# FORENZIČKA ANALIZA UREDSKIH DOKUMENATA

**Đuranec, Antun**

**VELEUČILIŠTE U RIJECI**

Antun Đuranec

# FORENZIČKA ANALIZA UREDSKIH DOKUMENATA

(specijalistički završni rad)

Rijeka, 2018.

**VELEUČILIŠTE U RIJECI**
Poslovni odjel
Specijalistički diplomski stručni studij
Informacijske tehnologije u poslovnim sustavima

# FORENZIČKA ANALIZA UREDSKIH DOKUMENATA

(specijalistički završni rad)

MENTOR

Dr.sc. Vukelić Bernard, viši predavač

STUDENT

Antun Đuranec

MBS: 2422000104/16

Rijeka, srpanj 2018.

VELEUČILIŠTE U RIJECI

Poslovni odjel

Rijeka, 21.6. 2018.

# ZADATAK
## za specijalistički završni rad

**Pristupniku Antun Đuranec** **MBS: 2422000104/16**

**Studentu specijalističkog diplomskog stručnog studija Informacijske tehnologije u poslovnim sustavima izdaje se zadatak specijalističkog završnog rada – tema specijalističkog završnog rada pod nazivom:**

**FORENZIČKA ANALIZA UREDSKIH DOKUMENATA**

**Sadržaj zadatka:** Opisati glavne pojmove uredskog poslovanja kao i računalne forenzike. Opisati vrste digitalnih podataka i dokumenata koje se koriste u uredskom poslovanju te definirati njihovu vrijednost kao mogući dokaz u procesu forenzičke analize. U praktičnom dijelu rada prikazati primjer forenzičke analize na slučaju ilegalnog izvlačenja uredskih podataka korištenjem i usporedbom *open-source* i komercijalnih forenzičkih alata.

**Preporuka** _____

Rad obraditi sukladno odredbama Pravilnika o završnom radu Veleučilišta u Rijeci.

**Zadano: 21.6.2018.** **Predati do: 15.9.2018.**

**Mentor:** **Pročelnik odjela:**

**Dr.sc. Bernard Vukelić, v. pred.** **Mr.sc. Marino Golob, v. pred.**

**Zadatak primio dana: 21.6.2018.**

Antun Đuranec
(Antun Đuranec)

**Dostavlja se:**
- **mentoru**
- **pristupniku**

# IZJAVA

Izjavljujem da sam specijalistički završni rad pod naslovom „Forenzička analiza uredskih dokumenata“ izradio samostalno pod nadzorom i uz stručnu pomoć mentora dr.sc. Vukelić Bernarda, višeg predavača.

Antun Đuranec

Antun Đuranec

(potpis studenta)

Sažetak:

U ovom specijalističkom završnom radu obrađene su teme uredskog poslovanja i digitalne forenzike na primjeru testnog slučaja prilikom počinjenja ilegalnog izvlačenja osjetljivih uredskih podataka firme. U forenzičkoj analizi korišteni su alati otvorenog koda, te komercijalni alati kako bi se prikazale funkcionalnosti istih. Kroz rad je izveden proces forenzičke analize, priprema za samu analizu, te su objašnjeni temeljni pojmovi iz uredskog poslovanja i računalne forenzike koje je potrebno poznavati za razumijevanje rada. Prilikom forenzičke analize pronađeni su uobičajeni digitalni podaci i tipovi dokumenata koje je moguće pronaći u današnjem uredskom poslovanju, te je prikazana njihova vrijednost kao mogući dokazi u procesu forenzičke analize. Izvedene su standardne forenzičke procedure prilikom digitalne forenzike kojih se istražitelji trebaju pridržavati kako bi njihovi nalazi bili prihvaćeni u sudskom procesu. Na kraju rada napravljena je analiza mogućnosti i usporedba dvaju programa, te su kroz sam rad prikazani rezultati forenzičke analize. Za praktički dio ovog rada korišteni je program otvorenog koda Autopsy i komercijalni program Forensic Explorer. Rezultatima izvršene analize, u ovom specifičnom slučaju izvlačenja uredskih podataka, pokazano je da oba programa sadrže potrebne funkcionalnosti za analiziranje dokaza.

