nagovijestiti koji je hardver korišten, te koji je softver instaliran. Primjena znanstvenih metoda tijekom istraživanja, uključuje razvoj i testiranje teorije o tome koje stavke sadrže relevantne digitalne dokaze, zašto očekivane stavke nedostaju i gdje se mogu pronaći.

Postoji mnogo proizvoda koji mogu sadržavati digitalne dokaze kao npr.: prijenosna računala, stolna računala, poslužitelji, usmjerivači, vatrozid i ostali mrežni uređaji. Uz to, također, postoji jako puno oblika medija za pohranu uključujući CD, disketu, magnetsku vrpcu, disk i USB memoriju. Različiti zločini rezultiraju različitim vrstama digitalnih dokaza. Sposobnost prepoznavanja dokaza ovisi o digitalnom istražitelju, odnosno njegovom poznavanju zločina koji je počinjen, operativnog sustava i računalnih programa koji su uključeni u proces. Osim traženja korisničkih dokumenata i multimedijskog sadržaja, digitalni istražitelji mogu pronaći relevantne podatke u registru, log datotekama i artefaktima poveznim s aplikacijom koja se koristi na računalu. Različite vrste digitalnih dokaza na računalu ograničene su samo na aktivnosti korisnika i kreativnost, [6].

2.3.3. Dokumentacija

Digitalni istražitelj nikako ne može biti osoba koja nema razvijene organizacijske vještine ili osoba koja jako teško prati točne bilješke. Upravo je to zbog toga što većina posla koju obavlja istražitelj sadrži brojnu, prije svega, vrlo važnu dokumentaciju.

Postoji pet razina dokumentacije koje se moraju održavati ili stvoriti tijekom svakog slučaja, a to su, [11]:

- opća dokumentacija slučaja
- proceduralna dokumentacija
- procesna dokumentacija
- vremenska crta slučaja
- lanac posjeda dokaza.

Opća dokumentacija slučaja započinje u trenutku kada je od istražitelja zatražena provedba istrage. U slučaju da istražitelj ne prihvaća izvršiti istragu, i tada je potrebno voditi dokumentaciju jer postoji mogućnost da će netko od nadležnih tijela zatražiti objašnjenje zašto je istraga odbijena.

Za razliku od opće dokumentacije, tijekom ispunjavanja *proceduralne dokumentacije* istražitelj bilježi svaki korak koji učini, alat koji je korišten za određeni zadatak, opis svake provedene procedure i kratak sažetak. Neke od organizacija koje se bave djelatnošću digitalne forenzike imaju vlastite predloške za istragu.

Proceduralna dokumentacija uključuje: zapise svih dokaza koju su pronađeni na mjestu istrage, točan zapis korištenih alata, egzaktan zapis o pronađenim podatcima (lokacija, vrijeme, podatci istražitelja).

U slučaju da je potrebno dokaze transportirati, potrebno je opisati kako su podaci zapakirani i zaštićeni. Procesna dokumentacija nije nužna u svakom izvješću, ali mora uvijek biti dostupna ako bi je zatražio sudac ili suprotni branitelj prilikom suđenja, [11].

Procesna dokumentacija mora sadržavati, [11]:

- upute za upotrebu
- upute za instalaciju
- datoteke pohranjene na instalacijskom medije
- ažurirane priručnike
- popis nadogradnji ili instalacijskih zakrpa.

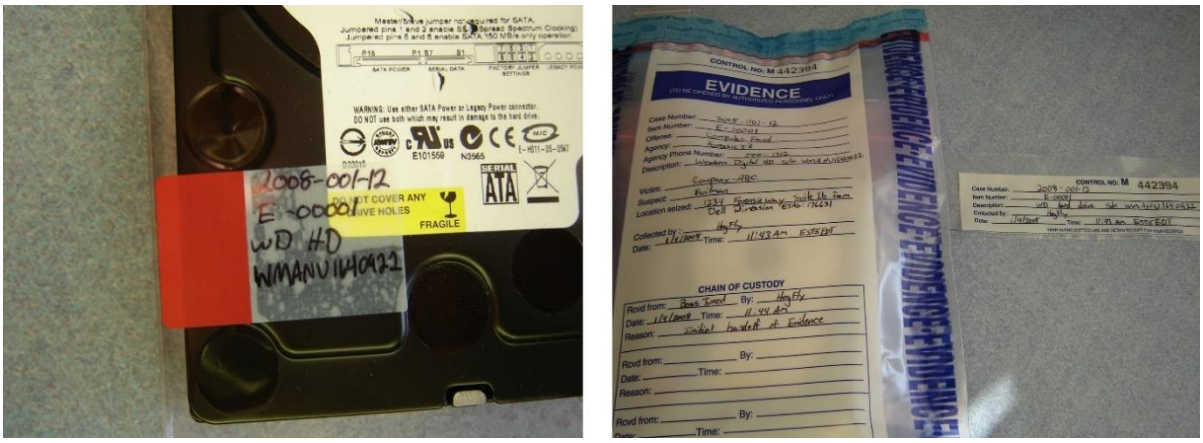
Svaki digitalni dokaz predstavlja potencijalni dokaz koji može biti korišten tijekom sudskog procesa. Kako bi se očuvao lanac posjeda dokaza potrebno je držati se pravila i digitalne dokaze pažljivo čuvati. Nužno je svaki dokaz koji je prikupljen, ostaviti u dokaznoj vrećici, zaključati i onemogućiti bilo kakav pristup dokazu kako bi se zaštitio od bilo kakve modifikacije podataka, brisanja ili dupliciranja. Ukoliko je lanac kompromitiran, dokaz se odbacuje i time se gubi sav uložen trud, a sudac poništava istragu, [12].

2.3.4. Očuvanje

Za razliku od tradicionalnih dokaza koji se susreću tijekom istraga, digitalni dokazi su jako osjetljivi. Kada se područje istrage osigura, prvi korak je prikupljanje tradicionalnih dokaza kao što su to npr. otisci prstiju. Tijekom digitalne forenzičke istrage dokazi nisu odmah vidljivi forenzičkom istražitelju, stoga se mora izvršiti puna forenzička analiza računala.

Forenzički stručnjak prikuplja dokaze koji se nalaze na računalu i nakon toga računalo se nosi u laboratorij. Prilikom iskopčavanja računala s distribucijske mreže, svi podaci koji nisu spremljeni na disk će nestati, a to može predstavljati gubitak velike količine podataka.

Podaci se moraju pravilno, brzo i nesmetano pohraniti na medij kako bi se u potpunosti očuvali. Na taj način ispravno su pohranjeni podaci na odgovarajući medij koji se zatim ubacuje u dokaznu vrećicu (slika 4). Za pohranu podataka često se koriste tvrdi diskovi, USB memorija, a u prošlosti koristile su se diskete.



Slika 4. Označavanje dokaznog diska i umetanje u dokaznu vrećicu, [13]

Najbolja i najbrža metoda za prikupljanje podataka s računala je putem mrežne veze. Bitno je odspojiti računalo s mreže, tj. spriječiti komunikaciju računala kako bi se izbjegli potencijalni napadi. Nakon toga računalo možemo spojiti na koncentrator (engl. *Hub*) kako bi se podaci s tog računala mogli dalje distribuirati po potrebi. Prvi bitni podaci s računala koje je potrebno prikupiti su podaci memorije, a nakon toga slijede ostali, [14].

2.3.5. Ispitivanje i analiza

Priroda i opseg pregleda digitalnog dokaza ovise o poznatim okolnostima istrage i ograničenjima postavljenima pred istražitelje. Ako je računalo plod ili sredstvo istrage, digitalni istražitelji fokusirat će se na hardver. U slučaju da zločin uključuje krijumčarenje informacija, digitalni istražitelji tražit će sve što se odnosi na te informacije, uključujući i hardver koji sadrži informacije i korišten je za njihovu produkciju.

Ako su informacije na računalu dokazi i ako digitalni istražitelji znaju što traže, prilično brzo mogu se izvući potrebni dokazi .U nekim slučajevima istražitelji ispitivanje moraju obaviti na licu mjesta u zadanom roku te se tada u takvim situacijama, upotrebljavaju mobilne jedinice za stvaranje forenzičke slike tvrdog diska računala (slika 5). Primjerice, ukoliko je riječ o tajnoj istrazi ili podatkovni medij je prevelik kako bi se prikupili dokazi u potpunosti, istraga se može premjestiti u prostoriju.

Slika 5. Forenzička mobilna jedinica za stvaranje forenzičkih slika tvrdog diska, [15]

Također, potrebni su i brzi pregledi u raznim okolnostima, npr. u slučaju da postoji strah kako će se zločin ponoviti. U drugim situacijama, potrebno je dugotrajno istraživanje u kontroliranom okruženju.

Proces filtriranja irelevantnih, povjerljivih ili povlaštenih podataka uključuje sljedeće, [6]:

- uklanjanje valjanih sustavskih datoteka i ostalih dobro poznatih entiteta koji nisu relevantni u istrazi
- fokusiranje na najvjerojatniji podatak koji je stvorio korisnik
- fokusiranje na datoteke s ograničenim vremenom
- upravljanje dvostrukim datotekama, što je osobito korisno kada se radi o rezervnim vrpcama
- prepoznavanje neslaganja između alata za ispitivanje digitalnih dokaza.

Manje metodične tehnike smanjivanja podataka, kao što je to pretraživanje određenih ključnih riječi ili izvlačenje samo određenih vrsta datoteka može biti efektivno u određenim slučajevima. Pretraga nespecificiranih ključnih riječi može istražitelju pokazati velik broj nebitnih dokaza, što mu samo otežava istragu i oduzima vrijeme.

2.3.6. Rekonstrukcija

Istraživačka rekonstrukcija vodi do kompletnije slike istrage: što se dogodilo, tko je počinitelj, kada, gdje i zašto. U nastojanju da se identificiraju odnosi između osumnjičenih, žrtava i mjesta istrage, korisno je stvoriti čvor koji predstavlja mjesta gdje su oni bili, korištene e-mail i IP adrese, financijske transakcije, birane telefonske brojeve te utvrditi postoje li ikakve veze između tih čvorova. U istrazi velike prevare, predstavljajući prijenos fonda crtanjem linija između individualaca i organizacije može otkriti najvažnije entitete. Kada se istražuje zločin, poželjno je znati vrijeme i slijed događaja. Većina operativnih sustava prati trag kreiranja, posljednje modifikacije i vrijeme pristupanja datotekama i mapama. Oznaka datuma i vremena može ukazivati na to što se kada dogodilo, te primjerice u slučajevima krađe podataka lako može prikazati koliko je vremena potrebno za izvršavanje takvog dijela, [6].

