Računalna forenzika: alati i metode

Baričević, Ana

Undergraduate thesis / Završni rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Pula / Sveučilište Jurja Dobrile u Puli**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:137:147914

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

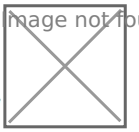
Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Digital Repository Juraj Dobrila University of Pula





Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

ANA BARIČEVIĆ

RAČUNALNA FORENZIKA: ALATI I METODE

Završni rad

Pula, kolovoz 2020.

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

ANA BARIČEVIĆ

RAČUNALNA FORENZIKA: ALATI I METODE

Završni rad

JMBAG: 0303061650, redovni student
Studijski smjer: Informatika

Predmet: Informatička tehnologija i društvo
Znanstveno područje: Društvene znanosti
Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i informatologija
Mentor: prof. dr. sc. Mario Radovan

Pula, kolovoz 2020.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Ana Baričević kandidat za prvostupnika informatike ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

Ana Baričević

U Puli, kolovoz, 2020. godine

IZJAVA

o korištenju autorskog djela

Ja, Ana Baričević dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom „Računalna forenzika: alati i metode“ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, kolovoz, 2020. godine

Potpis

Ana Baričević

Sažetak

U ovom radu pobliže ću objasniti što je računalna forenzika i koji su to alati i metode koji se koriste za njenu primjenu. U današnje vrijeme kada se tehnologija sve više razvija, računalni forenzičari moraju biti u korak sa novim tehnologijama i načinima rješavanja određenih vrsta kriminala. Iako se računala koriste već pola stoljeća, tek sa pojavom osobnih računala povećala se stopa računalnog kriminala. Kako digitalna tehnologija napreduje, tako i raste broj zloupotreba osobnih podataka, računala, mobitela, računalnih mreža i sl. Računalnu forenziku čine sve metode i alati za identifikaciju, prikupljanje, očuvanje, pretraživanje, analizu i prezentaciju dokaza koji su ključni za istragu. Ovisi o kakvoj se istrazi radi, forenzičari će se fokusirati na određeni dio informacijskog sustava. Dokazi koje je potrebno pronaći, ne mogu se pronaći uz pomoć standardnih alata operacijskog sustava, nego uz pomoć specijaliziranih forenzičkih alata. Dokazi se mogu pronaći u datotekama, e-pošti, bazama podataka, SMS porukama, pozivima, privremenim datotekama, kolačićima, sistemskim zapisima i sl. Uz temeljna znanja forenzičkih metoda, stručnjaci moraju neprekidno obnavljati svoje znanje i računalne vještine kako bi uvijek bili jedan korak ispred počinitelja.

Ključne riječi: računalna, forenzika, alati, metode, tehnologija, napredak

Summary

In this paper, I will explain more closely what are the tools and methods which computer forensics use. Nowdays as technonlogy evolves more and more, computer forensics need to keep up with new technologies and ways to tackle certain types of crime. Although, computers have been used for half a century, only with the appearance of personal computers the rate of computer crime increased. As digital technology progresses, so does the number of misuses of personal data, computers, mobile phones, computer networks, etc. Computer forensics consists of all methods and tools for identifying, collecting, preserving, searching, analysing and presenting evidence that are essential for the investigation. Depending on what kind of investigation it is, forensics will focus on particular part of the information system. The evidence cannot be found with the help of standard operating system tools, but with the help of specialised forensic tools. Evidence can be found in files, emails, databases, sms messages, calls, temporary files, cookies, system records etc. With basic knowledge of forensic methods, experts must continuously renew their knowledge and computer skills in order to always be one step ahead of the offender.

Keywords: computer, forensics, tools, methods, technology, progress

Sadržaj

1. UVOD 1
2. ŠTO JE RAČUNALNA FORENZIKA? 2
2.1. Proces računalne forenzike 3
3. GRANE RAČUNALNE FORENZIKE 5
3.1. E-mail i web forenzika 5
3.1.1. Praćenje rute e-mail paketa 6
3.1.2. E-mail struktura 6
3.1.3. Forenzička perspektiva e-maila 7
3.1.4. Istraživanje web orijentiranog sustava e-pošte 10
3.1.5. Pretraživanje datoteka preglednika 12
3.1.6. Privremene datoteke 12
3.2. Forenzika podataka 14
3.2.1. Pronalaženje skrivenih podataka 15
3.2.2. Izbrisane datoteke 15
3.2.3. Dohvaćanje izbrisanih datoteka 16
3.2.4. Dohvaćanje spremljenih datoteka 17
3.2.5. Nedostupan prostor 17
3.3. Forenzika dokumenata 18
3.3.1. Pregled metapodataka 18
3.3.2. Izdvajanje metapodataka 20
3.3.3. „Namamljivanje“ dokumenata iz lokalne pohrane 20
3.3.4. Podudaranja zaglavlja datoteka sa ekstenzijama 21
3.3.5. Izmjena zaglavlja datoteke 22
3.3.6. Pronalaženje veza i vanjske pohrane 23
3.3.7. Sigurnosne kopije 23
3.4. Forenzika mobilnih uređaja 24
3.4.1. Razmatranje mobilnih uređaja „forenzički“ 25
3.4.2. Oduzimanje mobilnog uređaja 27
3.4.3. Mobilni uređaji i SIM kartice 27
3.4.4. Mobilna mreža uređaja 28
3.4.5. Karakteristike mobilnog uređaja 29
3.4.6. Oprema za mobilnu forenziku 29
3.5. Mrežna forenzika 30

4. FORENZIČKI ALATI 32
4.1. Forenzički softverski alati 32
4.2. Forenzički hardverski alati 34
5. RAČUNALNI FORENZIČKI LABORATORIJ 35
5.1. Računalno forenzički poslužitelj podataka 36
5.2. Forenzički blokatori pisanja 36
5.3. Oprema za brisanje medija 36
5.4. Oprema za snimanje 36
6. RAČUNALNA FORENZIKA I ZAKONI 37
7. ZAKLJUČAK 38
8. LITERATURA 39
9. PRILOZI 40

1. UVOD

U današnje vrijeme, većina svjetske populacije ovisi o računalnoj i mobilnoj tehnologiji. Međutim, tehnološki napredak rezultirao je raznim modernim oblicima kriminala. Računalni kriminal ili cyber kriminal su dramatično promijenili moderno društvo. Iako je to teško shvatiti, prije dva desetljeća većina pojedinaca nije posjedovala niti mobitel niti osobno računalo jer su to bili nešto skuplji komadi opreme. Pojedinci nisu znali pisati ni tekst, a e-pošta je bila neuobičajena. Internetska povezanost je bila omogućena samo putem dial-up modema ili Ethernet kabela i ljudi su pristup internetu plaćali po satu. Sustavi videoigara koristili su 16-bitnu grafiku i nisu se povezivali s drugim uređajima. Sustavi za globalno pozicioniranje (GPS) su se u velikoj mjeri koristili samo u vojsci. Danas, pojedinci imaju svoja prijenosna računala koja su povezana putem wifi-ja i mobilnih uređaja koji se također mogu povezati s internetom. Ljudi mogu imati više računa e-pošte za osobnu i poslovnu upotrebu, kao i profile na društvenim mrežama na više različitih platformi. Mobiteli su postali poželjna metoda komunikacije, posebno tekstualne poruke. Činjenica je da mlađe generacije više preferiraju slanje poruka nego obavljanje telefonskih poziva i isto tako kupnju dobara putem interneta te sve više korištenje e-čitača za knjige i novine nego tradicionalnih pisanih medija. Napredak moderne tehnologije doveo je do povećanja cyber kriminala i digitalni napadi su povećani diljem svijeta.

2. ŠTO JE RAČUNALNA FORENZIKA?

Računalna forenzika je znanost o prikupljanju, dohvaćanju, čuvanju i prezentiranju podataka koji su elektronički obrađeni i pohranjeni na računalnim medijima. Računalna forenzika je relativno nova disciplina koja može uvelike utjecati na određene vrste istraga. Kako sve veći broj ljudi koristi računala, na njima se pohranjuje sve više informacija različitih vrsta. To uključuje informacije koje su značajne za klijente, organizacije ili koje imaju veze sa građanskim ili kaznenim slučajem, poput dokaza o financijskoj prevari, pronevjeri, nezakonitom prekidu radnog odnosa, krađi i sl.

Računalna forenzika se razlikuje od tradicionalnih forenzičkih disciplina. Za početak, potrebni alati i tehnike lako su dostupni svima koji žele računalno provesti forenzičku istragu. Za razliku od tradicionalne forenzičke analize, obično se javlja zahtjev da se računalni pregledi obavljaju na bilo kojem fizičkom mjestu, a ne samo u kontroliranom okruženju. Umjesto da donosi zaključke koji zahtijevaju stručno tumačenje, računalna forenzika proizvodi izravne informacije i podatke koji mogu igrati značaju ulogu u tom području uhićenja ili osude cyber kriminalca.

Prikupljanje digitalnih dokaza počinje onda kada se prikupljaju podaci i/ili fizički predmeti ili se pohranjuju za kasniji pregled. Izraz „dokazi“ podrazumijeva da sudovi prikupljaju dokaze i da se postupak prikupljanja također smatra pravnim. Objekt s podacima ili fizička stavka postaju dokaz samo ako službenik za provođenje zakona to smatra ili tako odredi. U nastavku ću navesti nekoliko važnih definicija američkog Federalnog istražnog ureda (*U.S. Federal Bureau of Investigation*) koje se koriste za razgraničenje određenih aspekata računalne forenzike:

- ✓ Objekti podataka (eng. *Data objects*) – objekti ili informacije potencijalne dokazne vrijednosti koji su povezani s fizičkim predmetima. Objekti podataka se mogu pojaviti u različitim formatima datoteka (npr. NTFS ili FAT32) bez promjene izvornih podataka.
- ✓ Digitalni dokazi (eng. *Digital evidence*) – podaci dokazne vrijednosti koji se pohranjuju ili prenose u digitalnom obliku.
- ✓ Fizički predmeti (eng. *Physical items*) – stavke u koje se mogu pohraniti podaci ili preko kojih se prenose objekti podataka.
- ✓ Izvorni digitalni dokazi (eng. *Original digital evidence*) – fizičke stavke i podatkovni objekti povezani s takvim stavkama u trenutku stjecanja ili oduzimanja.

- ✓ Duplikat digitalnih dokaza (eng. *Duplicate digital evidence*) – točna digitalna reprodukcija svih sadržani objekata na originalnom fizičkom predmetu.

Ne postoji istraga koja uključuje reviziju dokumenata bez uključivanja računalnih dokaza. Računalna forenzika osigurava očuvanje i provjeru autentičnosti računalnih podataka, koji su krhki i mogu se lako mijenjati, brisati ili podvrgavati neovlaštenim postupcima ako se njima pravilno ne koristi. Uz to, računalna forenzika olakšava oporavak i analizu izbrisanih datoteka i ostalih oblika uvjerljivih informacija koje su korisniku obično nevidljive.

Za razliku od papirnatih dokaza, računalni dokazi često postoje u digitalnim podacima pohranjenim na računalnim medijima za pohranu. Količina podataka koja se može pohraniti na trenutna računala nevjerojatno je ogromna. Postoje brojne vrste medija za pohranu: diskete, tvrdi diskovi, ZIP diskovi, magnetske vrpce, magnetno-optičke patrone, CD-R, CD-RW, CD-ROM, DVD, kao i flash, pametni uređaji za pohranu i memory stick kartice.

Opseg računalne forenzike nije limitiran samo na istraživanje kriminala. Izuzev toga, računalna forenzika se može koristiti za:

- Povrat podataka (eng. *Data recovery*)
- Nadzor dnevnika (eng. *Log monitoring*)
- Prikupljanje podataka sa oštećenih uređaja (eng. *Data acqusition*)
- Ispunjavanje potreba kompenzacije

2.1. Proces računalne forenzike

Proces računalne forenzike može biti podijeljen u 4 dijela:

1. prikupljanje informacija, podataka, dokaza
2. pretraživanje podataka
3. analiza usmjerena na davanje odgovora na izravni nalog za vještačenje
4. prezentacija dobivenih rezultata analize

Prikupljanje podataka izvodi se dolaskom na mjesto zločina (pod nadzorom suca zaduženog za osiguranje dokaza) i podaci se dokumentiraju uz pomoć zapisnika, fotografija i videozapisa, snimanjem zvuka. Upoznaje se sa dokaznim materijalom: stanje računala (prije isključenja, isključeno, nakon uključenja), operacijski sustav i instalirani softver, hardver.