Ključne riječi : Digitalna forenzika, uredsko poslovanje, forenzička analiza, Autopsy, Forensic Explorer

# SADRŽAJ:

# 1. Uvod

Uredsko poslovanje sastavni je dio poslovnih organizacija koji se kroz povijest razvijao prateći razvoj novih tehnologija, te se digitalizacijom uredskog poslovanja javila potreba za zaštitom dokumenata od digitalnog kriminala. Jednostavnije kopiranje i prenošenje digitalnih dokumenata predstavljaju veliki problem poslovnim organizacijama koje žele ograničiti pristup osjetljivim uredskim podacima dok pojedinci s kriminalnim namjerama svakodnevno otkrivaju nove načine za ilegalno izvlačenje osjetljivih digitalnih podataka. Kakve se sve vrste digitalnih dokumenata mogu naći u uredskom poslovanju i gdje pronaći dokaze? Prema nekim procjenama u 2017. godini prosječna šteta po ilegalnom izvlačenju uredskih podataka iznosila je preko 3 milijuna američkih dolara. Upravo kao uzrok povećanja digitalnog kriminala javlja se sve veća potreba za digitalnom forenzikom, znanosti koja se bavi analizom velikog broja digitalnih podataka kako bi se među njima, koristeći forenzičke alate, pronašli relevantni dokazi za utvrđivanje krivnje u sudskom procesu. Može li se digitalnom forenzikom pronaći relevantni dokazi u slučaju izvlačenja uredskih podataka i na kakve prepreke forenzičari mogu naići prilikom forenzičke analize? Sadrže li i komercijalni programi i alati otvorenog koda, koje forenzičari koriste, potrebne funkcionalnosti za pronalaženje i analiziranje dokaza? Ako i sadrže, hoće li rezultati analize biti drugačiji?

Cilj rada je prikaz procesa forenzičke analize prilikom ilegalnog izvlačenja uredskih podataka korištenjem komercijalnih programa i programa otvorenog koda, te usporedba njihovih funkcionalnosti. Svrha rada je prikaz uloge digitalne forenzike u procesu prikupljanja i analize dokaza za sudski proces.

Rad je podijeljen je kroz četiri cjeline. U prvoj djelu obrađeni su osnovni pojmovi uredskog poslovanja i njegova funkcija u poslovnoj organizaciji. Kroz drugu cjelinu objašnjena je digitalna forenzika i njezine grane, dok se u trećoj cjelini obrađeni dijelovi forenzičke analize. U petoj cjelini opisana je forenzička analiza kroz praktični primjer slučaja ilegalnog izvlačenja uredskih podataka, te usporedba korištenih forenzičkih programa Autopsy i Forensic Explorer.

## 2. Uredsko poslovanje

Uredsko poslovanje u tijelima državne uprave uređeno je uredbom o uredskom poslovanju na temelju članka 60. stavka 1. zakona o sustavu državne uprave. Članak 3. ove uredbe definira uredsko poslovanje:

„*Uredsko poslovanje je skup pravila, mjera u postupanju s pismenima, njihovu primanju i izdavanju pismena, njihovoj evidenciji i dostavi u rad, obradi, korištenju, otpremanju, čuvanju, izlučivanju i predaji nadležnom arhivu ili drugom nadležnom tijelu.*“ (NN, 2009.)

Ured je odvojena organizacijska jedinica, poslovni prostor, u kojem se raspolaže i upravlja različitim informacijama, te tako podržava funkcioniranje organizacije. Danas, kada se govori o uredskom poslovanju najviše se nalazi na računalom podržano uredsko poslovanje koje se bazira na digitalizaciji, automatizaciji i novim tehnologijama.

„*Uobičajeno, ured se smatra mjestom gdje se obavlja kancelarijski rad i gdje se održavaju i rješavaju sve vrste papirologije (pisma, dopisivanje, datoteke, zapisi, itd.). To je središnje mjesto gdje se vrše sve vrste kancelarijskog rada za koordinaciju i kontrolu poslova cijele organizacije.“* (Chopa, Gauri, 2015., 1.)