2.3.7. Izvještaj

Posljednja, ali ne i manje važna faza forenzičke istrage je integriranje svih nalaza i zaključaka u jedan dokument, tzv. izvještaj. Forenzički izvještaj predstavlja kulminaciju procesa koji uključuju intenzivan i mukotrpan rad. Izvještaj bi trebao biti ogledalo profesionalizma forenzičkih stručnjaka uključenih u slučaj istraživanja i prikupljanja dokaza. Izvještaj bi trebao biti dobro organiziran, bez gramatičkih i pravopisnih pogrešaka. Također, izvještaj mora biti jasno napisan kako bi čitatelj izvještaja u jednom pregledu mogao razumjeti napisano te na osnovu toga odrediti poruku samog izvještaja. Ukoliko čitatelj izvještaja, najčešće sudac, ne može razumjeti napisano, ima pravo na odbacivanje izvještaja i zahtijevanje novog, [16].

Oblik i sadržaj izvještaja o forenzičkoj analizi računala može sadržavati različite podatke, ali prema osnovnim pravilima moraju sadržavati navedeno, [17]:

- podatke o agenciji
- identifikacijski broj slučaja
- identitet podnositelja
- datum primitka
- datum izvještaja
- popis predanih stavki na ispitivanje, serijski broj, naziv proizvođača i model
- identitet i potpis istražitelja
- kratak opis koraka koji se poduzimaju tijekom ispitivanja
- rezultat/zaključak.

3. Karakteristike forenzičke analize mobilnih uređaja

Tijekom proteklih nekoliko godina, digitalni forenzični istražitelji vidjeli su značajan porast zahtjeva za ispitivanjem podataka s mobilnih telefona i drugih mobilnih uređaja. Ispitivanje i izvlačenje podataka s ovih uređaja predstavlja brojne jedinstvene izazove za forenzičare. Jedan od izazova je raznolikost mobilnih uređaja, tj. takvi uređaji koriste razne operativne sustave, ugrađene datotečne sustave, aplikacije, usluge i periferne uređaje. Svaki od tih jedinstvenih uređaja može biti podržan na različitim razinama dostupnim forenzičkim softverskim alatima ili uopće ne može biti podržan. Nadalje, uvijek je prisutno kašnjenje podrške forenzičkih alata za novijim mobilnim uređajem, [18].

Mobilni uređaji koriste razne unutarnje, izmjenjive i on-line mogućnosti pohrane podataka. U mnogim slučajevima potrebno je koristiti više od jednog alata za izdvajanje i dokumentiranje željenih podataka s mobilnog uređaja i medija za pohranu podataka. U određenim slučajevima, alati koji se koriste za obradu mobilnih telefona mogu prijaviti sukobljene ili pogrešne informacije. Podaci o mobitelu često su poželjni za obavještajne svrhe i atraktivna je sposobnost procesiranja telefona na terenu.

U ovu kategoriju uređaja koje istražuje mobilna forenzika ubrajaju se:

- mobilni uređaji
- pametni telefoni
- tablet uređaji
- pametni satovi
- GPS uređaji (engl*. Global Positioning System*)
- dlanovnici
- digitalne kamere i fotoaparati
- digitalni diktafoni
- uređaji za reprodukciju zvučnih zapisa (npr. Mp3 player i iPod).

Stoga ne čudi što su istražiteljima veoma zanimljivi podaci koji se mogu pronaći na mobilnim uređajima kao što su, [19]:

- povijest poziva
- kontakti
- multimedijske i tekstualne poruke
- podaci u kalendaru (sastanci, rođendani)
- slike, video zapisi i audio zapisi
- e-mail i podaci društvenih mreža
- karte
- povijest pregledavanja web stranica.

3.1. Izolacija mobilnog uređaja

Prije nego li se istražitelji udalje od mjesta pronalaska mobilnog uređaja ili započinjanja ekstrakcije podataka, potrebno je provesti izolaciju mobilnog uređaja. Izolacijom uređaja sprječava se bilo kakav utjecaj na dokaze, poput udaljenog brisanja podataka. Tehnike ili metode za izolaciju uređaja često ovise o tipu uređaja. Bez obzira na metodu ili tehniku, izolacija uređaja mora ostati konstantna za cijelu pretragu ako je uređaj uključen. U ovom odjeljku pokriva se nekoliko različitih metoda i tehnika izolacije, od ručnog mijenjanja komunikacije uređaja do postavljanja u prostore bez prisutnosti radio valova.

Slika 6. Vrećica za izolaciju mobilnog uređaja, [20]

Tijekom odabira vrste metode izolacije, ispitivač mora zapamtiti da različiti čimbenici mogu ometati dosljednost i pokrivenost tehnike. Tehnike koje koristi ispitivač potrebno je testirati na svim frekvencijama koje su se susrele tijekom ispitivanja. Možda gubitaka podataka neće biti, ali integritet podataka bit će izmijenjen dodatkom informacija koje nisu povezane sa slučajem. U slučajevima kada uređaj pristupi mobilnoj mreži ili Internetu, signal koji se šalje uređaju može i na daljinu obrisati sve podatke s uređaja, što čini bilo koju vrstu oporavka nemogućim, [21].

Razni načini za izoliranje mobilnog uređaja iz mreže postoje, a njihove razlike brojne su. Proizvodi za izolaciju kreću se u rasponu od besplatnih do onih po cijeni od tisuća dolara. Neki proizvodi izolacije signala prenosivi su, dok drugi nisu. Neki proizvodi zahtijevaju praktičnu upotrebu, drugi ne zahtijevaju.

Svaki uređaj koji će ispitivač koristiti mora biti provjeren prema stvarnim scenarijima, ali i testiran prije odlučivanja o najboljem rješenju jer mnoge varijable mogu utjecati i na najskuplje uređaje.

Ako se pretraga uređaja provodi samo u laboratoriju, testiranje se olakšava. Faraday-eva vrećica (slika 6) izgleda jako slično antistatičkoj vrećici, ali za razliku od nje, ona štiti uređaj od proboja vanjskoj signala do mobilnog uređaja koji se nalazi u vrećici. Izrađena je od materijala koji mogu blokirati bežične signale čime čuva integritet uređaja od vanjskog svijeta, [22].

Slika 7. Blokator signala mobilnog uređaja, [23]

Blokatori signali (engl. *Jammer)* uređaji su koji odašilju istu frekvenciju kao i mobilni uređaji čime ometaju komunikaciju između mobilnog uređaja i bazne stanice (slika 7). Osobni blokatori signala, kakve koriste istražitelji, najčešće su malih dimenzija i omogućavaju stvaranje „mrtvog područja“ od otprilike 9-30 m ovisno o modelu. Upotrebom blokatora signala, istražitelj osigurava mobilni uređaj od bilo kake komunikacije tijekom istrage, [24].

Najlakša tehnika koja se može izvršiti je postavljanjem uređaja u zrakoplovni mod. Postavljanjem uređaja u zrakoplovni mod onemogućava se bilo kakva komunikacija mobilnog uređaja, ali mnogi istražitelji ne primjenjuju ovu metodu pa posežu za drugima.

3.2. Postupci i metode ekstrakcije podataka

Ekstrakcija podataka je postupak prikupljanja bitnih dokaza iz različitih vrsta medija kako bi se dobiveni dokazi mogli obraditi ili pohraniti. Za potrebe forenzičke analize mobilnog uređaja, ovaj postupak neophodan je i zahtijeva puno pažnje. Vrijeme trajanje ekstrakcije podataka s mobilnog uređaja ovisi o sadržaju, odnosno o samoj količini podataka koja je bitna forenzičkom istražitelju. Na slici 8 prikazan je omjer brzine obavljanja ekstrakcije podataka i količine dobivenih podataka. Stoga, ručna ekstrakcija pripada najbržoj metodi ekstrakcije podataka, ali količina dokaza nije ni približna količini podataka koju daje Micro read ekstrakcija.

Slika 8. Usporedba brzine ekstrakcije i količine dobivenih podataka, [25]

Postoje razne metode ekstrakcije podataka, od onih jednostavnijih kojima se prikupljaju samo nužni podaci, a samim time takva ekstrakcija ne zahtijeva puno vremena, do onih kompliciranijih ekstrakcija za koje je potrebno puno više vremena i specijaliziranijih alata. Takve ekstrakcije namijenjene su posebnim službama kao što su: vojska, policija, obavještajne agencije i tvrtke čija je primarna djelatnost digitalna forenzika.

3.2.1. Ručna ekstrakcija

Ručna ekstrakcija podataka provodi se u slučaju kada je uređaj uključen i otključan. Istražitelj ručno pristupa uređaju preko korisničkog sučelja te mu je omogućen pregled postavki mobilnog uređaja i, naravno, sav sadržaj koji je dostupan korisniku. Kako bi se osiguralo da su sve pojedinosti detalja dokumentirane, cijeli proces je potrebno fotografirati. Zbog svoje jednostavnosti, za provođenje ovakve ekstrakcije nije potrebno osposobljavanje.

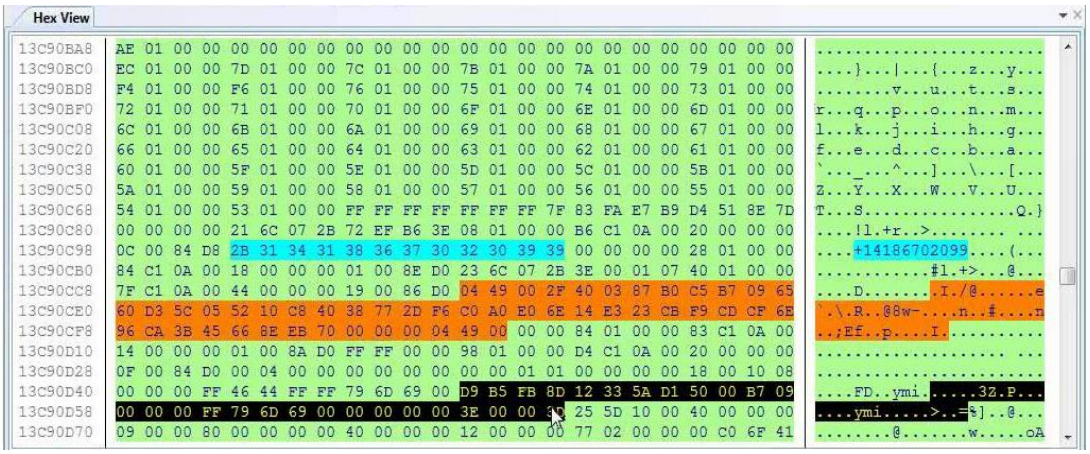
3.2.2. Logička ekstrakcija

Logička ekstrakcija uključuje povezivanje mobilnog uređaja s forenzičkim hardverom ili forenzičkom radnom stanicom putem USB kabela, RJ-45 kabela, infracrvenog ili Bluetooth veze. Nakon spajanja, računalo pokreće naredbu i šalje ga na uređaj, a zatim ga interpretira procesor. Zatim, traženi podaci se primaju iz memorije uređaja i šalju natrag na forenzičku radnu stanicu. Kasnije, ispitivač može pregledavati podatke. Većina trenutno dostupnih forenzičkih alata radi na ovoj razini klasifikacijskog sustava. Postupak ekstrakcije je brz, jednostavan za korištenje i zahtijeva kraći trening za ispitivače. Nasuprot tome, proces može zapisivati podatke na mobitel i tako može promijeniti cjelovitost dokaza. Osim toga, izbrisani podaci gotovo nikada nisu dostupni, [26].