Dokumentiranje se izvršava pisanjem natuknica i fotografiranjem zatečenog stanja te snimanjem razgovora diktafonom ili sličnim uređajima. Potrebno je utvrditi da li je računalo uključeno i obavezno ga ostaviti u tom stanju sve dok se ne utvrdi da gašenje računala neće stvoriti štetu, tj. da neće doći do gubljenja bitnih informacija. Potrebno je uočiti na kojem operacijskom sustavu računalo radi i koji hardver ima. Sljedeći korak je izrada kopije diska koja se naziva forenzička kopija diska. Forenzička kopija nije obična logička kopija jer ne sadrži samo one podatke koji su vidljivi na disku, nego i podatke koji su prethodno bili „trajno“ izbrisani.

Nakon prikupljanja osnovnih informacija o predmetu istrage, slijedi pretraživanje podataka. Disk se priključuje na testno računalo i započinje se pretraga. Najprije je potrebno eliminirati one datoteke za koje se zna da nisu potencijalni dokazi. Izdvajanje podataka se započinje sa *hash* analizom. Zatim se provjerava potpis datoteke uobičajeno uz pomoć *hex* editora. Svaka datoteka ima svoj potpis koji govori u kojemu je softverskom alatu datoteka nastala. Pretraga se nastavlja prema ključnoj riječi. Stvara se *.txt* datoteka i u nju se unose ključne riječi. Nakon izdvajanja svih datoteka koje su bile dostupne, kreću se pregledavati svi izbrisani podaci i swap (zamjenske) datoteke[1]. Zamjenska datoteka je koristan izvor informacija jer može sadržavati čak i izbrisane podatke. Mjesto na kojem možemo tražiti dokaze je „kanta za smeće“ (eng. *Recycle Bin*). Podaci koji se brišu sa računala, najprije završavaju u kanti za smeće. Podaci se mogu rekonstruirati jer se datoteke s diska ne brišu u potpunosti.

Analiza je proces tumačenja dokaza koji su prikupljeni tijekom procesa pretraživanja podataka. Postoje 3 vrte analize: vremenska analiza, analiza skrivenih podataka i analiza datoteka i aplikacija.

Vremenska analiza govori kada se neki događaj dogodio. Moguće ju je provesti na način da se pregledavaju vremenski metapodaci i datoteke zapisa. Analiza skrivenih podataka korisna je u rekonstrukciji skrivenih podataka. Ukoliko se pretraživanjem pronađu podaci koji imaju izmijenjenu ekstenziju, može se pomislit na skrivanje podataka. Analizom datoteka i aplikacija

[1] **Zamjenska datoteka** (eng. *swap file*) je binarna datoteka koja predstavlja virtualnu memoriju u koju se prosljeđuje sadržaj radne memorije koji se najdalje u prošlosti nije koristio, te iz koje se sadržaj po potrebi ponovno vraća u radnu memoriju.

dolazi se do zaključka o sposobnosti sustava i vještini korisnika. Potrebno je pregledati sadržaj datoteka, aplikacija, identificirati serijski broj i vrstu operacijskog sustava, te pregledati korisničke postavke.

Kod prezentacije podataka, rezultati istrage se prezentiraju onim osobama koje su zatražile pretragu. U sudskom procesu, forenzički stručnjak postaje svjedok. Forenzički stručnjak na jednostavan način mora obrazložiti rezultate istrage. Izvješće obuhvaća prikupljenu dokumentaciju, utvrđene dokaze i rezultate provedene analize u jednu cjelinu. Izvješće treba sadržavati datum i vrijeme analize, detaljno opisane rezultate i mora biti napisano na jednostavan način.

3. GRANE RAČUNALNE FORENZIKE

3.1. E-mail i web forenzika

E-pošta ima glavnu ili pomoćnu ulogu u većini kaznenih istraga. Većina državnih zakona omogućuje pregled e-pošte u svakom slučaju. Ne treba očekivati da će svaka istraga biti uspješna jer provjeru identiteta pošiljatelja nije uvijek lako napraviti. E-pošta i internetska pošta (web pošta) mogu se daleko proširiti.

Ray Tomlinson poslao je prvu mrežnu e-mail poruku 1971. godine. Kada se njegov izum udružio s novo izumljenim računalnom deset godina kasnije, e-pošta je postala široko rasprostranjena. Preoblikovana su područja poslovanja, prava, zabave, odnosa te osobnog i kriminalnog ponašanja. Za organizacije i ljude, e-pošta je postala Pandorina kutija koja je, kad se otvorila, stvorila nekontrolirani izvor tuge i vrijednih e-dokaza.

Izjava o privatnosti Google-ova Gmail-a na http://gmail.google.com/mail/help/privacy.html. Navodi da izbrisane poruke e -pošte mogu stalno ostati u njihovim izvanmrežnim sigurnosnim sustavima. Dakle, postoji mogućnost da sigurnosne kopije poruka nikada ne budu izbrisane.

3.1.1. Praćenje rute e-mail paketa

Svaka e-poruka šalje se kao niz paketa veličine bajta. U mrežama koje prenose ove pakete, svaki paket ima sljedeće elemente:

- ✓ Izvorna adresa: IP adresu računala koje je pošiljatelj, osim ako IP adresa nije sakrivena.
- ✓ Odredišna adresa: IP adresa računala koje je primatelj.
- ✓ Korisni teret: podatak ili poruka.

3.1.2. E-mail struktura

E-pošta funkcionira kao i poštanski ured. Središnji poštanski ured odgovara poslužitelju e-pošte, a računala povezana s njim su klijenti. Dvije vrste sustava e-pošte su klijent-poslužitelj i web orijentiran sustav e-pošte. Sustavi e-pošte također se mogu razlikovat i prema upotrebi pa mogu biti poslovni i osobni. Sustavi kao što su Gmail, Yahoo!, Outlook i slični koriste se za osobnu e-poštu, a većina tvrtki ima vlastiti interni sustav e-pošte koji koriste server klijent-poslužitelj. Klijent je računalo koje prima ili šalje e-poštu. To je na primjer kao kućni poštanski sandučić. Poslužitelj je računalo koje pohranjuje e-poštu koju prima dok je odredišni klijent ne preuzme. Poslužitelj bi bio kao lokalni poštanski ured gdje se pošta šalje i prima.

Struktura adrese e-pošte sastoji se od dva dijela, odijeljena poznatim simbolom @. Prvi dio je spremnik. To je dio s lijeve strane, koji se često naziva i korisničko ime. Drugi dio je domena. Dio s desne strane, naziv poslužitelja domene.

Prema ovoj strukturi poslužitelji e-pošte mogu brzo pronaći odredište e-pošte pretražujući IP adresu domene na poslužitelju koja se naziva DNS. DNS prevodi imena domena u IP adrese. Internet promet ovisi o funkcioniranju skrivenih DNS-ova.

Svaka poruke e-pošte putuje od izvora do odredišta istom putanjom. Sustavi e-pošte imaju jedinstveni jezik kada komuniciraju, a on se sastoji od sljedećih protokola:

- ✓ SMTP (eng. *Simple Mail Transfer Protocol*) – dostavlja poruke na predviđene poslužitelje e-pošte.
- ✓ POP (eng. *Post Office Protocol*) – jezik koji sustav e-pošte koristi za dohvaćanje poruka sa poslužitelja. Taj se protokol upućuje kao POP3. POP dohvaća poruke sa poslužitelja, briše izvorne poruke i preuzima kopije na odredišno računalo.

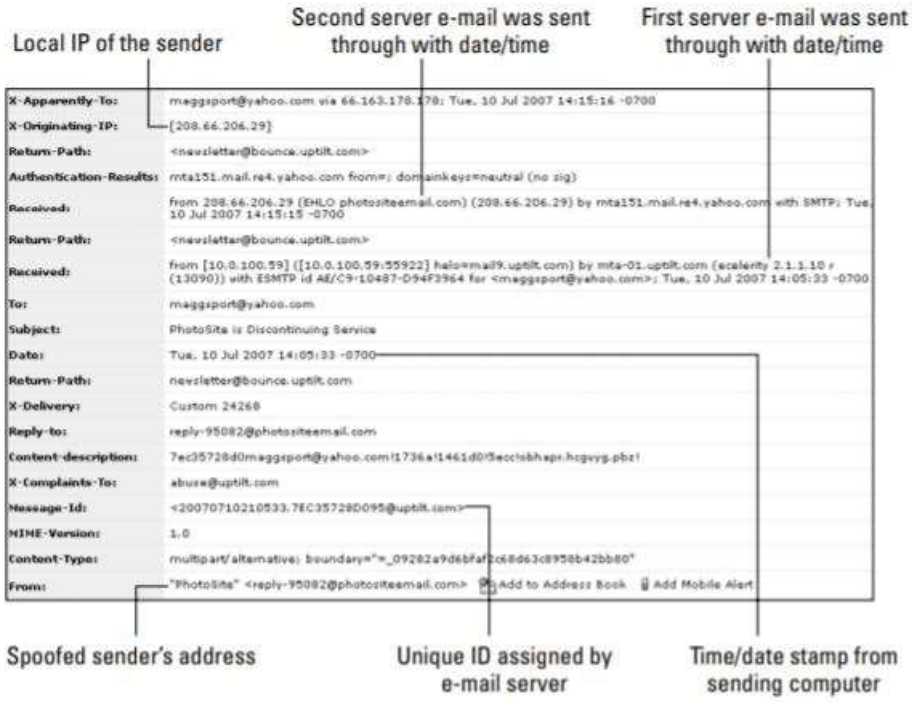
- ✓ IMAP (eng. *Internet Message Access Protocol*) – dizajniran je za obradu više korisnika na istom računu e-pošte.
- ✓ MAPI (eng. *Messaging Application Programming Interface*) – vlasnički protokol koji je koristio Microsoft za pokretanje Microsoft Outlook-a. MAPI šalje i prima e-mailove kao jedinstveni protokol, umjesto korištenja dva odvojena protokola poput SMTP i POP. Osim rukovanja e-mail komunikacijom, MAPI upravlja i organizacijskom strukturom klijentskog sustava, poput ulaznih mapa i mapa za pohranu.

3.1.3. Forenzička perspektiva e-maila

S forenzičkog stajališta, sustavi e-pošte klijent-poslužitelj najbolji su za pronalaženje informacija jer se poruke preuzimaju na tvrdi disk korisnika ili lokalno računalo. Budući da već postoji spreman pristup računalu, istraga je lakša. Obično postoji pristup poslužitelju s kojeg možete pristupiti porukama e-pošte i zapisima aktivnosti e-pošte. Prvi korak pronalaska dokaza u računalu bi trebalo biti pregledavanje sigurnosnih kopija sustava e-pošte i ako sve drugo ne uspije, tada se skida e-pošta reproducira uživo.

Poruke e-pošte se sastoje od dva dijela. Zaglavlje kao i vanjska strana koverte, sadrži adresu izvora i odredišta. Informacije sa zaglavlja se koriste za praćenje e-mail nazad do njegova izvora ili pošiljatelja. Tijelo sadrži stvarnu poruku i često sadrži informacije koje odvjetnici vole vidjeti. Kada se proučava poruka e-pošte vidjet će se samo ova dva dijela, ali ne i paketi koji su korišteni za dostavu poruke. Svi koji žele vidjeti pakete e-pošte, mogu to učiniti uz pomoć *„sniffer“* softverskog alata.

Većina klijenata za e-poštu prikazuje samo redovne podatke o zaglavlju. Postoje 4 osnovna polja informacija u zaglavlju. Adresa pošiljatelja može biti krivotvorena i prikazana kao da je druga osoba poslala mail, dok je zapravo skrivena IP adresa stvarnog pošiljatelja. Adresa primatelja koja također može biti krivotvorena. Predmet poruke, koji je ponekad prazan ili sadrži pogrešne informacije. Datum koji je uzet sa računala koje je pošiljatelj može biti pogrešno postavljen. Očito je da se ne može vjerovati informacijama zaglavlja. Možda se neće moći provjeriti stvarne informacije. Da bi se podaci potvrdili, zaglavlje se mora proširiti. Na slici 1. prikazane su informacije koje se mogu prikupiti iz zaglavlja e-pošte.



Slika 1: Informacije u proširenom zaglavlju

Informacije koje najviše pomažu je izvorna IP adresa ili domena. Ta adresa se može koristiti za pokušaj pronalaska osobe koja je poslala e-mail osim ako ona nije lažna. Jedinstveni ID poruci dodjeljuje prvi poslužitelj e-pošte kroz koji e-pošta prolazi. Uz pomoć ID-a, mogu se pronaći otisci na poslužiteljima e-pošte. Ako se zapisi poslužitelja e-pošte mogu uhvatiti prije prijepisa, doslovno se može pratiti pravi datum i vrijeme e-pošte dok prolazi kroz mrežu.