Jedna od ključnih funkcija u modernom uredu su prihvaćanje informacija koje mogu doći iz okoline ili iz organizacije. Neke od takvih informacija dospijevaju do ureda putem pisma, telefonskih poziva, izvještaja i sličnim načinima za prenošenje informacija. U uredu se zatim izvršavaju funkcije zapisivanja informacija. Zapisi se koriste kako bi informacije bile brže dostupne. Prva skupina zapisa mora se čuvati radi zakona država dok se drugi dio sprema radi menadžmenta i planiranja. Nakon faze zapisivanja informacije je potrebno pripremiti iz razloga što ured često dobiva neobrađene informacije u raznim oblicima. Ured je zadužen za obradu takvih informacija i njegovu prilagodbu. Spremljene obrađene informacije moraju biti spremne i dostupne menadžmentu za upotrebu. Zahtjevi za takvim podacima mogu biti rutinski ili neki od posebnih zahtjeva.

## 2.1. Razvoj uredskog poslovanja

Samo uredsko poslovanje prošlo je kroz različite faze kao posljedica razvoja tehnologija u cilju ubrzavanja i unaprjeđivanja uredskih aktivnosti. Prvu fazu mehanizacije, uredsko poslovanje doživjelo je 1870-tih izumom pisaćeg stroja koji su omogućili lakše i brže pisanje. Mehanizacija nije bila dovoljna prilikom konstantnog povećanja poslovnih aktivnosti i količine podataka, te se 1950-tih godina javljaju uređaji za automatizaciju jednostavnijih zadataka, dok se sredinom 70-tih javljaju jednostavna računala, te dolazi do faze automatizacije uredskog poslovanja. Daljnjim razvojem računala 80-tih godina ubrzava se proces prikupljanja i manipulacije informacijama, te uredsko poslovanje ulazi u fazu informatizacije uredskog poslovanja. Informatizacija uredskog poslovanja nastaje kao posljedica razvoja tehnologija za obradu teksta, organizaciju poslovnih informacija i osobnog rada, upravljanje projektima i mnogim drugima. Od 90-tih godina uredsko poslovanje prolazi kroz fazu integracije u kojem je cilj povezivanje svih aktivnosti tvrtke kako bi se uredske aktivnosti izvršavale sustavno, a time se javljaju i prvi uredski informacijski sustavi koji podržavaju sve veći broj aktivnosti .

„*Usporedba današnjeg ureda s uredom desetljeća ranije objašnjava dolazak eksplozije informacija i ogromne transformacije, što je rezultiralo načinom na koji je ured uspio prolaziti kroz brzu i značajnu promjenu. Informacijska se tehnologija mijenja velikom brzinom čime je upravljanje modernim uredom sada brže i puno bolje.*" (Chopa, Gauri, 2015.)

Danas se u uredu nalazi veliki broj informatičke opreme i programske podrške kao posljedica razvoja informacijskih tehnologija. Nemoguće je zamisliti ured bez osobnih računala, pisača, skenera i druge računalne opreme, te programskih paketa za lakše procesiranje uredskih dokumenata i informacija u obujmu u kojem danas dolaze.

„*Uredi će u 21. stoljeću biti elektronska zemlja čuda gdje će skupi rad na bazi papira biti zamijenjen rezultatima orijentiranom informacijskom tehnologijom.*" (Chopa, Gauri, 2015., 13.)

## 2.2. Obrada dokumenata u uredu

Dokument je prema uredbi o uredskom poslovanju na temelju članka 4. definiran kao:

„*…svaki podatak, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, fizički predmet, priopćenje ili informacija, koji sadržajem i strukturom čini raspoznatljivu i jednoznačno određenu cjelinu povezanih podataka*." (NN, 2009.)

Računala su danas sastavni dio ureda na kojima se odvijaju razna analiziranja nad informacijama kojima se znatno smanjuje upotreba papira.