3.2.3. Hex dump

Hex dump jedan je od načina fizičke ekstrakcije sirovih podataka pohranjenih u flash memoriji. Ekstrakcija Hex dump metodom provodi se spajanjem uređaja na forenzičku radnu stanicu, nakon čega slijedi prijenos nepotpisanih kodova ili bootloader-a u uređaj. Svaki od njih nosi instrukciju za preuzimanje memorije s mobilnog uređaja na računalo, odnosno forenzičku radnu stanicu. U konačnici, rezultat toga su podaci zapisani u binarnom sustavu kojeg istražitelj može analizirati samo u slučaju da jako dobro poznaje binarni zapis, [27].

S obzirom na to da su podaci u binarnom obliku, istražitelju se nudi opcija upotrebe nekih od forenzičkih alata (npr. Oxygen Forensic Suite ili UFED Physical Analyzer), a sve to kako bi na zaslonu mogli vidjeti heksadecimalne vrijednosti. Forenzički alati posjeduju Hex uređivače koji omogućavaju pregled i pretraživanje nepristupačnih prostora u memorijama i oporavak izbrisanih datoteka (slika 9).



Slika 9. Prikaz heksadecimalnog zapisa pomoću Hex preglednika, [28]

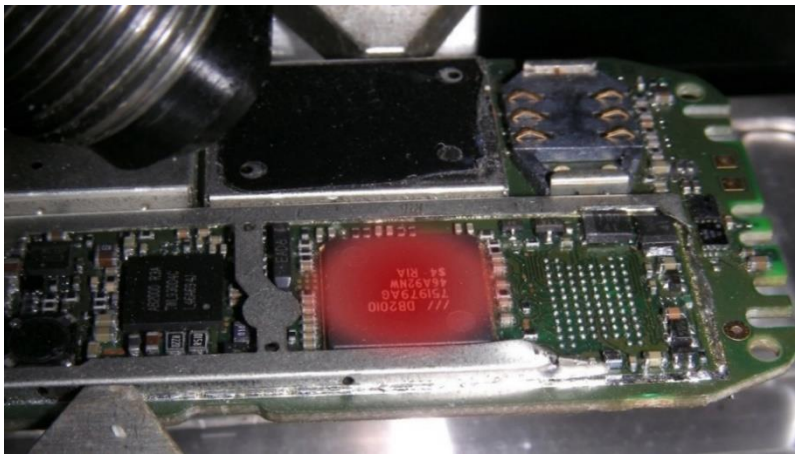
Forenzički postupak najviše ovisi o modelu uređaja, ali iz svakog mobilnog uređaja moguće je dobiti sljedeće, [29]:

- popis poziva
- imenik
- kalendar
- poruke
- predmemoriju interneta
- postavke uređaja
- izbrisane datoteke
- Hex dump datotečnog sustava.

3.2.4. Chip-off

Chip-off napredna je tehnika ekstrakcije digitalnih podataka koja uključuje fizičko uklanjanje flash memorijskog čipa iz uređaja i dobivanje neobrađenih podataka pomoću specijalizirane opreme. Memorijski čip odvaja se od uređaja, te se postavlja na čitač čipa ili drugi identični mobilni uređaj u svrhu izdvajanja podataka pohranjenih na uređaju. Ovakva metoda je tehnički zahtjevna zbog velikog broja vrste čipova. Također, proces Chip-off je skup, potrebna je obuka a ispitivač mora posjedovati potrebne alate za odlemljivanje i zagrijavanje memorijskog čipa (slika 10), [27].

Čak i najmanja pogreška može dovesti do oštećenja memorijskog čipa i trajnog gubitka podataka. Ova metoda često se koristi kada druge metode ekstrakcije nije moguće provesti ili kada je jako bitno sačuvati točno stanje memorije uređaja.



Slika 10. Primjena Chip-off metode zagrijavanjem čipa uređaja, [30]

Postupak Chip-off metode sastoji se od četiri koraka, [31]:

- fizičko uklanjanje čipa korištenjem lemilice ili posebnih kemijskih sredstava
- čišćenje i popravljanje čipa
- ekstrakcija podataka s čipa
- analiziranje dobivenih podataka s čipa forenzičkim alatima.

3.2.5. Micro read

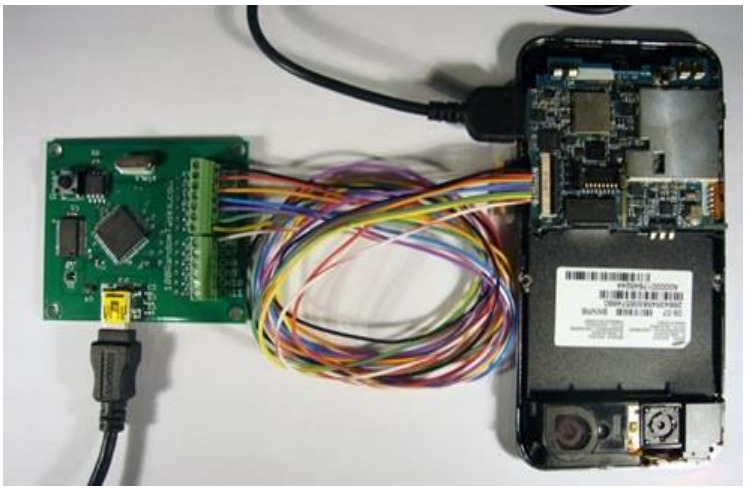
Micro read metodom vrši se ekstrakcija podataka fizičkim pregledom ulaza NAND ili NOR čipa koristeći se elektronskim mikroskopom. Zbog složenog postupka i spore analize, ova metoda primjenjiva je samo onda kada ostale metode ne daju zadovoljavajuće rezultate, [32]. Ova vrsta ekstrakcije provodi se u slučajevima visokog prioriteta, primjerice kada je ugrožena nacionalna sigurnosti. Danas, ovaj se proces gotovo rijetko kada provodi i nema komercijalnih alata koji imaju mogućnosti provesti Micro read metodu.

3.2.6. Ekstrakcija podataka JTAG metodom

JTAG (engl. *Joint Action Test Group*) metoda omogućuje forenzičkim istražiteljima da fizički „steknu“ uređaj kao što je pametni telefon. U digitalnom forenzičkom svijetu, "fizička akvizicija" odnosi se na izradu kompletnih (ili potpunije mogućih) slika svakog čipa u uređaju koji može pohraniti podatke. Suprotno je to stjecanju datotečnog sustava koji samo kopira datotečni sustav (uključujući strukturu i datoteke direktorija) i logičku akviziciju koja samo stječe sadržaj određenih objekata za pohranu.

Fizička akvizicija omogućuje da forenzičar pregleda sve, uključujući i stvari koje bi propustili ili stvari koje ne bi se uspjele izvući u višim površinskim ekstrakcijama.

No, kako bi fizički stekli uređaj poput pametnog telefona, forenzički istražitelj mora izravno pristupiti flash memorijskim čipovima unutar telefona. Taj postupak može zahtijevati invazivne i destruktivne postupke čišćenja koje može obaviti samo stručno i visoko obučeno osoblje za pažljivo uklanjanje čipova i potpuno rastavljanje pametnog telefona. JTAG forenzika daje forenzičarima različit pristup invazivnoj chip-off metodi. Za JTAG metodu, forenzički istražitelj povezuje vod do specifičnih pristupnih priključaka za testiranje na matičnoj ploči telefona, čime se podaci s NAND ili NOR flash memorijskih čipova pametnog telefona mogu izvući kroz njih izravno na sustav ispitivača (slika 11), [33].



Slika 11. JTAG ekstrakcija podataka s mobilnog uređaja, [34]

Danas, komercijalni alati za JTAG ekstrakciju ne postoje i rijetki su oni koji mogu izvesti ovakvu kompliciranu ekstrakciju.

4. Usporedni prikaz forenzičke analize računala i mobilnih uređaja

Tijekom forenzičke analize provode se isti procesi za forenzičku analizu računala i forenzičku analizu mobilnih uređaja. Iako je proces isti, procedura postupka različita je. Slika 12 prikazuje prednosti i nedostatke u forenzici mobilnih uređaja i računala. Jedna od glavnih i najvažnijih razlika je način na koji su podaci prikupljeni iz sustava. Primjerice, u slučaju da se provodi analiza isključenog računala, podatke je moguće preuzeti iz tvrdog diska i to procesom stvaranja slike pomoću forenzičke radne stanice.

Slika 12. Usporedba problematike forenzike računala i mobilnog uređaja, [6]

Proces stvaranja slike forenzički je ispravan način kopiranja svakog sektora diska, a to uključuje i nedodijeljeni prostor. U slučaju da je riječ o isključenom mobilnom uređaju, stvaranje forenzičke slike mobilnog uređaja zahtjeva uključivanje uređaja.

Bitna razlika je promjena stanja uređaja. Ukoliko je računalo ugašeno njegovo stanje se ne mijenja, dok prilikom ponovnog uključivanja mobilnog uređaja može doći do promjena stanja uređaja i zapisivanja novih podataka. Veliki problem stvaraju razne inačice operativnih sustava mobilnih uređaja i sam hardver, što zapravo ovisi od samog proizvođača uređaja, [35].

U nastavku ovog poglavlja analizirane su mogućnosti i karakteristike forenzičkih alata za forenzičku analizu računala ProDiscover Basic, OSForensics, FTK i EnCase, a zatim je prikazana usporedba forenzičkih alata koji su namijenjeni forenzici mobilnih uređaja, a to su: Cellebrite UFED Logical Analyzer, Paraben DDS, Oxygen Forensic Suite, MOBILedit! Forensics i XRY Logical. Osim usporedbe alata, uspoređeni su i izvori podataka koji su jako bitni.