Pored provjere zaglavlja i tijela poruka e-pošte potrebno je provjeriti i druge potencijalne izvore informacija: priloge (kao što su .doc ili .xls datoteke ili slike), cc kopije, osobe kojima je poruka proslijeđena i izvorne poruke ili niz poruka na koje e-pošta odgovorila.

Većina sustava e-pošte koristi SMTP, POP ili IMAP. Upotreba ovih protokola prijenos e-pošte čini prilično standardnim. Izazov istražitelja je izdvajanje e-pošte iz različitog klijent softvera e-pošte. Dva najviše uobičajena sustava za slanje e-pošte su: Outlook i Outlook Express.

Outlook je veliki brat Outlook Express-a i u paketu je s Microsoft Office Suite-om. Outlook je mnogo više od jednostavnom e-mail programa. Može djelovati kao „data assistant“ sa značajkama kao što su kalendar, popis zadataka i upravljanje kontaktima. Kada se istražuju slučajevi gdje se Outlook koristio za upravljanje svakodnevnim poslovima osumnjičenog,

mogu se pronaći ogromno detaljne informacije. Za razliku od Outlook Express-a, Outlook sve svoje podatke sprema u jedan identitet pomoću .pst ekstenzije datoteke. Za pregled sadržaja takve datoteke potreban je ili preglednik ili forenzički softver. FTK i EnCase nude najpotpuniju metodu za izvlačenje podataka iz Outlook datoteka.

Outlook Express iz Microsofta pohranjuje podatke u datoteke s *.dbx* ekstenzijom i zahtijeva nekog da čita te podatke. U svaki se kreiran račun u Outlook Express-u dodjeljuje heksadecimalni slijed brojeva koje Microsoft koristi za prepoznavanje računa. Ovisno o verziji sustava Windows, ovi se identiteti računa nalaze u podmapama mapa Dokumenti i Postavke osim ako korisnik nije prilagodio ili promijenio mjesto mape.

U nekim će se slučajevima morati izvući samo potrebna datoteka iz e-pošte ili će se možda trebati kopirati datoteka i prenijeti podaci na drugo računalo. Slika 2. pokazuje ekstenzije datoteka koje koriste e-mail klijenti. Forenzički softver često sam otvara ove datoteke i izdvaja e-mailove. Uvijek postoji mogućnost korištenja sustava e-pošte osumnjičenog za izdvajanje datoteka, ali upotreba forenzičkog softvera znatno olakšava automatizaciju procesa radi lakše analize i stvaranja izvještaja.

E-Mail Client	*Extensions*	*File Type*
AOL	`.abi` or `.arl`	Organizer file
	`.aim` or `.bag`	Instant messenger
Eudora	`.mbx`	Message base
Outlook	`.pab`	Personal address book
	`.pst`	Compressed personal folder
	`.wab`	Address book
Outlook Express	`.dbx`	Compressed database
	`.dgr`	Fax page
	`.e-mail`	Mail message
	`.eml`	E-mail
Thunderbird	`.msf`	Mail summary file

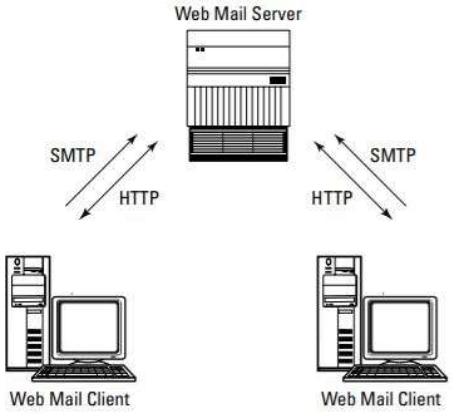
Slika 2: Proširenja datoteka za uobičajene klijente e-pošte

Postoji nekoliko mogućnosti za čitanje različitih vrsta datoteka i izdvajanje e-pošte iz njih, a to su:

- ✓ Klijent e-pošte – mogu se koristiti klijenti e-pošte kao što su Microsoft Outlook ili Eudora za pregled datoteka koje su izvorne s računala koje se istražuje.
- ✓ Preglednik treće strane – softver poput Outlook Extract Pro ili Outlook Export su dostupni za pregled različitih formata e-mail sandučića
- ✓ Forenzički softver – forenzički softveri poput FTK i EnCase, ugradili su preglednike koji izdvajaju sadržaj baza podataka klijenta e-pošte i dopuštaju izvoz informacija na druge medije za analizu.

3.1.4. Istraživanje web orijentiranog sustava e-pošte

Korisnici se često oslanjaju na web orijentirane sustave e-pošte za osobnu komunikaciju. Glavni pružatelji web e-pošte su Yahoo!, Hotmail (Outlook) i Google koji svoje osnovne usluge pružaju besplatno. Web pošta se može koristiti bez softvera klijent e-pošte. Jedini potrebni softver je besplatni web preglednik koji je već instaliran na većini računala. U stvarnosti, web pošta je sustav klijent-poslužitelj. Slika 3. pokazuje osnovne interakcije e-pošte na poslužitelju web pošte.



Slika 3: Transfer e-mail između Web klijenta i servera

U pozadini, sustav web pošte prenosi e-poštu putem SMTP protokola i preuzima ga uz pomoć POP ili IMAP protokola. Najveća tehnička razlika je da se web pošta obično ne pohranjuje na lokalnom računalu, osim ako korisnik ne zatraži takav način pohrane. Računalni forenzički istražitelj zbog toga mora napornije raditi na pronalaženju lokalnih datoteka.

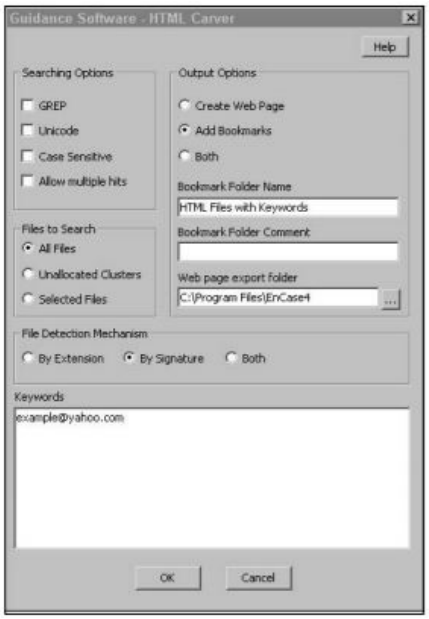
Predmemoriranje podataka pohranjenih u RAM-u bio je spas za mnoge forenzičke istražitelje, a njegova upotreba u e-mail-u forenzičarima nije iznimka. Kad korisnik provjerava svoju e-poštu ili sastavi poruku, operacijski sustav predmemorira podatke sa ekrana na tvrdi disk. Stoga su najbolja mjesta za pronalaženje web pošte u području privremene datoteke, kao što je sustav *swap* datoteka ili predmemorija datoteke i u nedodijeljenom prostoru nakon što su privremene datoteke izbrisane.

Najjednostavniji način pregledavanja sadržaja korisnikovog računa e-pošte je dobiti dozvolu od te osobe. Međutim, izgledi da se to dogodi nisu vjerojatni. Umjesto toga, podaci se mogu pronaći pomoću forenzičkih metoda na lokalnom stroju. Kada se traži internetska e-pošta, pregledavaju se samo web stranice koje imaju e-mail funkcije. Ne traže se datoteke sa e-mail proširenjem nego datoteke sa .html proširenjem. Pretraživanje svake web stranice koju je osumnjičeni ikad posjetio bilo bi gubljenje vremena.

Postoje dva načina za strukturiranje učinkovitog pretraživanja putem web-a:

- ✓ Korištenje ključnih riječi ili izraza zajedno sa oznakama web stranice. Pretpostavimo da je potrebno pronaći poruke e-pošte za joe@gmail.com koje se odnose na istragu bankarske prijevare. Pomoću forenzičkog softvera postavlja se pretraživanje i ograničava se na pretraživanje samo onih web stranica sa ključnim riječima ili izrazima koji su povezani sa specifičnostima istrage. Na ovaj način se uklanjaju vanjske web stranice i fokusira se samo na one sa Joe-ovom adresom.
- ✓ Potrebno se usredotočiti na vrstu usluge koju koristi osumnjičeni, kao što je Yahoo!, Hotmail, Google i sl. Svaki servis koristi riječi ili izraze jedinstvene baš za njih. Mogu se tražiti oni jedinstveni identifikatori da bi se otvorile samo web stranice tih usluga. Međutim, riječi ili izrazi se mijenjaju nakon ažuriranja, stoga treba biti svjestan promjena.

Koraci korištenja ove metode za traženje web pošte razlikuju se ovisno o forenzičkom softveru koji se koristi. FTK i EnCase automatiziraju dohvaćanje web pošte pomoću dijaloških okvira koji postavljaju pitanje koje se ključne riječi traže unutar web stranice. Na slici 4. prikazan je dijaloški okvir koji koristi EnCase za pretraživanje web stranica.



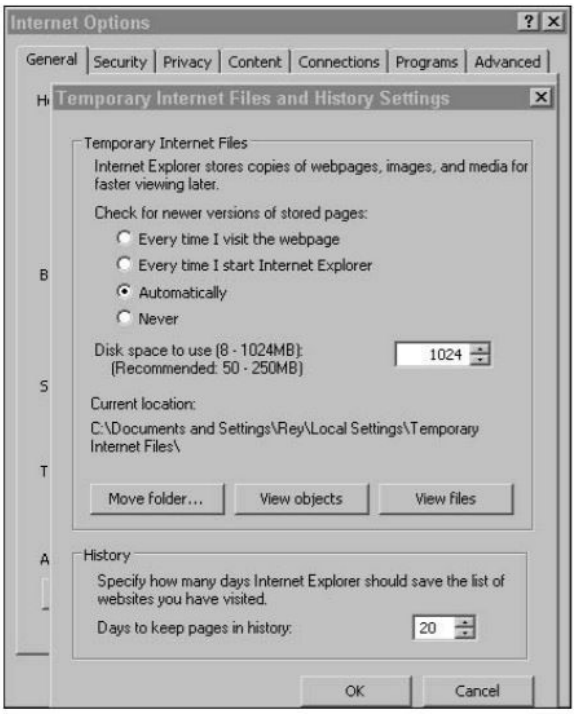
Slika 4: Dohvaćanje e-pošte uz pomoć alata EnCase

3.1.5. Pretraživanje datoteka preglednika

Osim e-pošte, internetski preglednici, poput Internet Explorera, čuvaju privremenu kopiju podataka koji su stigli s Interneta. Većina korisnika nikada niti ne vidi ovu stranu Internet Explorera jer su datoteke preuzete u pozadini. Ono što većina korisnika može vidjeti jest povijest pregledavanja koja prikazuje Web stranice koje je preglednik posjetio.

3.1.6. Privremene datoteke

Privremene datoteke su kreirane od strane aplikacija koja šalju i primaju podatke putem mreže i operativni sustav ih privremeno sprema. Datoteke su prvo pohranjene u RAM-u. Kada se RAM napuni ili operativni sustav te podatke gurne na kraj liste prioriteta koje trebaju dohvatiti aplikacije, datoteke se spremaju na uređaj za pohranu. Ne postoji samo jedno područje za privremene datoteke jer neki programi također stvaraju svoje privremene datoteke. Na primjer, Internet Explorer obrađuje privremene preuzete datoteke s Interneta putem postavki u softveru kao što je prikazano na slici 5.



Slika 5: Postavke povijesti pregledavanja Internet Explorera

Ako aplikacija nema mogućnost privremenog pohranjivanja datoteka za kasniju upotrebu, često omogućuje operativnom sustavu da upravlja ovom funkcijom preko *swap* datoteke ili virtualne memorije. Zamjenska datoteka (*swap* datoteka) je funkcija operacijskog sustava koja djeluje poput RAM memorije, ali koristi tvrdi disk ili uređaj za pohranu umjesto memorijskih mikročipova. Ako aplikaciji trebaju informacije iz *swap* datoteke, operativni sustav dohvaća podatke i briše podatke s uređaja za pohranu. S obzirom da je swap datoteka napisana, a zatim izbrisana, informacije su i dalje fizički na uređaju za pohranu i može ih se preuzeti. Slika 6. pokazuje upravljački dijaloški okvir za postavke virtualne memorije u sustavu Microsoft Windows-u. Virtualna memorija je samo velika datoteka koja se može prilagoditi veličini i može se pisati i brisati slično kao bilo koja druga datoteka u operativnom sustavu.



Slika 6: Postavke virtualne memorije Microsoft Windows-a

3.2. Forenzika podataka

Da bi se moglo izvući podatke s računala, potrebno je shvatiti osnovna načela kako i gdje podaci mogu biti spremljeni. Forenzička znanost o korištenju ispravnog postupka za izvlačenje podataka primjenjuje se nakon što se zna gdje podaci mogu biti pronađeni. Jednostavnije rečeno, izvlačenje podataka je teško ako ne znamo gdje se oni nalaze.

Ovaj postupak može zvučati kao običan i čini se lakim, ali postoji prilično velik broj operativnih sustava kao i specijaliziranih hardvera koji koriste vlastiti način rukovanja podacima. Mobilna industrija računarstva je dosegla svoj vrhunac i sadrži samo desetak ili više različitih operativnih sustava. Dobra vijest je da ako se razumiju osnovni pojmovi najpopularnijih operativnih sustava, jer većina inačica ne zaostaje za originalnim verzijama. Bonus kod većine operativnih sustava je da se temelje na tri popularna proizvoda koji pokrivaju više od 90 posto proizvoda za rad u svijetu računalne forenzike: Microsoft, Apple i Linux.

Dokazi koji se traže većinom se nalaze negdje u prostoru za pohranu na računalu, Područja mobilne i mrežne forenzike imaju zadaću pronaći zapise podataka ili njihovih meta podataka tijekom prolaska kroz njihove sustave, ali područja računalnog sustava za pohranu imaju uobičajene podatke poput e-mailova i dokumenata. Da bi se razumjele osnove funkcioniranja

datotečnih sustava, prvo se moraju znati osnovni pojmovi funkcioniranja hardvera računala u odnosu na operacijski i datotečni sustav. Zamislimo to na ovakav način: Možemo imati kartu kako doći iz Los Angelesa do New Yorka, ali ako se ne razumiju osnovna pravila ceste, poput prometnih znakova ili razloga zašto cesta ima prugu žute boje umjesto bijele pruge, putovanje može završiti katastrofalno.

3.2.1. Pronalaženje skrivenih podataka

Da bi se pronašli digitalni dokazi na uređaju za pohranu, osoba prvo mora znati što traži. Ako slučaj uključuje e-poštu koja sadrži seksualno uznemiravanje, treba se pronaći e-pošta. Kod slučaja pronevjere trebaju se tražiti proračunske tablice ili drugi dokumenti koji obično sadrže iznos valute. Istražitelj će rijetko reći „samo pogledajte računalo i pogledajte što možete pronaći.“ Taj je zadatak veliki gubitak vremena, jer suvremena računala sadrže ogromne količine informacija. U većini slučajeva vrlo je dobar suvremeni računalni forenzički softver koji može izvući velike količine podataka. Međutim, to je dvosjekli mač. Često se nađe toliko informacija i razdvajanje dijelova koji su zaista potrebni postaje problem. Gotovo svatko može shvatiti kako se koristi softver za izdvajanje podataka, ali malo istražitelja zapravo uistinu razumije umjetnost računalne forenzike u odnosu na znanost računalne forenzike.

3.2.2. Izbrisane datoteke

Kada se datoteka izbriše, datotečni sustav stavlja oznaku u svoje upravljanje datotekama, kako bi znao da se datoteka više ne nalazi u tom klasteru. Datotečni sustav na taj način logički briše datoteku iz svoje evidencije, ali fizički nije prošao kroz uređaj za pohranu i obrisao binarne podatke. Kako bi se taj zadatak izbjegao, operativni sustav je ostavio za sobom virtualno binarno arheološko nalazište kroz koje se može „prekopati“. Ironija je da se uređaji za pohranu povećavaju, a količina preostalih podataka iz prethodnih brisanja ostaje netaknuta jer je tako puno više prostora za pohranu na raspolaganju.

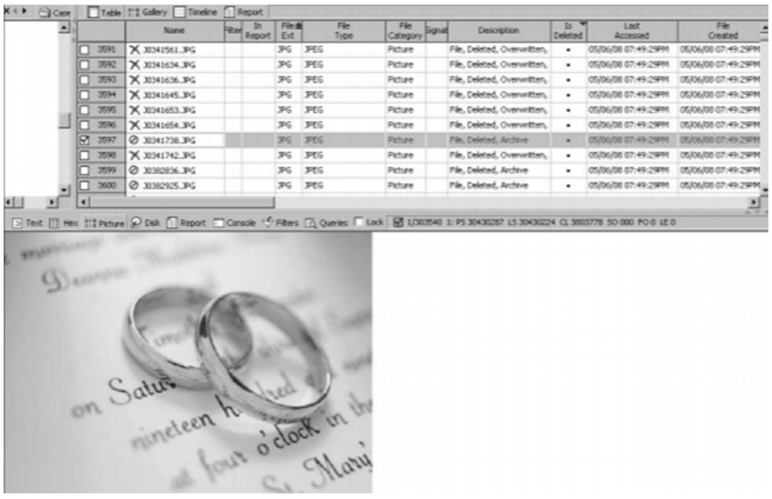
Nelocirani prostor je prostor koji sustav datoteka smatra praznim i spremnim za korištenje. Iako operativni sustav misli da je područje prazno, tamo se može pronaći puno podataka. Stariji datotečni sustavi imaju tendenciju brisati podatke u nerazvrstanom prostoru. Dok kod modernih Microsoftovih računala to nije slučaj. Noviji operacijski sustavi koriste proces u dva koraka, uključujući koš za smeće za brisanje datoteka. U ovom slučaju prvo je potrebno provjeriti koš

za smeće, a onda nelocirani prostor. Predmemorirani podaci se također mogu pronaći u nelociranom prostoru.

Na primjer, ako posjećujemo svoju e-poštu, zaslon se sprema u uređaj za pohranu u određeno vrijeme. Predmemoriranje se u ovom slučaju koristi za ubrzani pregled web stranice. Međutim, i nakon pregledavanja web stranice, ona se sprema i nakon što je datoteka izbrisana iz predmemorije. Pretpostavimo da je tajnica slučajno izbrisala neku važnu e-poštu koja pokazuje otkazivanje rezervacije nekog hotela za sljedeći mjesec. Hotel i dalje naplaćuje tvrtki, a tajnica mora dokazati da je e-mail postojao inače će dobiti otkaz. Nakon brzog forenzičkog ispitivanja, nije samo pronađena e-pošta, nego je primljena i poslana ona pošta koju je imala na e-računu prethodne dvije godine. Dakle, neki podaci se nalaze na računalu još dugo vremena nakon njihovog pregledavanja.

3.2.3. Dohvaćanje izbrisanih datoteka

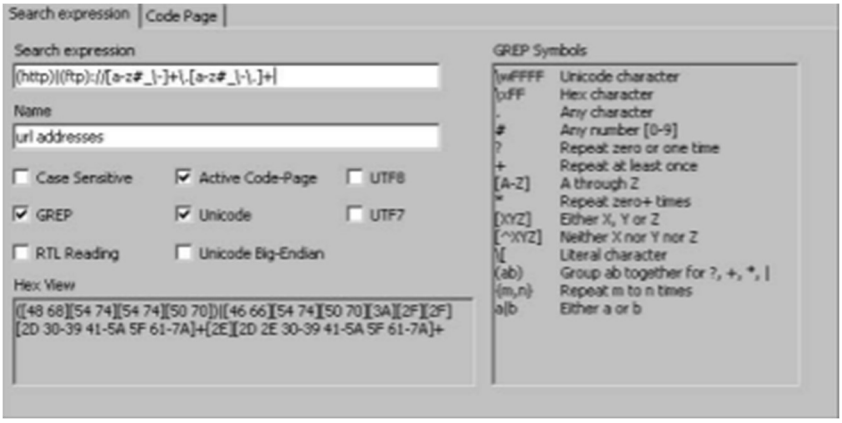
Uz pomoć forenzičkog softvera dohvaćanje izbrisanih datoteka je vrlo jednostavno. Slika 8. prikazuje listu obrisanih JPEG datoteka koje i dalje imaju unose u sustav. U slučaju slike vjenčanog prstena, cijela datoteka se nalazi na tvrdom disku iako je operativni sustav ne vidi. Svi relevantni metapodaci su netaknuti, uključujući oznake vremena i datuma. Ovisno o softveru koji se koristi, postupak popisa izbrisanih datoteka može biti tako jednostavan. Na slici 8 su prikazane sve datoteke koja su u sustavu, samo je potrebno odabrati stupce i retke da bi se prikazali podaci koji su potrebni. Ovo obično funkcionira onda kada je datoteka netaknuta, ali ne funkcionira onda kada se datoteka za predmemoriranje koristila za spremanje na uređaj.



Slika 7: Lista slika pronađena na uređaju za pohranu

3.2.4. Dohvaćanje spremljenih datoteka

Za pronalaženje datoteka poput web stranica ili privremene datoteke u predmemoriji aplikacije, potrebno je izvršiti detaljnije pretraživanje. Ako je potrebno pronaći web stranicu koju je osumnjičeni posjetio, mora se unijeti pretraživački niz koji se nalazi negdje na web stranici kako bi se pronašla odgovarajuća datoteka. Forenzički softver taj postupak čini prilično lakim. Računalni softver treba pronaći sve reference na ključne riječi koje se unose u pretraživanje. Softver će izvući stranicu koja je tražena. Potrebno je koristiti ključne riječi za pretragu i onda ručno izvući tražene informacije. Ova metoda omogućuje bolju kontrolu pretraživanja jer se ne izvlači gomila podataka koji nisu potrebni. Slika 9 prikazuje tipični dijaloški okvir za pretraživanje putem ključnih riječi. Ova metoda uključuje malo više ručnog rada, ali omogućuje preskakanje podataka. Temeljito poznavanje strukture datoteka izuzetno pomaže u ovoj vrsti pretraživanja.



Slika 8: Ručna metoda pretraživanja uz pomoć ključnih riječi

3.2.5. Nedostupan prostor

Područje gdje osumnjičenici mogu sakriti podatke nalazi se na mjestima koja operacijski sustav ne vidi. Operacijski sustav klasificira područja kao oštećena ili im jednostavno ne može pristupiti zbog ograničenja datotečnog sustava.

Budući da datotečni sustav mjesto za pohranu može smatrati oštećenim, postoji mogućnost korištenja heksadecimalnog uređivača za izmjenu postavki datotečnog sustava u kojem se to kontrolira tako da ta područja označi kao loša, a zatim se informacije kopiraju u njih. Taj proces

nije nemoguć, ali je potrebno malo vještine, jer se mora znati kako izmijeniti konfiguracijske datoteke datotečnog sustava.

Drugo mjesto gdje datoteke mogu biti skrivene nalazi se u području uređaja za pohranu koji operacijski sustav ne prepoznaje. Mnogi uređaji za pohranu imaju mala područja koja su potpuno nedostupna operacijskom sustavu. Taj se prostor obično nalazi na fizičkom kraju uređaja za pohranu i može mu se pristupiti samo uz pomoć hex editor-a.

3.3. Forenzika dokumenata

Prilikom forenzičke analize, potrebno je obratiti pozornost na metapodatke. Metapodaci su "podaci o podacima" i bitan su izvor informacija. Sadrže podatke kao što su: autor, organizacija, revizije gdje mogu biti pohranjeni i autori prethodnih revizija i lokacija na kojoj je datoteka bila pohranjena, prethodni autori, korišteni predložak, naziv računala na kojemu je) datoteka stvorena, tvrdi disk i lokacija, ime mrežnog poslužitelja, vrijeme trajanja obrade, izbrisani tekst i sl. Osim metapodataka, potrebno je obratiti pažnju na to da ekstenzija i zaglavlje dokumenta odgovaraju jedno drugome. Svaki tip dokumenta mora imati jedno zaglavlje. Ako bi neki korisnik htio sakriti sliku (ekstenzija .JPEG) koja bi ga mogla otkriti on može promijeniti ekstenziju datoteke. Kada bi istražitelj napravio površnu pretragu putem ekstenzije on može taj dokument označiti kao nebitan. No, ako zaglavlje odgovara .JPEG dokumentu on se još uvijek može otvoriti alatom za pregledavanje fotografija. Postoje forenzički programi koji uspoređuju ekstenziju a zaglavljem i javljaju ako je došlo do promjene.