4.1. Usporedba svojstva forenzičkih alata

Kako bi forenzički stručnjaci lakše obavili istragu, bilo da je riječ o računalu ili mobilnom uređaju, potrebno je odabrati alat koji najbolje zadovoljava potrebe istrage. Izbor pravog alata je krucijalan i stoga je potrebno uvidjeti funkcije i pod funkcije koje nudi određeni alat. Izbor pravog alata za provedbu analize veliki je izazov jer još uvijek nije istraženo cijelo područje forenzike. Kako bi se istraga pojednostavila i olakšala, neovisno o vrsti uređaja koja se pregledava, potrebno je odabrati alat koji zadovoljava potrebe istrage. Izbor takvog alata od velike je važnosti stoga je potrebno i razmotriti koje sve funkcije alat nudi.

Forenzičke alate možemo klasificirati u nekoliko kategorija, [36]:

- alati za snimanje diska i podataka
- preglednici datoteka
- alati za analizu datoteka
- alati za analizu registra
- alati za analizu ip prometa
- alati za analizu e-pošte
- alati za analizu mobilnih uređaja
- Mac OS alati za analizu
- mrežni forenzički alati
- alati za forenziku baze podataka.

Široka paleta alata uključuje specijaliziranu opremu, računalni hardver i softver koji su nužni tijekom istrage kako bi se dobili potrebni dokazi s elektroničkog uređaja.

4.1.1. Alati za forenzičku analizu računala

Računala su vrlo važan dokaz jer podaci s računala uvijek su točni osim u slučajevima kada je primijenjena neka od antiforenzičkih metoda. Tijekom pronalaženja podataka, pa čak i onih dublje skrivenih, koriste se različiti forenzički alati.

Glavna svrha tih alata je pružanje pomoći istražiteljima u istrazi, ali uz to oni rade i na ubrzanju tijeka istrage. Najčešće se preporučuje upotreba nekoliko različitih alata jer svaki od njih daje drukčije rezultate. Kako bi se uočile razlike između alata, u nastavku opisane su mogućnosti koje pružaju alati dok su njihove funkcije i podfunkcije opisane u tablici 1.

ProDiscover Basic je forenzički alat koji omogućuje istražitelju pronalazak podataka na disku računala pritom štiteći dokaze i kreiranje izvještaja. Za razliku od ostalih alata, ovaj alat nema mogućnosti dekriptiranja ekstraktiranih podataka i dekompresiju podataka. GUI (engl. *Graphical User Interface*) sučelje omogućuje brzo i lako korištenje, [37]. Osim toga, brojni su nedostatci ProDiscover Basic-a, počevši od akvizicije pa do nemogućnosti provođenja postupka enkripcije.

OSForensic demo verzija nema mogućnosti pregleda NTFS (engl. *New Technology File System*) direktorija i uvoz i izvoz Hash-a. Može detektirati mali broj nedavnih aktivnosti. Prednost ovog alata je u njegovom besplatnom preuzimanju što omogućuje korisniku da u 30 dana isproba demo verziju i naknadno odluči želi li kupiti punu verziju koja sadržava i dodatne mogućnosti, [38].

Produkt kompanije AccessData, FTK (engl. *Forensic Toolkit*) pripada naprednijim forenzičkim alatima za računalnu forenziku. Kao što možemo vidjeti iz tablice 1, FTK od preostala tri forenzička alata ima najviše mogućnosti i upravo zbog toga je favoriziran do strane stručnjaka računalne forenzike.

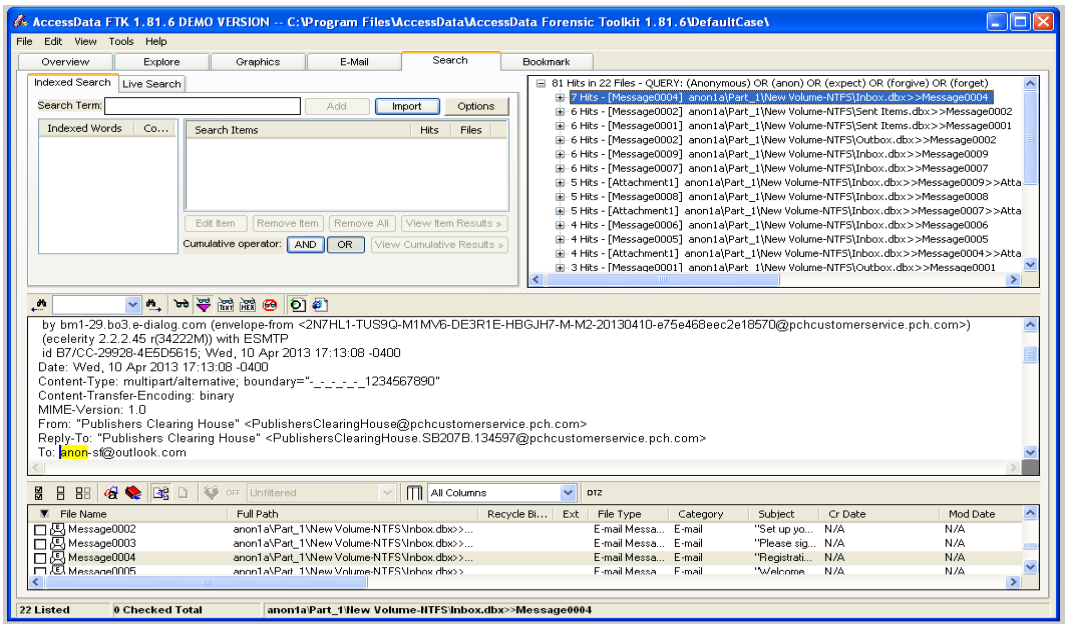
FTK ima mogućnost oporavka lozinki za veliki broj aplikacija, a uz to jako je stabilan alat tijekom čijeg korištenja ne dolazi do rušenja. Vizualizacijska tehnologija omogućuje prikaz podataka preko vremenske crte, graf klastera[1], geo-lokacije i još mnogo toga, [39]. Slika 13 prikazuje grafičko sučelje FTK alata.

[1] Klaster je skupina nekoliko sektora tvrdog diska

Tablica 1. Mogućnosti forenzičkih alata za računalnu forenziku

KARAKTERISTIKE	FORENZIČKI ALATI			
	ProDiscover Basic	OSForensics demo verzija	FTK	EnCase Forensic
Akvizicija				
Fizička kopija podataka	DA	DA	DA	DA
Logička kopija podataka	DA	DA	DA	NE
Datotečna akvizicija	DA	DA	DA	DA
GUI	DA	DA	DA	DA
Udaljena akvizicija	NE	DA	DA	DA
Validacija i verifikacija				
Hashing	DA	DA	DA	DA
Verifikacija	DA	DA	DA	DA
Filtriranje	NE	DA	DA	DA
Analiza zaglavlja	NE	DA	DA	DA
Ekstrakcija				
Pregled podataka	DA	DA	DA	DA
Pretraživanje	DA	DA	DA	DA
Dekompresija podataka	NE	NE	DA	DA
Dekriptiranje	NE	DA	DA	DA
Označavanje	DA	DA	DA	DA
Rekonstrukcija				
Kopiranje diska na disk	DA	DA	DA	DA
Kopiranje particija	DA	DA	DA	DA
Kopija slike na disk	DA	DA	DA	DA
Kopija slike na particiju	DA	DA	DA	DA
Kopija diska na sliku	DA	DA	DA	DA
Obnova podataka	DA	DA	DA	DA
Izvještavanje				
Označavanje	DA	DA	DA	DA
Log izvještaj	NE	DA	DA	DA
Generator izvještaja	DA	DA	DA	NE

Izvor: [40]



Slika 13. Grafičko sučelje forenzičkog alata FTK, [41]

EnCase alat već je duže prisutan na forenzičkoj sceni i postavio je definiciju kakav treba biti forenzički alat. Ovaj alat nudi nekoliko vrsta enkripcijskih shema, a dokumentacija koju pruža vrhunska je. Stoga, ovaj alat i slovi kao omiljeni među forenzičkim stručnjacima, [42].

4.1.2. Alati za forenzičku analizu mobilnih uređaja

Forenzička analiza mobilnih uređaja slična je analizi računala, ali postoje određene razlike. Neke od najvažnijih razlika su: količina potencijalnih dokaza te raznolikost hardvera i softvera. Ono što je bitno naglasiti je i razlika u osjetljivosti podataka koja je kod mobilnih uređaja izraženija nego kod računala. Naravno, prisutan je konstantan i brz tehnološki razvoja mobilnih uređaja, što zahtjeva stalnu nadogradnju forenzičkih alata.

Forenzički alati za oporavak dokaza sastoje se od hardvera koji obuhvaća razne kablove za povezivanje mobilnog uređaja i radne stanice ili uređaja za ekstrakciju. Softver je potreban kako bi se izdvojili potrebni dokazi, provela analiza i kreirao izvještaj. Na tržištu je dostupno mnogo alata od kojih su jedni komercijalne prirode (UFED i Oxygen Forensic Suite), a drugi otvorenog koda (Autopsy i iPhone Analyzer).

U nastavku, pomoću tablice 2. prikazane su neke od mogućnosti najpoznatijih forenzičkih alata za potrebe analize mobilnih uređaja.

Tablica 2. Mogućnosti forenzičkih alata za forenzičku analizu mobilnih uređaja

KARAKTERISTIKE	FORENZIČKI ALATI				
	Cellebrite UFED Logical Analyzer	Paraben DDS	Oxygen Forensic Suite	MOBILedit!	XRY Logical
Potvrda integriteta podataka					
MD-5	DA	DA	DA	DA	NE
SHA-1	NE	DA	DA	NE	NE
SHA-256	DA	NE	DA	NE	NE
Prikupljanje podataka					
Logičke datoteke	DA	DA	DA	DA	DA
Memorijska kartica	NE	DA	NE	NE	DA
Fizički izvadak[2]	NE	DA	NE	DA	DA
Podrška SIM kartica					
GSM	DA	DA	DA	DA	DA
CDMA	NE	NE	NE	NE	NE
Kloniranje SIM kartice	DA	DA	NE	DA	DA
USIM	DA	DA	NE	NE	DA
Analiza i obrada					
Označavanje	NE	DA	DA	NE	NE
Hex preglednik	NE	DA	DA	DA	NE
Tekstualni preglednik	NE	DA	DA	DA	NE
Multimedijske datoteke	NE	DA	NE	NE	NE
Usporedba podataka	NE	DA	NE	NE	DA
Oporavak podataka	DA	DA	DA	DA	DA
Sortiranje podataka	NE	DA	DA	NE	NE
Mogućnost mapiranja	NE	NE	NE	NE	DA
Preglednik slika	NE	DA	DA	DA	NE
Preglednik registra[3]	NE	DA	NE	NE	NE
Formati izvještaja					
CSV	DA	NE	DA	NE	NE
HMTL	DA	NE	DA	DA	NE
PDF	DA	NE	DA	NE	NE
TXT	NE	NE	NE	DA	NE
XML	DA	NE	DA	DA	DA
Funkcije pretraživanja					
Booleova	NE	DA	NE	NE	NE
Jednostavna	DA	DA	DA	DA	NE

Izvor: [43]

[2] Fizički izvadak kompletnog sadržaja iz uređaja
[3] Windows CE preglednik registra

Cellebrite je izraelska tvrtka specijalizirana za uređaje čija je namjena ekstrakcija podataka, prijenos i analiza mobilnih uređaja. Najpoznatiji proizvod tvrtke Cellebrite je alat UFED. UFED ima dvije inačice, jednu koja može izvršiti logičku ekstrakciju i manje je napredna i drugu koja može izvršavati i fizičku ekstrakciju podataka. Cellebrite UFED podržava velik broj uređaja, raznih proizvođača i različitih operativnih sustava. UFED Logical Analyzer je aplikacija koja čita UFED datoteke (UFED dump datoteke .ufd) i UFED izvješća (.xml) stvorena kao dio logičke ekstrakcije i paketa izvješća UFED (.ufdr) generirane iz analiziranih podataka logičke ekstrakcije UFED Logical Analyzer, [44].

UFED Logical se sastoji od dvije komponente, [44]:

- UFED uređaj (slika 14) s logičkim modulima koji se koriste za stvaranje logičke ekstrakcije s mobilnih uređaja ili SIM (engl. *Subscriber Identity Module*) kartica, a koje se zatim mogu spremiti na USB disk, SD memorijsku karticu ili izravno na računalo.

- UFED Logical Analyzer aplikacija, omogućuje istražiteljima izvođenje dubinske analize podataka ekstraktiranih kao dio logičke ekstrakcije.

Slika 14. Forenzički alat Cellebrite UFED, [45]

Mnogi forenzički istražitelji smatraju Paraben DDS (engl. *Deployable Device Seizure*) nevjerojatnim alatom za brzo dohvaćanje podataka s određenog mobilnog uređaja. Digitalni istražitelji vrlo lako mogu istražiti mobilne uređaje ili bilo koje druge uređaje pomoću DDS-a bez neke posebne obuke.

Paraben DDS dostupan je na tablet uređajima koji su korisni tijekom ispitivanja mobilnog uređaja, digitalnih kamera i SIM kartica na licu mjesta, a mogu pomoći i ovlaštenima osobama u brzom pronalasku dokaza kod osumnjičenih osoba. DDS omogućava dohvaćanje podataka s približno 4000 mobilnih uređaja i otključavanje istih, uključujući sve BlackBerry uređaje, [46].

Oxygen Forensics Suite je mobilni forenzički softver za logičku analizu mobitela, pametnih telefona i dlanovnika razvijen od strane tvrtke Oxygen Osftware. Omogućava izdvajanje informacija o uređaju, kontakte, podatke iz kalendara, SMS poruke, datoteke i ostalo. Osim navedenog moguće je i izdvajanje metapodataka[4] iz uređaja, poput lokacije fotografiranja određene fotografije te očitavanje skrivenih informacija kao što su Wi-Fi i Internet djelatnosti, [47].

MOBILedit Forensics jedini je alat od navedenih koji pruža bežično povezivanje mobilnog uređaja putem Wi-Fi i logičku ekstrakciju. Ovaj alat podržava skoro sve uređaje (uključujući razne generičke kineske uređaje, pa čak i one stare nekoliko godina koji su bazirani na starijim operativnim sustavima, poput Symbian-a, [48].

XRY Logical forenzički je alat švedske tvrtke MSAB koji se koristi za analizu i oporavak podataka s mobilnih uređaja, GPS uređaja i tableta. Omogućuje ekstrakciju podataka s digitalnih uređaja komunikacijom s operativnim sustavom uređaja. Usluga je automatizirana, ali ekvivalent je ručnom pregledavanju svakog zaslona na uređaju i snimanju onoga što se prikazuje. Pomoću XRY formata datoteka, podaci i integritet dokaza sačuvani su od ekstrakcije sve do suda i uvjeravanja, [49].

4.2. Usporedni prikaz digitalnih dokaza

Razvojem tehnologije pojavila se i sve češće zloupotreba računa i mobilnih uređaja. Svaka zloupotreba podataka ostavlja i dokaze iza sebe koji su sveprisutni. Digitalni dokazi najčešće su povezani s e-kriminalom što uključuje dječju pornografiju ili prevare s kreditnim karticama. Naravno, osim e-kriminala, digitalni dokazi prisutni su i u drugim kategorijama kriminalnih dijela, a posebno pomažu u istragama protiv terorizma.

Tijekom prikupljanja digitalnih dokaza stručnjaci moraju biti organizirani i dobro upoznati sa slučajem kako bi uspjeli pronaći što više materijala potrebnog za istragu.

[4] Metapodatci su podatci koji opisuju karakteristike digitalnih podataka

4.2.1. Digitalni dokazi računala

S obzirom na popularnost Microsoft Windows-a operativnog sustava, digitalni istražitelji najčešće se susreću s ovim sustavom kao izvorom digitalnih dokaza na računalima. Rezultat popularnosti Windows operativnog sustava razvoj je moćnih komercijalnih alata koji olakšavaju forenzički pregled računala. Zbog raznovrsnosti Windows operativnih sustava i aplikacija, nije moguće opisati, pa čak ni i identificirati svaki mogući izvor informacije koji bi mogao biti koristan tijekom istrage. Nadalje, svaki slučaj je drukčiji, zahtijeva da digitalni istražitelj istražuje određeni artefakt i operacije na Windows sustavima.

Datotečni sustavi Microsoft Windows operativnog sustava:

- FAT (engl. *File Allocation Table*)
- NTFS

NTFS se značajno razlikuje od FAT datotečnog sustava jer pohranjuje podatke o sustavu na više sustavskih datoteka, a osim toga dizajniran je tako da je moguće oporaviti disk jer ima mogućnost čuvanja kopije sustavske datoteke.

Ono što se pred istražitelje često stavlja kao zadatak i zahtjev jest povrat izbrisanih datoteka iz sustava. Upravo je to često glavni pokazatelj onoga što je osumnjičeni pokušavao sakriti. Kada se datoteka izbriše u NTFS sustavu, ona zapravo nije obrisana fizički, te je moguće oporaviti je, [50].

Log datoteke su važan izvor za određivanje stanja sustava i korištene su za hvatanje događaja koji su se dogodili unutar računalnog sustava i mreža. Log datoteke za forenzičku analizu mogu se poistovjetiti s crnom kutijom zrakoplova, jer bilježe sve događaje koji se događaju u sustavu i na mreži. Također, igraju jako bitnu ulogu u prikupljanju dokaza jer svaki zapis sadrži informacije vezanu uz određeni događaj, [51].

Windows sustavi koriste registre za pohranu konfiguracije sustava i korištenih detalja koji se zovu „ključevi“. Datoteke registra na Windows 95 i 98 nalaze se u instalacijskoj datoteci Windowsa i nose naziv „system.dat“ i „user.dat“. Registar možemo nazvati i trezorom informacija jer sadrži jako puno informacija, poput, [52]:

- konfiguracija sustava
- uređaji u sustavu
- korisničko ime
- lozinka
- osobne postavke
- aktivnosti na web pregledniku
- povijest otvaranih datoteka i itd.

Pristupanjem na Internet ostavlja se velika količina podataka, uključujući posjećene web stranice i ostali pregledani sadržaj. Windows sustavi održavaju zapis računa koji su korišteni za povezivanje na Internet, zapisnik o mrežnim uređajima i aktivnostima. Tijekom posjeta web stranice, web preglednik sprema stranicu i pridružene elemente na disk kao što su slike. Baze podataka web preglednika sadrže informacije koje su bitne istražiteljima stoga dugotrajan pregled baze često rezultira otkrivanjem bitnih podataka. Danas, razvijeni su specijalizirani programski alati za forenziku web preglednika i istražiteljima mogu olakšati istragu.

Važna komponenta forenzičkog pregleda je identificiranje udaljene lokacije gdje se digitalni dokazi mogu nalaziti. Žrtva može održavati web stranicu ili prekršitelj može prenijeti inkriminirajuće podatke na drugo računalo putem Interneta. Jedna od najčešćih udaljenih lokacija za pohranu je ISP (engl*. Internet Service Provider*). Osim toga, za pohranu e-pošte neki ISP daju svojim korisnicima prostor za pohranu web stranica ili podataka. Uobičajeni oblik udaljenog pohranjivanja je zajednički mrežni pogon. Većina Windows sustava može omogućiti da svi ili određeni dio tvrdog diska bude dostupan preko mreže. Mnoge organizacije koriste Windows datotečne servere kako bi omogućili svojim korisnicima prostor za pohranu podataka. Digitalnim istražiteljima ne preporučuje se pristupanje udaljenim lokacijama za pohranu bez autorizacije, čak i kada poznaju lozinku. Primjerice, računalo može biti konfigurirano tako da se automatski spaja na udaljeno mjesto za pohranu. Iako je moguće pristupiti podatcima preko mreže, takav postupak može dovesti do izmjene dokaza, [6].

4.2.2. Digitalni dokazi mobilnih uređaja

Digitalni dokazi na mobilnom uređaju mogu biti različiti u ovisnosti o slučaju, tj. digitalni dokazi ovise o mogućnostima uređaja, te kako je uređaj korišten i što je s njim učinjeno.

Korisni podaci na mobilnom uređaju nalaze se u:

- SIM kartici
- ugrađenoj memoriji (ROM i RAM)
- vanjskoj memoriji (memorijska kartica).

Zbog različitih vrsta uređaja koji su danas dostupni, istražitelji ponekad ne mogu dobiti željene podatke zbog karakteristika uređaja. U najgorem slučaju, istražitelj može pronaći listu kontakata, primljenih i propuštenih poziva, SMS-ova, MMS-ova (engl. *Multimedia Messaging Service*) i sl. na svakom uređaju, neovisno o kategoriji uređaja (pametni telefon ili mobilni uređaj), što je i prikazano u tablici 3.