3.3.1. Pregled metapodataka

Informacije koje korisnik može pronaći kada pregledava metapodatke su:

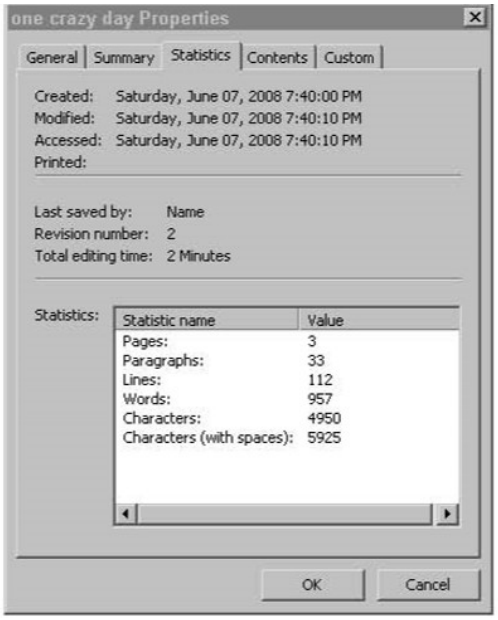
- Osnovni podaci o korisniku: Tipičan Wordov dokument koji prikazuje osnovne korisničke informacije koje se odnose na dokument. Slika 10. prikazuje općenite informacije o dokumentu.

- Statistika dokumenta: Statističke informacije koje su često korisne za određivanje vremenskih crta i potvrđivanje boravišta često se nalaze i u dijaloškom okviru *"Svojstva"*

ovisno o tome koja se kartica odabere (*Općenito, Sažetak, Statistika)*. Slika 11. prikazuje statistiku samog dokumenta, npr. koliko stranica ili odlomaka dokument ima.



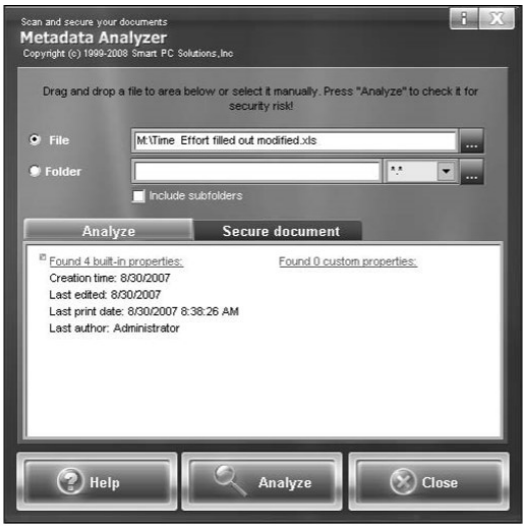
Slika 9: Dijaloški okvir "Svojstva" programa Microsoft Word



Slika 10: Dijaloški okvir "Svojstva" programa Microsoft Word

3.3.2. Izdvajanje metapodataka

Prilikom izdvajanja metapodataka moraju se koristiti posebni alati kao što su *Metadata*, *Analyzer* ili *iScrub* da bi se mogli izdvojiti podaci koji se ne mogu lako vidjeti. Ti alati mogu analizirati dokument na binarnoj razini ili izbrisani tekst koji bi mogao i dalje biti prisutan u dokumentu. Slika 12. prikazuje informacije koje Analyzer može izdvojiti. IScrub je još jači program koji čak pronalazi povijest dokumenta i promjene koje su napravljene u njemu.



Slika 11: Glavni zaslon Analyzer softvera

3.3.3. „Namamljivanje“ dokumenata iz lokalne pohrane

Prvo mjesto za traženje dokumenata je aplikacija u kojoj su stvoreni. U većini aplikacija čuva se popis nedavnih dokumenata koji prikazuje u kojoj su mapi ili direktoriju te nedavne datoteke posljednji put spremljene. Navedeni su putovi datoteka, što uvelike olakšava pronalazak mjesta spremljenih datoteka. Datoteke se ne moraju „loviti“ preko cijelog uređaja za pohranu, a dobiva se i ideja gdje bi se mogle nalaziti ostale datoteke. Ova metoda ima i dobru prednost jer ukazuje trebaju li se pregledati i vanjski uređaji za pohranu.

Ako korisnik računala ima prilično dobro tehničko znanje, najvjerojatnije je obrisana povijest datoteka. U tom slučaju, sljedeći korak je koristiti forenzički program za otvaranje datoteka koje odgovaraju vrsti koja se traži. Forenzički softveri, kao što su FTK i EnCase, imaju značajke

koje omogućuju brzo sortiranje datoteka po vrsti i puno je lakše pretraživanje velikog broja podataka. Slika 13. prikazuje popis datoteka sortiranih prema vrsti datoteke.

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Descr
204951	Cast of Characters ...			wpd	WordPerfect Demo	Document\Education		File, Archive
204952	black codes.wpd			wpd	WordPerfect Demo	Document\Education		File, Archive
204953	Background.wpd			wpd	WordPerfect Demo	Document\Education		File, Archive
204954	Background2.wpd			wpd	WordPerfect Demo	Document\Education		File, Archive
204955	wordpfct.wpg			wpg	WordPerfect Graphic	Picture		File, Archive
204956	WORDPFCT.WPG			WPG	WordPerfect Graphic	Picture		File
204957	wordpfct.wpg			wpg	WordPerfect Graphic	Picture		File, Archive
204958	MS.WPG			WPG	WordPerfect Graphic	Picture		File, Archive
204959	wordpfct.wpg			wpg	WordPerfect Graphic	Picture		File, Archive
204960	wordpfct.wpg			wpg	WordPerfect Graphic	Picture		File, Archive
204961	wordpfct.wpg			wpg	WordPerfect Graphic	Picture		File, Archive
204962	MS.WPG			WPG	WordPerfect Graphic	Picture		File, Archive
204963	wordpfct.wpg			wpg	WordPerfect Graphic	Picture		File, Archive
204964	Default.rul			rul	WordPerfect Rule	Code\Application		File, Archive
204965	Normal.wpt			wpt	WordPerfect Template	Document		File, Archive
204966	Normal.wpt			wpt	WordPerfect Template	Document		File, Archive
204967	CA9CE1E52B76875...			bm	X Window Bitmap	Picture		File, Archive
204968	flower.xpm			xpm	X-Pixelmap Graphic	Picture		File, Archive
204969	foliage.xpm			xpm	X-Pixelmap Graphic	Picture		File, Archive
204970	waffle.xpm			xpm	X-Pixelmap Graphic	Picture		File, Archive
204971	marker.xpm			xpm	X-Pixelmap Graphic	Picture		File, Archive

Slika 12: Grupiranje datoteka prema vrsti

Ako je potrebno tražiti datoteke određene vrste, ovakav način pretraživanja je lako izvršiti. Microsoft Word-ove datoteke nalaze se u mapi *Moji dokumenti*, a prva pretpostavka je da su to datoteke programa Microsoft Word. Nažalost, kada se istražitelji bave pametnim računalnim kriminalcima, ta pretpostavka često može dovesti do predviđanja dokaza koji bi mogli biti na vidljivom mjestu. Ako je potrebno tražiti JPEG datoteke, a pronađu se samo datoteke Word programa, potrebno je pregledati se datoteke. Moguće je da je osumnjičeni promijenio ekstenziju ili zaglavlje datoteke. Potrebno je napraviti dodatni korak podudaranja zaglavlja datoteke sa ekstenzijama datoteka. Ako se podudaraju, ali se datoteke ne mogu otvoriti, potrebno je izmijeniti zaglavlje datoteke.

3.3.4. Podudaranja zaglavlja datoteka sa ekstenzijama

Da bi se lakše shvatilo da li je proširenje datoteke neovlašteno, mora se razumjeti način na koji se datoteke prepoznaju od strane operativnih sustava i aplikacijskog softvera. Programi općenito prepoznaju datoteku ili po zaglavlju datoteke ili nastavku datoteke, dok se operacijski sustavi uglavnom oslanjaju na ekstenziju datoteke kako bi odredili njezinu vrstu.

Zaglavlje datoteka je slijed znakova na početku datoteke koji označava kakve je vrste datoteka. Postoje tisuće različitih vrsta datoteka i pronalaženje zaglavlja može biti izazov ako je datoteka stvorena od strane nejasnog programa. Na sreću, većina datoteka pripada popularnim softverskim paketima, kao što su Microsoft, Novell, Adobe ili Sun.

3.3.5. Izmjena zaglavlja datoteke

Iako se ekstenzija i zaglavlje datoteke podudaraju, ne znači da je datoteka upravo ono što se čini da je. Korisnik također može izmijeniti zaglavlje datoteka kako bi je sakrio čak i na vidljivom mjestu. Ako korisnik promijeni zaglavlje datoteke, ekstenzija datoteke i ime datoteke da bi izgledala kao sistemska datoteka sustava, analiza potpisa samo potvrđuje da se nastavak i zaglavlje podudaraju kako softver ne bi označio datoteku sumnjivom. Prilikom pokretanja datoteke javlja se poruka o pogrešci koja kaže da datoteka ne funkcionira ili se ne može koristiti.

Kako bi se utvrdilo da li je korištena navedena tehnika skrivanja, treba se provjeriti da li se datoteka može otvoriti. Ako se datoteka pokuša otvoriti iz aplikacije, u poruci o pogrešci se navodi da se ta datoteka ne može otvoriti jer je nepoznata vrsta datoteke. Potrebno je znati koje zaglavlje datoteke treba umetnuti na početku datoteke kako bi ona mogla ponovno funkcionirati.

Drugi način je korištenje *hash* vrijednosti poznatih datoteka kako bi ih uklonili iz razmatranja. Biblioteke *hash* vrijednosti postoje za gotovo svaki operativni sustav. Najpopularniji aplikacijski softver (i njihove datoteke podrške) kao što su Microsoft Word ili Excel, također sadrže mnoge *hash* biblioteke kako bi ih eliminirao kao potencijalno skrivene datoteke. Ako korisnik pokušava sakriti datoteku na taj način, datoteka se ističe kao datoteka s *hash* vrijednosti koja ne odgovara nikakvim standardnim datotekama za taj operativni sustav ili aplikaciju. Nacionalna biblioteka referenci softvera (NSRL) je koristan izvor informacija u vezi s vrijednostima *hash* poznatih datoteka. Biblioteke se izravno preuzimaju sa stranica NSRL-a i mogu se umetnuti u forenzički softver za filtriranje poznatih datoteka.

Treći način je pronalaženje datoteka koje su nedavno izmijenjene ili koje su mijenjane prilično često. Korisnik mora izmijeniti datoteku kako bi je otvorio, a zatim je ponovno izmijeniti kako bi je sakrio. Potrebno je imati na umu da se izmjenjuje na tisuće datoteka dnevno i da je ova opcija na posljednjem mjestu.

3.3.6. Pronalaženje veza i vanjske pohrane

Kada se datoteka pohrani ili izvana kopira na lokalno računalo, generira se link datoteka i operacijski sustav zna gdje se ona nalazi. Prilično često, link datoteke su jedini trag da je vanjski uređaj za pohranu bio povezan sa računalom.

Link datoteke se mogu pronaći uz pomoć forenzičkog softvera. Slika 14 prikazuje tipičan popis link datoteka. Ovisno o forenzičkom softveru, koraci dohvaćanja link datoteke se razlikuju. Potrebno je pronaći vezu između mjesta gdje su dokazi pronađeni u odnosu na mjesto gdje je osumnjičeni boravio. Ako je osumnjičeni imao ili ima pristup jednoj ili obje lokacije, vjerojatno ima i pristup dokazima.