Tablica 3. Izvori podataka na mobilnom uređaju

Izvor podataka	Podatci
SIM kartica	Broj pretplatnika, identifikator kartice, birani brojevi, lokacija
Davatelj usluge	Zapisnik poziva, korištenje interneta, informacije naplate, popis povijesti spajanja na bazne stanice, te neprecizna trenutna lokacija
Pametni telefon	Fotografije, vidio i audio sadržaj, MMS i SMS poruke, email poruke, pohranjeni podatci, GPS upute, online računi, lokacija, itd
Osnovni telefon	Popis kontakata, SMS, kalendar, popis poziva

Izvor: [6]

Forenzika društvenih mreža na pametnim telefonima bazira se na pronalaženju i oporavljanju artefakta i tragova koji su vezani za aplikacije društvenih mreža. Aplikacije nude različite dokaze u ovisnosti o operativnom sustavu uređaja. Usporedna analiza je izvedena za aplikacije Facebook, Twitter i MySpace na tri mobilne platforme, odnosno tri operativna sustava BlackBerry OS, iOS i Android.

Tablica 4. Usporedni prikaz dokaza društvenih mreža s mobilnih uređaja različitih operativnih sustava

Aplikacija / Operativni sustav	Facebook	Twitter	MySpace
BlackBerry OS			
iOS	Korisnički podatci, podatci prijatelja uključujući detalje i profilnu sliku, fotografije, objave, prethodno prijavljeni korisnici	Korisnička imena, profilna slika, objavljeni tweetovi	Korisničko ime/lozinka, objavljeni komentari
Android	Korisnički podatci, podatci prijatelja uključujući detalje i profilnu sliku, fotografije, objave, kreirani albumi, chat poruke	Korisnička imena, profilna slika, objavljeni tweetovi	Korisničko ime/lozinka, kolačići i privremene datoteke

Izvor: [53]

Rezultati analize (tablica 4) pokazuju kako nije bilo moguće pronaći tragove aktivnosti društvenih mreža na uređaju koji koristi BlackBerry OS. Za razliku od BlackBerry-a, uređaji s iOS i Android sustavom, sadrže puno više vrijednih podataka koji mogu biti otkriveni i korišteni za forenzičku analizu. Veliku prepreku u forenzici društvenih mreža predstavljaju različiti mehanizmi zaštite uređaja i enkripcije podataka na uređaju što otežava i onemogućava pronalazak dokaza, a ujedno su to metode i antiforenzike koja je opisana u sljedećem poglavlju.

5. Digitalna antiforenzika

Digitalna antiforenzika predstavlja alate i metode kojima se otežava ili sprječava proces istrage. Proces antiforenzike obuhvaća korištenje malicioznih alata ili metoda te korištenje mehanizma zaštite poput enkripcije. Digitalna antiforenzika velika je prepreka svakom forenzičkom istražitelju i tijekom provođenja istrage potrebno je posvetiti povećanu pažnju kako bi se osigurao integritet dokaza.

5.1. Primjena digitalne antiforenzike na računala

Metode koje se koriste za provođenje antiforenzike računala mogu se podijeliti u nekoliko glavnih kategorija, [54]:

- skrivanje dokaza
- uništavanje dokaza
- uklanjanje izvora dokaza
- krivotvorenje dokaza.

Skrivanje podataka proces je kojim se otežava pronalaženje podataka pri čemu isti ostaju dostupni za kasniju upotrebu. Neki od najčešćih oblika skrivanja podataka su: enkripcija, steganografija i drugi hardversko-softverski oblici. Svaka od ovih metoda na svoj način otežava i usporava forenzičku istragu, a kombiniranjem više različitih metoda skrivanja podataka, forenzička istraga postaje skoro nemoguća.

Enkripcija, proces je u kojim se vrši izmjena podataka tako da postanu nečitljivi za osobe koje nemaju dovoljno znanja o kriptografiji. Jedna je od najčešće korištenih antiforenzičkih tehnika, a njezinom upotrebom korisnik može stvoriti virtualno kriptirani disk kojemu se može pristupiti isključivo šifrom.

Steganografija znanstvena je disciplina koja se bavi prikrivenom razmjenom informacija. Osnovni princip steganografije počiva na prikrivanju samog postojanja informacije koja se prenosi unutar nekog, naizgled bezazlenog, medija ili skupa podataka. Moderna steganografija, koja između ostaloga koristi i prednosti digitalne tehnologije, najčešće podrazumijeva skrivanje tajne poruke unutar neke multimedijske datoteke, npr. slike, audio ili video datoteke. Multimedijske datoteke u pravilu sadrže neupotrijebljene ili nevažne podatkovne prostore koje različite steganografske tehnike koriste tako da ih popune tajnim informacijama, [55].

Osim navedenih metoda moguće je korištenjem određenih alata i tehnika sakriti podatke na različitim mjestima na računalu kao što su:

- Loš sektor (engl. *Bad Sector*)
- Mrtav prostor (engl. *Slackspace*)
- Skrivene particije i mape.

Uništavanje korisničkih objekata metoda je kojom se trajno eliminiraju određeni podaci ili čitave grupe datoteka koje je korisnik kreirao u sustavu. Uništavanje se postiže upotrebom različitih metoda koje uključuju programe za čišćenje diskova, namjensko brisanje datoteka i tehnike za uništavanje diskova.

Programi za čišćenje diskova koriste različite metode za prepisivanje preko postojećih datoteka. Programi za brisanje datoteka koriste se za uklanjanje datoteka iz operativnog sistema, a prednost takvih programa je brže izvršavanje svojih zadataka pri čemu ostavljaju mnogo manje tragova nego programi za čišćenje diskova, [56].

Kako je i prethodno navedeno, forenzički postupak isključuje osnovno pretraživanje sadržaja diskova, a sve u cilju pronalaženja mogućeg dokaza o kršenju zakona ili internih pravila firme. Predmet istrage mora biti ciljano usmjeren samo na dokazivanje traženih dokaza kako bi forenzičar tragao samo za relevantnim podacima (npr. istražitelj traži dokaze o ukradenim popisima kreditnih kartica neće se baviti analizom video ili audio sadržaja na disku). Ta činjenica može se iskoristiti kako bi se zavarao trag dokumentima koji žele biti skriveni. S obzirom na to da svaki podatak u svom zaglavlju ima podatke o vrsti ekstenzije, razvijene su tehnike kojima se taj podatak u zaglavlju može promijeniti tako da se, primjerice, datoteka s ekstenzijom .doc zamijeni ekstenzijom .mp3 datoteke. Neiskusniji forenzičari takve datoteke jednostavno preskaču tijekom pretrage, [57].

Djelovanje protivi digitalnih forenzičkih alata metoda je koja podrazumijeva napade i varanja alata koji se koriste u digitalnim istragama, na način da se sakriju aktivnosti, promjene neke sistemske vrijednosti na računalu i sl. Jedan od načina korištenje je alata koji brišu sve tragove aktivnosti korisnika kako na računalu i programima, tako i na internetu. Programi kao što su Evidence eliminator, Track Eraser, Window Washer potpuno uklanjaju sve tragove aktivnosti korisnika: povijest pretraživanja, priručnu memoriju i mrtav prostor. Ovim programima onemogućuje se istražiteljima zaduženim za digitalnu istragu, pronalaženje takvih aktivnosti. Također, u praksi je čest slučaj korištenje alata za promjenu sustavskog datuma i vremena kreiranja, modificiranja, pristupa i ažuriranja datoteka na NTFS sustavu, [58].

Program “Transmogrify” omogućava korisniku mijenjanje zaglavlja datoteka, tako da je moguće zaglavlje .jpg slike staviti u .doc datoteku ili obrnuto, a sve s ciljem zavaravanja rada EnCase, FTK ili drugih forenzičkih programa.

5.2. Primjena digitalne antiforenzike na mobilne uređaje

Na tržištu je sve veći broj mobilnih uređaja što povećava količine pohranjenih informacija, posebno osobnih. Pametni mobilni uređaji upravo su iz tog razloga posebno zanimljivi forenzičkim istražiteljima. Kako bi se ometala istraga pametnog mobilnog uređaj ili u potpunosti spriječio pronalazak dokaza, moguće je koristiti neke od metoda antiforenzike.

U nastavku opisane su metode antiforenzike pametnog mobilnog uređaja baziranog na Android OS. Za potrebe usporedbe metoda antiforenzike korišteni su programski alati SecureView, Paraben i XRY forenzički alat kako bi pronašli sve popise kontakata na mobilnom uređaju.

Navedeni forenzički alati imaju slične korake prikupljanja podataka, [59]:

- kopiranje aplikacijskog paketa u /data/local/temp/ mapu
- instaliranje aplikacije
- brisanje datotečnog paketa iz privremene mape
- pokretanje aplikacije
- povrat i prijenos podataka mobitela do alata
- deinstalacija aplikacije nakon završetka vađenja podataka.

Iznenadna smrt predstavlja najjednostavniji antiforenzički pristup. Aplikacija je instalirana na mobilni uređaj i konfigurirana za automatsko pokretanje nakon svakog bootup-a kao pozadinski servis za praćenje telefonskih zapisa. Bitna funkcionalist ove metode je ta što uređaj može detektirati povezivanje s forenzičkim alatom. Kada uređaj detektira da je povezan na forenzički alat, automatski isključuje mobilni uređaj i briše sve podatke koji su skladišteni na njemu, [59].

Brisanje osjetljivih podataka je pristup koji omogućava korisniku mobilnog uređaja da unaprijed označi povjerljive kontakte u imeniku. Kada se mobilni uređaj spoji na forenzički alat, uređaj prepoznaje povezanost i automatski briše sve kontakte, osim onih koje je korisnik unaprijed označio kao povjerljive.

Zamjena svih podataka je vrlo jednostavna metoda kojom se zamjenjuju izvorni podatci u imeniku s lažnim podatcima. Aplikacije će generirati sve potrebne podatke o lažnim kontaktima i po potrebi ih zamijeniti ukoliko mobilni uređaj bude spojen na forenzički alat.

6. Zakonska regulativa

Zakon ima presudan utjecaj na računalnu forenziku jer postoje 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 mora se voditi kada se pristupa podacima osumnjičenika, virusima, elektromagnetskim i mehaničkim oštećenjima, a ponekad i računalnim zamkama, [2].

Postoji nekoliko pravila kojih se treba pridržavati kako se ne bi ugrozila pravna upotrebljivost dokaza, [2]:

- koristiti samo alate i metode koji su prethodno ispitani i ocijenjeni
- Ispitivanje alata provode institucije poput proizvođača programskih paketa vladinih organizacija 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.

Tijekom provođenja istrage u kojoj vlasnik računala ili drugog elektroničkog uređaja kojim je počinjeno kazneno djelo ne izdaje pristanak za pregled uređaja, istražitelj mora imati sve dozvole i autoritet. U suprotnom, svi dokazi koji su pronađeni i prezentirani sudu se odbacuju, a istražitelj bi mogao biti kažnjen.

6.1. Zakon o zaštiti osobnih podataka

U Republici Hrvatskoj u članku 2. Zakonu o zaštiti osobnih podataka (NN 106/2012) definirani su navedeni izrazi:

Osobni podatak je svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati (u daljnjem tekstu: ispitanik); osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet, [60].

Obrada osobnih podataka je svaka radnja ili skup radnji izvršenih na osobnim podacima, bilo automatskim sredstvima ili ne, kao što je prikupljanje, snimanje, organiziranje, spremanje, prilagodba ili izmjena, povlačenje, uvid, korištenje, otkrivanje putem prijenosa, objavljivanje ili na drugi način učinjenih dostupnim, svrstavanje ili

kombiniranje, blokiranje, brisanje ili uništavanje, te provedba logičkih, matematičkih i drugih operacija s tim podacima, [60].

Također u Članku 6. definirano je sljedeće:

- Osobni podaci moraju se obrađivati pošteno i zakonito.
- Osobni podaci mogu se prikupljati u svrhu s kojom je ispitanik upoznat, koja je izričito navedena i u skladu sa zakonom i mogu se dalje obrađivati samo u svrhu u koju su prikupljeni, odnosno u svrhu koja je podudarna sa svrhom prikupljanja. Daljnja obrada osobnih podataka u povijesne, statističke ili znanstvene svrhe neće se smatrati nepodudarnom, pod uvjetom da se poduzmu odgovarajuće zaštitne mjere.
- Osobni podaci moraju biti bitni za postizanje utvrđene svrhe i ne smiju se prikupljati u većem opsegu nego što je to nužno da bi se postigla utvrđena svrha.
- Osobni podaci moraju biti točni, potpuni i ažurni.
- Osobni podaci moraju se čuvati u obliku koji dopušta identifikaciju ispitanika ne duže no što je to potrebno za svrhu u koju se podaci prikupljaju ili dalje obrađuju. Odgovarajuće mjere zaštite za osobne podatke koji se pohranjuju na duže razdoblje za povijesnu, statističku ili znanstvenu uporabu propisuju se posebnim zakonima.

Za postupanje u skladu s odredbama ovoga članka odgovoran je voditelj zbirke osobnih podataka.

Osobni podaci smiju se prikupljati i dalje obrađivati isključivo:

- uz privolu ispitanika samo u svrhu za koju je ispitanik dao privolu, ili
- u slučajevima određenim zakonom, ili
- u svrhu izvršavanja zakonskih obveza voditelja zbirke osobnih podataka, ili
- u svrhu sklapanja i izvršenja ugovora u kojem je ispitanik stranka, ili
- u svrhu zaštite života ili tjelesnog integriteta ispitanika ili druge osobe u slučaju kada ispitanik fizički ili pravno nije u mogućnosti dati svoj pristanak, ili
- ako je obrada podataka nužna radi ispunjenja zadataka koji se izvršavaju u javnom interesu ili u izvršavanju javnih ovlasti koje ima voditelj zbirke osobnih podataka ili treća strana kojoj se podaci dostavljaju ili
- ako je obrada podataka nužna u svrhu zakonitog interesa voditelja zbirke osobnih podataka ili treće strane kojoj se podaci otkrivaju, osim kada prevladavaju interesi zaštite temeljnih prava i sloboda ispitanika iz članka 1. stavka 2. ovoga Zakona, ili
- ako je ispitanik sam objavio te podatke.

6.2. Konvencija o kibernetičkom kriminalu

Konvencija o kibernetičkom kriminalu predstavlja oblik međunarodnog ugovora, te je Republika Hrvatska prihvatila ovu konvencija u svrhu prilagodbe zakona. Vijeće Europe je dalo smjernice za borbu protiv računalnog kriminala, s posebnim naglaskom na Internet kriminal.

U drugom poglavlju po grupama definirane su mjere koje treba poduzeti na nacionalnoj razini, [61]:

- grupa djela protiv tajnosti, nepovredivosti i dostupnosti podataka (ovdje pripadaju takve povrede kao što su nezakonit pristup, nezakonito presretanje, ometanje podataka, ometanje sustava i zlouporaba naprava)
- računalna kaznena djela (računalno krivotvorenje i prijevara)
- kaznena djela vezana uz sam sadržaj podataka na računalu (distribucija i širenje dječje pornografije)
- kaznena djela povrede autorskih i srodnih prava.

Također definirane su i odredbe o:

- sankcioniranju pomaganja ili prikrivanja kaznenih dijela
- kaznena odgovornosti pravnih osoba
- sankcije i mjere.

Osim navedenog u Konvenciji je opisana hitna zaštita pohranjenih računalnih podataka, koja obvezuje stranku na to da štiti i čuva sav sadržaj podataka sve dok je to nužno, ali ne više od 90 dana.

Zemlje potpisnice Konvencije su obvezane da u svoj pravni poredak unesu i odredbe koje omogućuju pristup i pretragu podataka na računalima korisnika koji su osumnjičeni za počinjenje nekog kaznenog dijela. Također omogućena je suradnja između zemalja potpisnica vezanim uz istraživački rad, ukoliko se ukaže potreba.

6.3. Zaštita osobnih podataka

Direktiva EU-a o zaštiti podataka (također poznata kao Direktiva 95/46 / EZ) propis je koji je usvojila Europska unija radi zaštite privatnosti i zaštite svih osobnih podataka prikupljenih za ili o građanima EU, osobito kada se radi o preradi, korištenju Ili razmjeni takvih podataka. Direktiva EU o zaštiti podataka temelji se na preporukama koje je predložila Organizacija za ekonomsku suradnju i razvoj (OECD).

Ove su preporuke utemeljene na sedam načela, [62]:

1. Osobe čiji se podaci prikupljaju trebaju biti obaviješteni o prikupljanju.
2. Osobe čiji se osobni podaci prikupljaju trebaju biti obaviješteni o stranci ili strankama koje prikupljaju takve podatke.
3. Nakon prikupljanja, osobni podaci trebaju biti osigurani i sigurni od potencijalne zloupotrebe, krađe ili gubitka.
4. Osobni podaci se ne smiju otkrivati ili dijeliti s trećim stranama bez pristanka svojih subjekata.
5. Subjekti bi trebali odobriti pristup njihovim osobnim podacima i dopustiti da ispravite netočnosti.
6. Prikupljeni podaci trebaju se koristiti samo za navedene svrhe i bez ikakvih drugih namjena.
7. Subjekti bi trebali moći zadržati osobne podatke prikupljača odgovornih za pridržavanje svih sedam ovih načela.

6.4. 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 upravno 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.

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, [63].

7. Zaključak

Posljednjih nekoliko godina vidljiv je napredak u razvoju informacijsko-komunikacijske tehnologije koja uvelike olakšava život. Bez računala i mobilnih uređaja danas ne možemo zamisliti normalan život. Razvojem tehnologije uvijek se pojavljuju one loše strane, poput ekoloških aspekta i mogućnost zloupotrebe. Zbog sve većeg porasta zlouporabe računala i mobilnih uređaja, pojavila se potreba za zaštitom informacijskog-komunikacijskog sustava od neželjenih napada.

Kako često svaki napad ili zlonamjerno korištenje ostavljaju digitalni trag, pojavila se potreba za pronalaskom i analizom digitalnih dokaza. Na taj način došlo je i do nastanka digitalne forenzike, kao najmlađe grane forenzičkih znanosti.

Tijek forenzičke istrage računala sastoji se od nekoliko faza, koje se moraju slijediti i poštivati kako bi se uspjeli pronaći valjani dokazi. Valjane digitalne dokaze potrebno je pažljivo analizirati te kasnije prezentirati na sudu. Jedan od većih problema tijekom analize uređaja predstavlja stalna evolucija tehnologije, stoga forenzički stručnjaci stalno moraju pratiti razvoj tehnologije te ići u korak s njom.

Forenzička analiza računala nije toliko kompleksna kao analiza mobilnih uređaja, ponajviše zbog sporijeg tehnološkog razvoja i male razine hlapljivosti podataka. Veliki problem stvaraju mobilni uređaji zbog različitih faktora kao što su: vrsta OS, proizvođač, starost i stanje uređaja, te naravno primjenjivost ispravnog alata. Potrebno je koristiti ispravan alat koji će dati najbolje rezultate, jer svaki forenzički alat je drugačiji, a ukoliko usporedimo podatke iz tablice 1 i 2 možemo vidjeti bitne razlike forenzičkih alata. Nadalje, veliki problem stvara proces certifikacije forenzičkih stručnjaka za određeni alat, što zahtjeva mnogo novčanih sredstava. Stoga kako bi netko bio dobar istražitelj mora poznavati alat i ovlašteno obavljati forenzičku istragu jer svaki krivi korak može dovesti do gubitka dragocjenih podataka, a samim time naštetiti u daljnjoj istrazi.

Primjena antiforenzičke metode na računalu može poslužiti kao odličan alat za prikrivanje dokaza, njihovo brisanje i skrivanje. Upotrebom samo jednog alata, mogu se izbrisati svi tragovi aktivnosti i time forenzičarima uništiti dragocjene dokaze. Većina mobilnih uređaja koji koriste neku od metoda antiforenzičke zaštite imaju posebne mehanizme koji uočavaju povezanost mobilnog uređaja s forenzičkim alatom i automatski izvršavaju različite radnje kako bi spriječile čitanje povjerljivih podataka, a najčešće je to uništavanje podataka ili generiranje lažnih podataka.

U Republici Hrvatskoj, digitalna forenzika nije toliko zastupljena i opće poznata, ali zbog porasta računalnog kriminala očekuje se da će u budućnosti digitalna forenzika imati sve veću primjenu, ali i da će postati jedan od glavnih sredstava u borbi protiv kriminala i terorizma.

Literatura

[1] Milosavljević M, Grubor G. Digitalna forenzika računarskog sistema. Beograd: Univerzitet Singidunum; 2009.

[2] Hrvatska akademska i istraživačka mreža, CERT. Računalna forenzika, Zagreb, 2010.

[3] Procesor. Preuzeto sa: http://whatis.techtarget.com/definition/processor [Pristupljeno: srpanj 2017.].