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed
194621	A0096975.lnk			lnk	Link	Windows		File, Deleted, Archive, Com	•	05/07/08 10:48
194622	Smart Pix Manager.lnk			lnk	Link	Windows		File, Archive		05/07/08 08:43
194623	MUSICMATCH Burner Plus.lnk			lnk	Link	Windows		File, Archive		05/07/08 08:43
194624	A0097021.lnk			lnk	Link	Windows		File, Deleted, Overwritten,	•	05/07/08 10:48
194625	A0096985.lnk			lnk	Link	Windows		File, Deleted, Archive, Com	•	05/07/08 10:48
194626	New Volume (G).lnk			lnk	Link	Windows		File, Archive		05/07/08 01:07
194627	A0096778.lnk			lnk	Link	Windows		File, Deleted, Archive, Com	•	05/07/08 10:48
194628	A0096785.lnk			lnk	Link	Windows		File, Deleted, Archive, Com	•	05/07/08 10:48
194629	Cases.rar.lnk			lnk	Link	Windows		File, Archive		05/07/08 01:07
194630	Sample Pictures.lnk			lnk	Link	Windows		File, Archive		05/07/08 08:40
194631	A0100276.lnk			lnk	Link	Windows		File, Deleted, Overwritten,	•	05/07/08 10:49
194632	msoffice2003.zip.lnk			lnk	Link	Windows		File, Archive		05/07/08 08:43
194633	A0096788.lnk			lnk	Link	Windows		File, Deleted, Archive, Com	•	05/07/08 10:48
194634	Mozilla Thunderbird (No Extensi...			lnk	Link	Windows		File, Archive		05/07/08 10:31
194635	default.lnk			lnk	Link	Windows		File, Archive		05/07/08 08:43
194636	A0096944.lnk			lnk	Link	Windows		File, Deleted, Archive, Com	•	05/07/08 10:48
194637	A0100275.lnk			lnk	Link	Windows		File, Deleted, Overwritten,	•	05/07/08 10:49
194638	A0096789.lnk			lnk	Link	Windows		File, Deleted, Archive, Com	•	05/07/08 10:48

Slika 13: Popis link datoteka

Nakon pronalaska link datoteka, prva stvar koju treba učinit jest provjeriti jesu li uređaji za pohranu na dohvat ruke. U laboratoriju, najprije je potrebno pregledati dokumentaciju mjesta zločina; ako se istražitelj nalazi na mjestu zločina, potrebno je još jednom provjeriti da se tamo ne nalaze uređaji za pohranu kao što su: vanjski tvrdi disk, kamera, audio snimač, digitalna kopirka i sl.

3.3.7. Sigurnosne kopije

U organizacijama, postoji tendencija pronaći sustave sigurnosne kopije podataka neke vrste. Većina organizacijskih korisnika nema pojma kako sustav sigurnosne kopije funkcionira dok ne izgube datoteku ili uređaj za pohranu, a čak i tada zaborave sigurnosne sustave.

Za kriminalce koji su prilično tehnološki pametni i znaju kako sakriti svoje digitalne tragove na računalima, analiza backup medija je prilično produktivna jer obično imaju malu kontrolu nad sigurnosnim sustavima.

Podaci se mogu pohraniti na nekoliko načina, a svaki ima prednost i mane s obzirom na računalnu forenzičku analizu. Mogu se napraviti mape informacija o dupliciranim uređajima za pohranu i koristiti usluge mrežnog pohranjivanja.

Treba obratiti pozornost da sigurnosne kopije koje su spremljene na dupliciranim uređajima za pohranu i mrežnim uređajima za pohranu slijede iste formate kao i izvorne verzije. Posao postaje mnogo lakši jer su formati datotečnih sustava prilično standardizirani. Problem s takvim metodama mapiranja podataka je u tome što su skupe i imaju iste točke neuspjeha kako i mediji za pohranu koji se sigurnosno kopiraju.

Korištenje trake za sigurnosno kopiranje je daleko najpopularnija metoda. Vrpce postoje već desetljećima, prijenosne su, stabilne i mogu se ponijeti sa sobom kako bi se još bolje zaštitili podaci. Nedostatak je što postoje mnogi različiti standardi za sustave sigurnosne kopije vrpce.

3.4. Forenzika mobilnih uređaja

Pametni telefoni su višenamjenski telekomunikacijski uređaji koji su postali dio svakodnevnog života. Pohranjuju velike količine podataka vezanih za komunikaciju, pristup internetu, GPS lokacije, kalendar, kontakte, fotografije, video i audio zapise čime su prestigli mogućnosti osobnih računala. Kao jedna od grana digitalne forenzike, forenzika mobilnih uređaja postala je nezaobilazna u istragama. Postoji sve veća potreba za pronalaskom, oporavkom i analizom takvih tragova. Podaci zapisani u elektroničkom obliku često predstavljaju jedine ključne i neoborive dokaze nekog kaznenog djela.

Mobilna tehnologija se mijenja vrlo brzo i mnogi od nas ne mogu ići u korak s tim. Iako korisnici računala često povećavaju količinu RAM-a ili prostora na tvrdom disku na računalima, računala istu tehnologiju koriste iz godine u godinu. Kada se istražuju mobilni uređaji, potrebno je zapamtiti da se od računala razlikuju na tri načina:

- ✓ Česta promjena operativnih sustava, metoda sučelja, hardverskih standarda i tehnologija; mogu se promijeniti nekoliko puta unutar raspona od jedne godine. S druge strane, računalni softver ima tendenciju da se ažurira svake godinu ili dvije.

- ✓ Mnogo različitih platformi mobilnih uređaja: da bi otkrivali potencijalne tajne mobilnih uređaja za istragu, potrebno je koristiti nekoliko alata. Na primjer, ako se već nekoliko godina koristi mobilni telefon, dobre su šanse da postoji nekoliko starih punjača koji rade samo na tim modelima mobilnih uređaja. S druge strane, računala još uvijek koriste isti izvor napajanja, povezuju se s mrežom na isti način, pa čak i sadrže ista sučelja, kao što je USB.
- ✓ Mobilni uređaju za komunikaciju koriste bežične tehnologije; Budući da su mobilni uređaju u pokretu, korištenje metode kojim se eliminiraju žice jedina je metoda koju dosta njih koristi kao isključivo sredstvo komunikacije, dok stolna računala mogu koristiti i žičanu komunikaciju.

Postoje tri osnovna sredstva komunikacije za mobilne uređaje osim radija za mobilne telefone koje koriste sve tvrtke:

- ✓ **802.11:** Ovaj standard danas koriste se bežične mreže. Naši kućni usmjerivači koriste 802.11 za bežičnu komunikaciju sa prijenosnim računalom. Raspon mobilnog uređaja uz pomoć ovog standarda varira zbog ograničenja napajanja uređaja.

- ✓ **Bluetooth:** Novi standard koji se koristi za male udaljenosti, kao što je soba standardne veličine. Izvorni Bluetooth standardi sukobili su se s nekim 802.11 uređajima, ali promjene na oba standarda su eliminirale taj problem. Udaljenost od 10 metara smatra se prosječnom za Bluetooth uređaj.

- ✓ **Infracrveno:** Starija metoda komunikacija mobilnih uređaja koja koristi infracrveni dio svjetlosnog spektra za razmjenu informacija. Tijekom komunikacije ova metoda radi na način da se cilja infracrveni priključak mobilnog uređaja do infracrvenog priključka drugog uređaja. Velika većina daljinskih upravljača radi uz pomoć infracrvenog.

3.4.1. Razmatranje mobilnih uređaja „forenzički“

Kada se pogledaju potencijalni dokazi u bilo kojoj istrazi, gotovo uvijek postoji ideja koja se vrsta dokaza traži. Isto vrijedi i za mobilnu forenziku; potrebno je znati koji su dokazi dostupni na određenom uređaju. Ovisno o vrsti uređaja, mogu se pronaći slijedeće vrste dokaza:

- **Identifikatori pretplatnika** – na mobilnim telefonima te informacije koristi mreža za provjeru autentičnosti korisnika na mrežu i provjeru usluga koje su vezane uz račun. Identitet mobilnog uređaja može se povezati sa zapisima koje su pohranjene kod davatelja usluga. Moduli identiteta pretplatnika (SIM) imaju ugrađene te informacije. Ako mobilni uređaj ne podržava SIM kartice, informacije su kodirane u sam uređaj.

- **Dnevnici (eng. *logs*) –** mobilni uređaji često imaju dnevnike poziva koji su postavljeni. Propušteni i primljeni pozivi često mogu formirati ključne vremenske linije. Ostali zapisnici koji se čuvaju, u pozadini sadrže GPS, mrežnu vezu s ćelijama i informacije o prekidu mrežnih ćelija. Ti dnevnici mogu postojati, ali i ne moraju. Ako postoje, vrlo lako se mogu pratiti lokacije mobilnog uređaja.

- **Telefonski imenik/popis kontakata –** popis imena i brojeva često daje tragove istražiteljima, kao i potencijalne svjedoke i žrtve. U tipičnom telefonskom imeniku mogu se pronaći informacije kao što su adrese e-pošte, fizičke adrese, fotografije, pa čak i alternativni telefonski brojevi.

- **Tekstualne poruke** – ove sažete poruke često sadrže komadiće dokaza, kao i datume i vremenske oznake koje su važne istražiteljima. Većina korisnika vjeruje da, nakon što se poruke obrišu, one zauvijek nestanu. Međutim, to često nije tako jer se mogu ponovno vratiti uz pomoć softvera.

- **Kalendari** – gledajući podatke kalendara i imenovanja često se mogu naći tragovi i potencijalni klijenti.

- **Elektronička pošta** – kao i u redovnoj računalnoj forenzici, e-mail na mobilnim uređajima često može dati vrijedne dokaze.

- **Izravne poruke –** live verzija tekstualnih poruka često sadržava cijele razgovore koji imaju važnu dokaznu vrijednost, kako u njihovom sadržaju tako i u informacijama o vremenu i datumu.

- **Fotografije** – gotovo svi mobilni telefoni i PDA-i imaju kamere ugrađene u njih. Sve fotografije i video snimke su potencijalni dokazi.

- **Audio snimke –** uređaji se često udvostruče kao digitalni audio snimači i vrijedni su vremena za istraživanje zbog čega je nešto snimljeno.

- **Multimedijske poruke** – na novijim mobilnim uređajima korisnici sada mogu slati ne samo tekstualne poruke već i audio i video poruke.

- **Datoteke aplikacije** – s novijim mobilnim uređajima koji koriste softver produktivnosti za pregled i proizvodnju dokumenata, proračunske tablice, prezentacije i mnogih drugih formata datoteka, prilično je vjerojatno da će se u tim područjima pronaći dokazi.

3.4.2. Oduzimanje mobilnog uređaja

Postupak izvlačenja podataka iz mobilnih uređaja razlikuje se ovisno o vrsti uređaja. Neki mobilni uređaji, kao što su kamere, tretiraju se kao uređaji za pohranu na isti način kao i USB pogodni. Mobilni telefoni, s druge strane, zahtijevaju specifičan forenzički softver za izvlačenje podataka. Iako je polje relativno novo, moraju se slijediti osnovne smjernice u svim situacijama prilikom rukovanja digitalnim forenzičkim podacima; potrebno je izbjegavati promjenu podataka na izvornom mediju, biti kompetentan i obučen, dokumentirati sve aspekte istrage i za sve aspekte pronaći jednu odgovornu osobu ili organizaciju.

3.4.3. Mobilni uređaji i SIM kartice

Područje mobilne forenzike jedno je od najtežih za praćenje zbog brzo mijenjajuće prirode industrije i širokog spektra nestandardnih uređaja na tržištu. Stalna obuka i studiranje, istražitelje održava u toku s novim tehnologijama koje stalno izlaze na tržište. Unatoč svim razlikama, mobilni uređaji imaju tri temeljen komponente: ROM, RAM i mjesto za pohranu podataka.

ROM (eng. *Read Only Memory*) je područje memorije na mobilnom uređaju gdje je smješten operativni sustav i softver za otklanjanje poteškoća za dijagnosticiranje uređaja.

RAM (radna memorija) je područje memorije koje se često koristi za privremenu pohranu podataka; ako je mobilni uređaj isključen, svi se podaci gube.

Većina mobilnih uređaja ima kapacitet unutarnje pohrane koji se temelji na tehnologiji *flash* memorije i većina naprednih modela isporučuje se s utorima vanjske memorijske kartice koja proširuje kapacitet pohrane na uređaju.

Vanjska pohrana često ima oblik MiniSD ili MMC mobilnih kartica koje zahtijevaju posebne čitače kartica. Većina računalnih forenzičkih alata tretiraju kartice kao redovne uređaje za pohranu osobnih računala i pristupa im se na isti način.

3.4.4. Mobilna mreža uređaja

Jedna od stvari koje istražitelj treba znati je s kojom vrstom mobilnog telefonskog mrežnog sustava mobilni telefon povezuje.

Code Division Multiple Access (CDMA) je dizajniran od strane Qualcomm-a i u upotrebi je u SAD-u. Dva primarna mobilna operatera u SAD-u su Sprint i Verizon. CDMA sustav nema odvojeni Modul identiteta pretplatnika (SIM) u mobilnom uređaju, što znači da su svi podaci pohranjeni na samom uređaju.

Global System for Mobile Communication (GSM) je dizajniran od strane Ericsson-a i Nokie; tehnologija je koja je u upotrebi u Europi, ali se koristi i u SAD-u od strane dva velika prijenosnika mobilnih telefona, Cingular i T-Mobile. GSM sustavi imaju SIM kao zasebnu komponentu dizajniranu da bude prijenosna s jednog mobilnog uređaja na drugi. Za potrebe istražitelja to znači da se mora analizirati i mobilni uređaj i SIM kartica da bi se dobili svi podaci.

Integrated Digital Enhanced Network (iDEN) je vlasnički sustav koji je razvila Motorola, a koji koristi napredne SIM kartice (USIMs) i koji je namijenjen za zamjenu CDMA i GSM. iDEN sustavi imaju SIM kao zasebnu komponentu namijenjenu za prijenos s jednog uređaja na drugi. Kao i kod GSM sustava, potrebno je analizirati i USIM i mobilni uređaj kako bi se pronašli svi podaci.

Mobilni uređaj može se identificirati uz pomoć: logotipa, serijskih brojeva, softvera za sinkronizaciju i proizvodnih kodova.

Proizvodni logotipi često su istaknuti zajedno s brojevima modela. Potrebno je provjeriti web mjesto proizvođača za ažurne informacije o modelu s kojim se radi.

Serijski brojevi čak i unutar istog modela mobilnog uređaja utječu na način pristupa istrazi. Provjera karakteristika mobilnog uređaja s proizvođačem putem serijskog broja, daje iznenađujuće rezultate. Većina serijskih brojeva može se pronaći ispod baterije ili negdje oko odjeljka za baterije.

Mobilni uređaji često su upareni s osobnim računalom osumnjičene osobe. Nakon što se forenzički izdvoje podaci iz osobnog računala, često se mogu pronaći podaci o uređaju koji daju tragove o kojoj se vrsti uređaja radi.

Uz pomoć proizvodnih kodova mogu se identificirati proizvođači telefona, modela, koda države pa čak i serijski broj. Kao i kod serijskog broja mobilnog uređaja, proizvodni kodovi se često nalaze u ili oko odjeljka za baterije. Te informacije se također mogu pronaći u softveru operacijskog sustava mobilnog uređaja.

3.4.5. Karakteristike mobilnog uređaja

Nakon određivanja vrste mobilnog uređaja, važne su i njegove karakteristike koje su navedene od strane proizvođača. Popis značajki koje proizvođač ima za mobilni uređaj, može se znatno razlikovati od stvarnosti onoga što se zapravo nalazi na uređaju.

Kod metoda bežičnog pristupa potrebno je utvrditi koristi li uređaj samo mobilnu tehnologiju za komunikaciju ili koristi Bluetooth, WiFi ili infracrveno.

Potrebno je saznati može li se uređaj koristiti za surfanje webom, provjeravanje e-pošte ili sudjelovanje u chat sesijama. Također treba pogledati da li uređaj ima kameru, a zatim snima li i dalje fotografije ili videozapise.

Što se tiče aplikacija, potrebno je saznati s kojim je vrstama aplikacija mobilni telefon isporučen.

3.4.6. Oprema za mobilnu forenziku

Područje mobilne forenzike je još uvijek prilično novo i zbog toga, jedan forenzički alat ne pokriva sve situacije. Potrebno je imati više alata pri ruci. U određenim slučajevima, forenzički alati ne mogu izvući određene podatke i zbog toga se moraju koristiti razni drugi softveri.

Forenzički softver služi za: čuvanje podataka od promjene na uređaju iz kojeg se izvlače podaci i pružanje mehanizama za provjeru integriteta podataka koji se izdvajaju kako bi se matematički dokazalo da se ništa nije promijenilo.

Uz praćenje svih ostalih pravila i postupaka koji se inače slijede tijekom redovne istrage računalnog forenzičkog mjesta zločina, prioritet prilikom istraživanja mobilnog uređaja je izolacija uređaja iz njegove bežične mreže. Pod svaku cijenu, novi podaci se moraju sačuvati od kontaminiranja mobilnog uređaja nakon što je on zaplijenjen iz nekoliko razloga:

- Radi praktičnosti – kako nove informacije ne bi prebrisale ili eliminirale dokaze koji su već na uređaju.
- Radi sigurnosti – mehanizmi u divljini korisnicima omogućuju daljinsko zaključavanje ili uništavanje podataka mobilnog uređaja.
- Radi zakonitosti – sudovi neće dopustiti dokaze koji su dodani mobilnom uređaju nakon njegove zaplijene.

Mobilni uređaj se može izolirati na nekoliko načina:

1. Izoliranje bežičnih značajki (korištenjem uređaja za ometanje, uređaj se može izolirati dok mu baterija ne bude prazna)
2. Isključivanje uređaja (ova metoda izolira uređaj, ali se ne preporučuje, jer sigurnosni protokol uređaja može biti omogućen kada ga se ponovno uključi)
3. Postavljanje uređaja u način rada „avion“ (ova značajka na nekim pametnim telefonima osmišljena je za isključivanje radija unutar bežičnih uređaja)

Nakon izoliranja mobilnog uređaja, baterija mora biti napunjena tako da se ne izgubi niti jedan podataka. Treba imati na umu da je i mobilni uređaj izoliran, pa korištenje punjača može povećati rizik od poništavanja izolacije.

3.5. Mrežna forenzika

Mrežna forenzika sadrži analizu mrežne opreme kao što su usmjeritelji, preklopnici (eng. *switch*), koncentratori (eng. *hub*), NIC (eng. *Network Interface Card),* samo računalo te razni mediji poput parica, optičkih kablova i slično.

Mrežna forenzika ima dvije uporabe. Prva, ona se odnosi na sigurnost i uključuje praćenje mreže za praćenje neobičnog prometa i utvrđivanje upada. Napadač bi mogao izbrisati sve

datoteke zapisnika na ugroženom domaćinu, stoga mrežni dokazi mogu biti jedini dostupni za forenzičku analizu. Drugi obrazac odnosi se na provedbu zakona. U tom slučaju analiza zarobljenog mrežnog prometa može uključivati i zadatke kao što su ponovno sastavljanje prenesenih datoteka i traženje ključnih riječi.

Vrsta opreme koja se može pronaći na tipičnoj mreži je:

- Usmjerivač (eng. *router*) – računalo posebne namjene koje usmjerava podatke po mrežama. U tu svrhu koristi IP adrese.

- Preklopnik (eng. *switch*) – mrežna komponenta koja koristi identifikaciju kontrole pristupa medijima (MAC) za premještanje prometa unutar mreže.

- Koncentratori (eng. *hub*) – njegova jedina funkcija je ponavljanje bilo kojeg signala primljenog na bilo kojem priključku.

- Network Interface Card (NIC) – kartica mrežnog sučelja je uređaj koji sadrži MAC adresu računala koja je jedinstveni identifikator računala.

- Domaćin (eng. *host*) – bilo koji računalni uređaj priključen na mrežu; sadrži jedan od oblika adresiranja, IP adresu ili MAC adresu.

- Mediji – komponenta koja drži mrežu na okupu. Mediji mogu imati oblik bakrenog ožičenja, optičkih kabela ili radio valova.

Podaci koji su potrebni, mogu se prikupljati sa ovih uređaja:

- Računalo domaćin – prikuplja standardne podatke. Obuhvaća slike uređaja za pohranu, sadržaj radne memorije ili bilo kakve statičke podatke koji se mogu slati preko mreže.

- *Router* – dizajniran je prvenstveno za premještanje podataka između mreža. Vrsta podataka koja se može pronaći, više se odnosi na zapisnike nego na pohranu detaljnih mrežnih razgovora. Mogu sadržavati greške do kojih je došlo tijekom usmjeravanja i sumnjive aktivnosti.

- Vatrozid (eng. *firewall*) – čuva detaljne zapisnike aktivnosti koji se događaju u sustavu. Vode dnevnik aktivnosti kao što su napadi, odbačeni paketi, aplikacije kojima je dopušten izlaz ili ulaz i popisuje sve sumnjive aktivnosti.

- *Intrusion-detecion system (IDS)* – bilježi svaku aktivnost koja je bar malo sumnjiva. Svrha IDS-a je zapisati događaj za daljnje proučavanje, kako se taj događaj ne bi ponovio. Zapisuju se sljedeći podaci: skenovi porta, promet koji dolazi iz sumnjivih portova, IP adrese izvora napada, iskorištenost veze, anonimni pokušaji korištenja i sl.

- *Instrusion-prevention system (IPS)* – sustav za sprečavanje upada blokira ili isključuje bilo kakve uočljive prijetnje na mreži. Njegov glavni zadatak je analiziranje podataka u mreži u stvarnom vremenu, kako bi se ti podaci skenirali.

- Mrežni pisač – moderni pisači pohranjuju zapise o dokumentima koji su se ispisivali zajedno sa metapodacima.

- Mrežni uređaj za kopiranje – pohranjuje zapise o kopiranim i ispisanim dokumentima.

- *Wireless access point* (WAP) – bežična pristupna točka koja zapisuje sve što i „žičani“ usmjeritelj uz podatke specifične za bežični promet kao što su SSID identifikatori mreža.

4. FORENZIČKI ALATI

4.1. Forenzički softverski alati

Nakon obavljene istrage i prikaza njenih rezultata, dokaz postaju subjekti temeljitog proučavanja u sudnici. Da bi se osigurala pravovaljanost dokaza, postoji mnogo softverskih alata koji pomažu istražiteljima pri pregledu, pretraživanju i analizi dokaza.

EnCase alat, koristi bezbroj organizacija za bilo koju forenzičku istragu. Moć ovog alata i mogućnost da se prilagodi za jedinstvena pretraživanja, izdvaja ga od ostalih alata iste namjene. Dolazi ugrađen sa mnogo značajki, kao što su: pretraživanje ključnih riječi, pretraživanje e-pošte i isijecanje web stranica. Pretraživanja se potpuno mogu prilagoditi i automatizirana je funkcija izvješća. Podrška za EnCase je solidna, a tehničko osoblje probleme zna riješiti vrlo brzo.

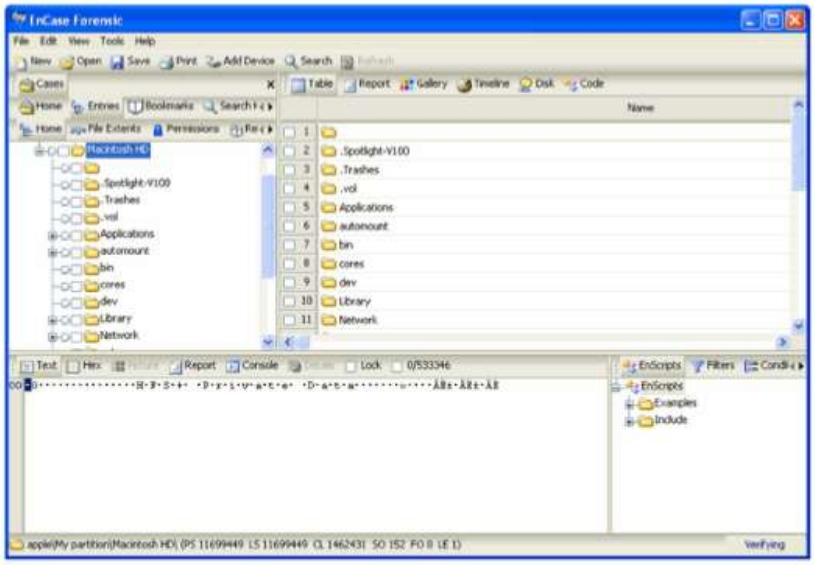
Forensic ToolKit (FTK) je forenzički alat koji je jednostavan za rad zbog svog *one-touch-button* sučelja, a također je i relativno jeftin. Nova verzija FTK-a je još jednostavnija za korištenje, a *AccessData* je pokrenuo forenzičku certifikaciju na temelju svog softvera.

Device Seizure je alat koji se koristi za pristup i preuzimanje gotovo svih informacija koje se nalaze u mobilnom uređaju, kao što su tekstualne poruke ili korisnički podaci na način koji je forenzički prihvatljiv na sudu.

PDBlock je alat tvrtke *Digital Intelligence* koji sprječava pisanje po izvornom disku prilikom forenzičkog kopiranja diska.

DriveSpy je alat temeljen na operacijskom sustavu DOS i on omogućuje stvaranje forenzičke kopije diska, vraćanje obrisanih podataka i analizu upotrebom kriptografskog sažetka.

010 Hex editor je alat tvrtke *SweetScape* koji služi za pregledavanje binarnih datoteka. *Hex Workshop* je programski paket tvrtke *BreakPoint* koji služi za pregledavanje i upravljanje datotekama, predviđen za rad na operacijskom sustavu Windows.