[4] What is BIOS and How to Update the BIOS on Your Dell System. Preuzeto sa: http://www.dell.com/support/article/hr/en/hrbsdt1/sln284433/what-is-bios-and-how-to-update-the-bios-on-your-dell-system?lang=en [Pristupljeno: srpanj 2017.]

[5] Hrvatska akademska i istraživačka mreža. Osnove računalne forenzičke analize, Zagreb, 2006.

[6] Casey, E. Digital Evidence and Computer Crime. Forensic Science; 2011.

[7] Building a Low Cost Forensics Workstation. Preuzeto sa: https://www.sans.org/reading-room/whitepapers/incident/building-cost-forensics-workstation-895 [Pristupljeno: srpanj 2017.].

[8] Abdalla S, Hazem S, Hashem S. Guideline Model for Digital Forensic Investigation. Annual ADFSL Conference on Digital Forensics, Security and Law, 2. 2007.

[9] Forenzička radna stanica TALINO KA-Nano. Preuzeto sa: https://www.insig2.eu/forenzicka-radna-stanica-talino-forensic-workstation-31?lang=hr [Pristupljeno: srpanj 2018.].

[10] Digital Forensics Certificate Program Begins Winter Quarter. Preuzeto sa: http://lowercolumbiacollege.blogspot.com/2012/11/digital-forensics-certificate-program.html [Pristupljeno: kolovoz 2018.].

[11] The Anatomy of a Digital Investigation. Preuzeto sa: http://www.informit.com/articles/article.aspx?p=2129764&seqNum=4 [Pristupljeno: kolovoz 2017.].

[12] Chain of Custody: How to Ensure Digital Evidence Stand Up In Court. Preuzeto sa: https://www.govtechworks.com/chain-of-custody-how-to-ensure-digital-evidence-stands-up-in-court/#gs.g9K2Tdk [Pristupljeno: kolovoz 2017.].

[13] The bag and tag. Preuzeto sa: http://forensicir.blogspot.com/2008/01/bag-and-tag.html [Pristupljeno: kolovoz 2018.].

[14] Kornblum J. Preservation of Fragile Digital Evidence by First Responders; 2002.

[15] Forenzička mobilna jedinica za stvaranje forenzičkih slika tvrdog diska. Preuzeto sa: https://www.media-clone.net/SuperImager-Rugged-12-LCD-SAS-SATA-USB-3-0-p/sir-0024-00b.htm [Pristupljeno: kolovoz 2018.].

[16] National Computer Forensics Institute. Network Intrusion Responder Program 2(2). Preuzeto sa: https://info.publicintelligence.net/NITROstudentV2.pdf [Pristupljeno: kolovoz 2017.].

[17] Ashcroft, J, Daniels, D. J, Hart S. V.: Forensic Examination of Digital Evidence:A Guide for Law Enforcement, Washington: U.S. Department of Justice, Office of Justice Programs, 2004

[18] Det. Muprhy C.A. Developing Process for Mobile Device Forensics. Madion PD-Computer Forensics, 2013.

[19] Forenzika mobilnih uređaja. Preuzeto sa: http://www.cis.hr/WikiIS/doku.php?id=mobile_forenzika [Pristupljeno: srpanj 2017.].

[20] EDEC Faraday Bag. Preuzeto: https://www.edecdf.com/product/black-hole-faraday-bag-standard-non-window/ [Pristupljeno: srpanj 2017.].

[21] Reiber L. Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation, SAD, 2015

[22]] The Need for A Faraday Bag. Preuzeto sa: https://www.forensicmag.com/article/2014/02/need-faraday-bag [Pristupljeno: srpanj 2017.].

[23] Phone jammer. Preuzeto sa: http://abcnews.go.com/blogs/technology/2012/03/ agitated-man-uses- cell-phone-jammer-to-block-chatter-on-bus/ [Pristupljeno: kolovoz 2017.].

[24] Signal isolation. Preuzeto sa: https://mobileforensics.files.wordpress.com/2007/03/rf-isolation.pdf [Pristupljeno: srpanj 2017.].

[25] Usporedba brzine ekstrakcije i količine dobivenih podataka. Preuzeto sa: https://www.packtpub.com/sites/default/files/ArticleImages/8311OS_01_03.png [Pristupljeno: srpanj 2017.].

[26] Uvod u digitalnu forenziku. Preuzeto sa: https://www.packtpub.com/books/content/introduction-mobile- forensics [Pristupljeno: kolovoz 2017.].

[27] Introduction: Importance of Mobile Forensics. Preuzeto sa: https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/#gref [Pristupljeno: kolovoz 2018.].

[28] Physical Analyzer Use Advanced Decoding Techniques. Preuzeto sa: https://www.youtube.com/watch?v=DOnSDhI19rU [Pristupljeno: kolovoz 2018.].

[29] Hex Dumping Flash From A Mobile. Preuzeto sa: https://digital-forensics.sans.org/blog/2008/09/03/hex-dumping-flash-from-a-mobile [Pristupljeno: kolovoz 2017.].

[30] Mobile Phone Forensic Chip Off Process. Preuzeto sa: https://pressdispensary.co.uk/image_library/q991448.html [Pristupljeno: kolovoz 2017.].

[31] Chip-Off Forensics. Preuzeto sa: http://www.binaryintel.com/services/jtag-chip-off-forensics/chip-off_forensics/ [Pristupljeno: kolovoz 2017.].

[32] Mahalik H, Bommisetty S, Tamma R: Practical Mobile Forensics, 2016.

[33] JTAG Forensics .Preuzeto sa: https://www.gillware.com/forensics/jtag-chip-off-forensics/jtag-forensics-services [Pristupljeno: kolovoz 2017.].

[34] JTAG Pin Finder. Preuzeto sa: http://www.100randomtasks.com/jtag-pin-finder [Pristupljeno: kolovoz 2017.].

[35] Gary J. Are Mobile Device Examinations Practiced like 'Forensics'?, SAD, 2015.

[36] Infosec institute. 22 Popular Computer Forensics Tools. Preuzeto sa: https://resources.infosecinstitute.com/computer-forensics-tools/#gref [Pristupljeno: kolovoz 2018.].

[37] Silicon Forensics, Prodiscover Forensics. Preuzeto sa: https://siliconforensics.com/products/software/prodiscover-forensics.html [Pristupljeno: kolovoz 2017.].

[38] PassMark Software, Feature comparison. Preuzeto sa: https://www.osforensics.com/compare.html [Pristupljeno: kolovoz 2017.].

[39] AccessData FTK. Preuzeto sa: http://accessdata.com/products-services/forensic-toolkit-ftk [Pristupljeno: kolovoz 2017.].

[40] Nelson B,Phillips A, Steaurty C:Guide to computer forensics and investigiations, SAD, 2014.

[41] Using FTK. Preuzeto sa: https://samsclass.info/121/proj/p15-FTK1.htm [Pristupljeno: srpanj 2018.].

[42] EnCase Forensic v7.09.02 product information. Preuzeto sa: https://www.scmagazine.com/encase-forensic-v70902/review/6892/ [Pristupljeno: kolovoz 2017.].

[43] Mobile Forensic Tools Comparison Chart. Paraben Corporation. Preuzeto sa: http://herrymorison.tistory.com/ [Pristupljeno: srpanj 2018.].

[44] UFED Logical Analayzer. User Manual, 2014. Preuzeto sa: http://www.mcsira.com/WEB/8888/NSF/Web/3128/UFED%20Logical%20Analyzer2014.pdf [Pristupljeno: srpanj 2018.].

[45] Doherty E. Digital Forensics for Handheld Devices; 2012.

[46] Oxygen Forensic Suite. Preuzeto sa: https://www.giga.de/downloads/oxygen-forensic-suite-2013/ [Pristupljeno: srpanj 2018.].

[47] MOBILedit Forensic Express. Preuzeto sa: http://www.mobiledit.com/forensic-solutions [Pristupljeno: srpanj 2017.].

[48] XRY Logical. Preuzeto sa: https://www.msab.com/products/xry/xry-logical/ [Pristupljeno: srpanj 2018.].

[49] Cellebrite UFED. Preuzeto sa: http://ec2-107-23-31-70.compute-1.amazonaws.com/mobile-forensics [Pristupljeno: srpanj 2018.].

[50] Mahant SH, Meshram BB. NTFS Deleted Files Recovery: Forensics View. Departmnet of Computer Engineering Veermata Jijabai Technological Institute, Mumbai, India; 2012.

[51] A Review of Computer forensic & Logging System. Preuzeto sa: https://www.ijarcsse.com/docs/papers/january2012/V2I1023.pdf [Pristupljeno: kolovoz 2017.].

[52] Registry Forensics. Preuzeto sa: www.cse.scu.edu/~tschwarz/COEN252_09/PPtPre/Registry.ppt [Pristupljeno: srpanj 2017.].

[53] Mutawa N, Baggili I, Marrington A. Forensic Analysis of Social Networking Applications on Mobile Devices. University of New Haven, 2012.

[54] Harris R. Arriving at an Anti-forensics Consensus: Examining How to Define adn Control the Anti-forensics Problem. DFRWS, SAD, 2016.

[55] Steganografija. Preuzeto sa: http://www.cert.hr/node/17277 [Pristupljeno: srpanj 2017.].

[56] Milanović Z, Milanović T: Digitalna anti-forenzika kao kriminogeno sredstvo zaštite kiber kriminala. Naučno stručno savetovanje Ziteh, Beograd, 2010.

[57] Digitalne antiforenzičke tehnike. Preuzeto sa: http://slobabgd.webs.com/Tutorijali/Digitalne%20antiforenzicke%20tehnike.htm [Pristupljeno: srpanj 2017.].

[58] Ćosić J, Ćosić Z: Digitalna antiforenzika–manipulacija procesom digitalne istrage, 18. Telekomunikacioni forum TELFOR 2010, Srbija, 2010.

[59] Azdegan S, Yu W, Liu H, Sistani M, Acharya. Novel Anti-forensics Approaches for Smart Phones. Towson University; 2012.

[60] Zakon o zaštiti osobnih podataka, Narodne Novine, br. 106/12.

[61] Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu, Narodne novine, br.9/02.

[62] EU Data Protection Directive (Directive 95/46/EC). Preuzeto sa: http://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC [Pristupljeno: kolovoz 2017.].

[63] Kokot I: Kaznenopravna zaštita računalnih sustava, programa i podataka, Pregledni znanstveni rad, Zagreb, 2004.

Popis slika

Popis tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.
Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.
Izjavljujem također, kako 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 rada pod naslovom **Usporedni prikaz forenzičke analize računala i mobilnih uređaja**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 2.9.2018

Student/ica:
Petar Majić
(potpis)