Slika 14: Primjer grafičkog sučelja programa EnCase

4.2. Forenzički hardverski alati

Dok se forenzički računalni softver koristi za pravovremeno izdvajanje podataka i dokaza s logičnog stajališta, forenzički hardver se prvenstveno koristi za povezivanje fizičkih dijelova računala, kako bi se pomoglo izdvojiti podatke. Osnovna ideja forenzičkog hardvera je olakšati forenzički prijenos digitalnih dokaza s jednog uređaja na drugi što je brže moguće. Postoji nekoliko proizvođača takvih forenzičkih uređaja za analizu dokaznog materijala i najvažniji među njima su *Digital Intelligence* i *Vogon International*.

FRED (eng. *The Forensic Recovery of Evidence Device*) je forenzička radionica koja sadrži sučelje za sve prilike. Osim laboratorijske verzije, on dolazi i u mobilnim verzijama koje olakšavaju prikupljanje dokaza na terenu. Jedna od korisnih funkcija FRED-a je zbirka softverskih paketa koji se mogu učitati na njega (EnCase, FTK i sl.)

Logicube je oprema za hvatanje podataka koja hvata podatke sa ciljnog medija i prenosi ih na drugi disk dok istovremeno obavlja provjeru integriteta kako bi se osigurala forenzička kopija.



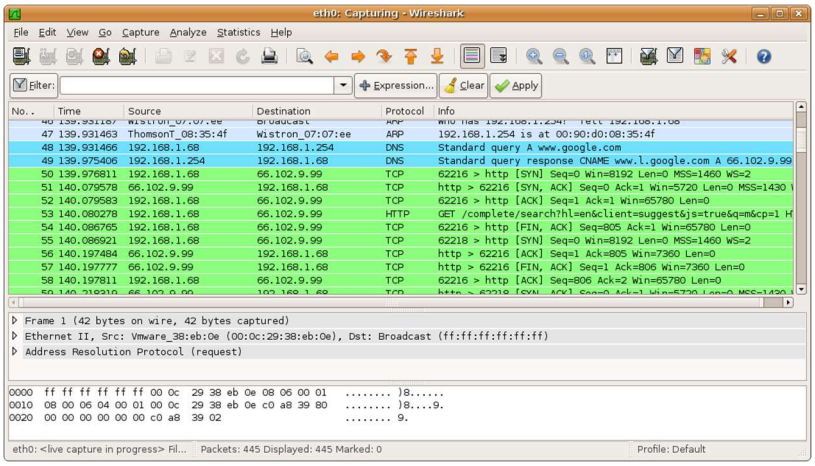
Slika 15: Logicube oprema



Slika 16: FRED - Forensic Recovery of Evidence Device

Neki od besplatnih forenzičkih alata su:

- *Helix* – skupina forenzičkih alata koja uključuje *Sleuth Kit* i mnoge druge aplikacije.
- *Sleuth Kit* – biblioteka i kolekcija komandno-linijskih alata koji omogućuju pretraživanje diska i datotečnog sustava.
- *Win Hex* – alat za upravljanje datotekama, diskovima i radnom memorijom u heksadekadskom formatu.
- *SMART Linux* – Linux-ova distribucija posebno osmišljena za forenzičku analizu dokaza. Sadrži alate za analizu i pretraživanje podataka.
- *Wireshark* – alat za analizu mrežnog prometa.
- *NTFSWalker* – alat za analizu NTFS datotečnog sustava.



Slika 17: Grafičko sučelje alata Wireshark

5. RAČUNALNI FORENZIČKI LABORATORIJ

Svakom dobrom računalnom forenzičaru i istražitelju treba mjesto za rad. Idealna lokacija za provođenje istrage postoji apsolutna sigurnosna kontrola, alati, pa čak i fizičko okruženje. To je forenzički laboratorij. Kao i u bilo kojem području znanosti, računalna forenzika zahtijeva vlastiti skup laboratorijskih alata, kako bi se obavio posao.

5.1. Računalno forenzički poslužitelj podataka

Forenzički poslužitelj podataka omogućuje čuvanje forenzičkih slika na centraliziran i siguran način koji omogućuje da se istražitelj više usredotoči na analizu slučajeva nego na potragu za njima. Poslužitelj treba imati veliki kapacitet za pohranu podataka, mogućnost provjere autentičnosti korisnika u sigurnosne svrhe i kapacitet za izvođenje sigurnosnih kopija svih podataka u slučaju da uređaji za pohranu to ne mogu izvesti.

5.2. Forenzički blokatori pisanja

Iako većina softverskih alata ima ugrađene blokatore pisanja, potreban je asortiman fizičkih blokatora pisanja kako bi se pokrilo što više situacija ili uređaja. Blokator pisanja koristi se za zadržavanje operacijskog sustava od unošenja bilo kakvih promjena u izvorni ili sumnjiv medij kako bi se spriječilo brisanje ili oštećenje potencijalnih dokaza. Blokatori pisanja softvera rade na razini operacijskog sustava. Oni rade samo na operativnom sustavu na kojem su instalirani. Fizički blokator pisanja radi na razini hardvera i može raditi sa bilo kojim operativnim sustavom, jer na fizičkoj razini blokira električne signale uređaju za pohranu.

5.3. Oprema za brisanje medija

Dovršivši jedan slučaj godišnje ili jedan slučaj dnevno, moraju se obrisati mediji s kojima se radilo, kako ne bi došlo do kontaminacije između slučajeva. Oprema za brisanje medija osigurava da na medijima više nema podataka iz prethodnog slučaja. Većina brisača podataka ne briše postojeće podatke, nego prebriše podatke slučajnim binarnim nizovima. Osim ove mogućnosti, potrebno je i izvješće uređaja kako bi se dokazalo da je pogon izbrisan.

5.4. Oprema za snimanje

Korištenje video ili audio opreme za snimanje važnih dijelova slučaja je koristan način trajnog snimanja prikaza slučaja. Koristeći video kameru, više se puta može „posjetiti“ mjesto zločina kako bi se uočio trag koji je možda propušten. Istražitelji svoje metode mogu dokumentirati izravno snimanjem rada ili čak snimanjem zaslona računala.

6. RAČUNALNA FORENZIKA I ZAKONI

Zakon ima presudan utjecaj na računalnu forenziku iz razloga što sadrži stroga pravila o prihvaćanju prikupljenih podataka kao dokaza. Da bi se prikupljene informacije smatrale dokaznim materijalom, mora postojati visoka razina formalnosti u postupanju. Da se ne bi ugrozila pravna upotrebljivost dokaza potrebno je pridržavati se nekoliko pravila. Treba koristiti metode i alate koji su prethodno ispitani i ocijenjeni. Ispitivanje alata provode institucije poput proizvođača softvera i vladinih organizacije. Dokaze treba što manje mijenjati i pohraniti ih na sigurno mjesto. Potrebno je zapisivati sve što je napravljeno jer će dokumentacija biti dio izvještaja. Nadalje, treba paziti na osjetljivost informacija. Zakoni nisu isti u svim državama, ali su im namjene jednake. Stručnjaci za računalnu forenziku moraju imati sve dozvole za pregledavanje, kopiranje, otuđivanje i korištenje svih uređaja i njihovog sadržaja.

Digitalna forenzika je znanstvena disciplina koja je relativno nova i zakoni koji su temelj za priznavanje elektroničkih dokaza na sudu su još uvijek nedorečeni. Napredak tehnologije dovodi do većeg broja dokaza i alata, što ponekad može biti loše jer dokazi nisu posve jasni.

Najstarije tijelo Europske Unije, Vijeće Europe postavilo je temelje dokumenta nazvanog *„Konvencija o kibernetičkom kriminalu“* (eng. *Convention on cybercrime*). Konvencija je prvi međunarodni dokument koji želi prikazati rast informatičkog kriminala. Hrvatska je taj dokument ratificirala[2] 2002. godine.

[2] ***Ratifikacija*** je jednostrani međunarodni čin kojim država na međunarodnom planu daje svoj pristanak da bude vezana međunarodnim ugovorom. Radi se o jednostranom očitovanju jedne ugovorne stranke drugoj ugovornoj stranci kojim se potpisani međunarodni ugovor prihvaća kao obvezatan.

7. ZAKLJUČAK

Kao što sam već i navela, računalna forenzika je grana znanosti koja je relativno nova, ali uvelike pomaže prilikom rješavanja različitih zločina. U ovo vrijeme, kada se svi ljudi svijeta koriste internetom i drugim medijima, stopa kriminala je u porastu, posebice stopa cyber kriminala. Uz pomoć novih metoda i tehnologija, računalna forenzika na kvalitetniji i brži način pomaže prikupiti dokaze i doći do rješenja istrage. Postoje razne prednosti, ali i nedostaci računalne forenzike.

Glavna prednost računalne forenzike je sposobnost da brzo i učinkovito pretražuje i analizira veliku količinu podataka. Dokazi se mogu tražiti provjerom potpisa datoteka, pretraživanjem uz pomoć ključnih riječi, zamjenskih datoteka i sl. Vrijedni podaci koji su izgubljeni ili obrisani mogu se dohvatiti i iskoristiti kao dokaz na sudu.

Prvi od problema korištenja digitalnih dokaza je taj što se podaci mogu vrlo lako izmijeniti. Računalni forenzičar mora prikazati legitimne podatke i cjelokupna istraga mora biti dokumentirana. Još jedan od nedostataka je trošak prilikom dohvaćanja podataka. Analiziranje podataka može potrajati duže vremena i ovisit će o prirodi slučaja. Digitalnim dokazima se mora pristupati sa velikom pažnjom i temeljito ih predstaviti na sudu.

Iako postoji mnoštvo alata za prikupljanje i analizu dokaza, bez stručnog nadzora mnoge stvari mog poći po zlu i uništiti dokaze. Forenzičku istragu ne može provesti bilo tko služeći se alatima koji su dostupni putem interneta, nego je kvalitetno mogu provesti samo forenzički stručnjaci.

Danas postoje razne izobrazbe o prikupljanju, ispitivanju i korištenju digitalnih dokaza. Uz sve to, uskoro će biti potrebno i profesionalno obrazovanje u području računalne forenzike zbog napretka tehnologije i porasta kriminala. Računalna forenzika će proširiti svoje granice.

8. LITERATURA

Knjige:

1. Volonino L., Anzaldua R., *Computer Forensics for Dummies*, 2008.

2. Britz T. M., *Computer Forensics and Cyber Crime,* 2013.

3. Schweitzer D., *Incident Response: Computer Forensics Toolkit*, 2003.

Internetski izvori:

1. https://www.ieee.hr/_download/repository/03_Ieee_Uvod_u_racunalnu_forenziku.pdf pristupljeno: 02.08.2020.

2. https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-05-301.pdf pristupljeno: 05.08.2020.

3. https://www.cis.hr/WikiIS/doku.php?id=network_forenzika , pristupljeno: 20.09.2020.

4. https://digitalna-forenzika.com/forenzika-mobilnih-uredaja/ , pristupljeno: 23.09.2020.

5. https://en.wikipedia.org/wiki/Network_forensics , pristupljeno: 23.09.2020.

6. https://www.srce.unizg.hr/arhiva_weba/sistemac2015/index.php%3fid=35&no_cache=1&tx_ttnews%255Btt_news%255D=1148.html , pristupljeno: 20.09.2020.

9. PRILOZI

Slika 1: Informacije u proširenom zaglavlju 8
Slika 2: Proširenja datoteka za uobičajene klijente e-pošte 9
Slika 3: Transfer e-mail između Web klijenta i servera 10
Slika 4: Dohvaćanje e-pošte uz pomoć alata EnCase 12
Slika 5: Postavke povijesti pregledavanja Internet Explorera 13
Slika 6: Postavke virtualne memorije Microsoft Windows-a 14
Slika 7: Lista slika pronađena na uređaju za pohranu 16
Slika 8: Ručna metoda pretraživanja uz pomoć ključnih riječi 17
Slika 9: Dijaloški okvir "Svojstva" programa Microsoft Word 19
Slika 10: Dijaloški okvir "Svojstva" programa Microsoft Word 19
Slika 11: Glavni zaslon Analyzer softvera 20
Slika 12: Grupiranje datoteka prema vrsti 21
Slika 13: Popis link datoteka 23
Slika 14: Primjer grafičkog sučelja programa EnCase 33
Slika 15: Logicube oprema 34
Slika 16: FRED - Forensic Recovery of Evidence Device 34
Slika 17: Grafičko sučelje alata Wireshark 35