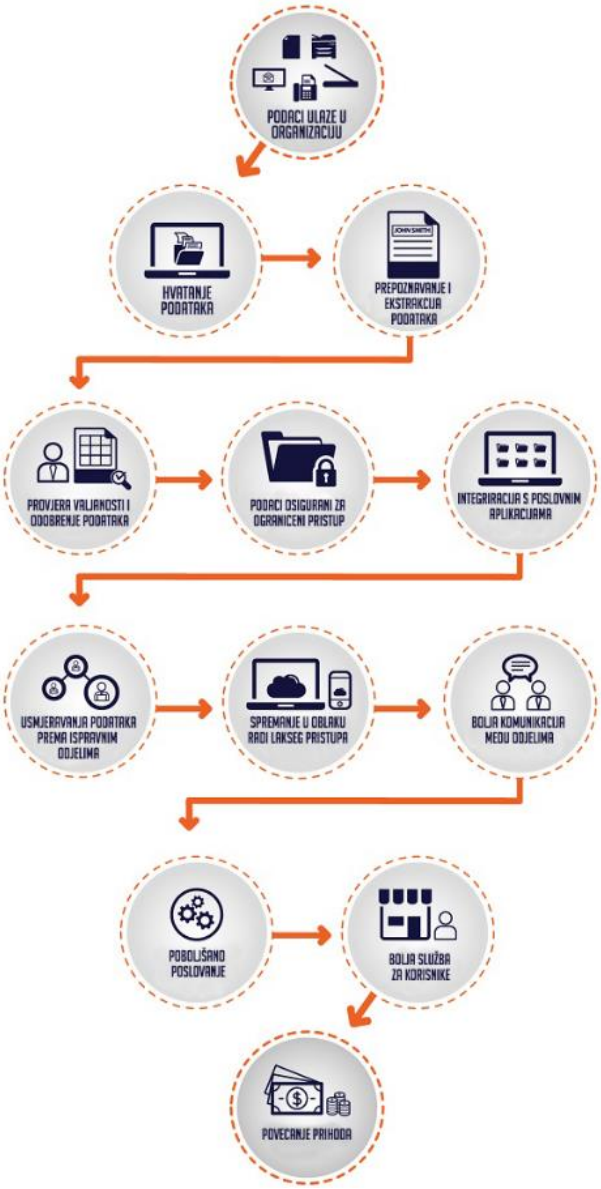
„*Integrirani pristup u kojem se informacije tretiraju kao primarni resurs neophodan je kako bi se postigle maksimalne koristi od automatizacije uredskog poslovanja. Nadalje, programi koje podržava elektronički ured moraju biti potpuno pouzdani, dostupni svima i dovoljno jednostavni da ih svi mogu koristiti bez obzira na njihovu sposobnost ili status...*" (Chopa, Gauri, 2015., 15.)

Danas se automatizacijom procesuiranja dokumenata objašnjava proces koji omogućava kreiranje digitalnih dokumenata koristeći razne alata i skenere. Digitalne dokumente uz pomoć računalnih programa znatno je lakše analizirati, proslijediti, spremiti i čuvati, dok se u isto vrijeme oslobađa fizički prostor od papira. U uredu se obrađuju sa stajališta automatiziranog postupka vrlo složene obrade raznih obrazaca koji se mogu pojavljivati u raznim tipovima digitalnih datoteka, te dokumenti u obliku slika. Digitalni dokumenti mogu biti spremljeni na tvrdom disku ili optičkim mediju a takvi dokumentni mogu sadržavati informacije kao ime autora, datum, vrijeme nastajanja, te ih je moguće pregledati, ispisati i dijeliti.

„*Problem je u tome što se mnoge male tvrtke moraju nositi s mješavinama staromodnih podataka na papiru i elektronskim datotekama – a u nekim slučajevima, udio papira je mnogo veći.*" (Ward, 2018.)

Neke od prednosti koje se postižu digitalizacijom dokumenata su centralizacija prilikom korištenja servera i računalstva u oblak i jednostavan pristup informacijama neovisno o lokaciji. Indeksiranje i arhiviranje omogućuju brzo pronalaženje potrebnih dokumenata u trenutku potrebe. Mogućnost integracije s drugim poslovnim aplikacijama, te dijelovima drugih sustava poput ERP-a (*Enterprise Resource Planning*) omogućuju pregled svih poslovnih procesa koji se izvode unutar organizacije.

Slika 1. - Proces obrade dokumenata i prednosti automatizacije




Izvor: obrada autora prema https://invensis.net/blog/data-processing/paperless-office-document-process-automation-way/ (26.5.2018.)

Proces obrade dokumenata moguće je izvršavati u raznim računalnim programima poput Microsoft Word-a za obradu teksta, te Microsoft Excel-a za tablične podatke. Oba programa omogućuju veliki broj automatiziranih procesa, kao npr. ispisivanje postojećih dokumenata u slike koje onemogućuju naknadno mijenjanje sadržaja. Digitalni dokumenti mogu biti i uneseni, te spojeni s raznim drugim vrstama zapisa poput zvuka i video isječaka.

„*Ove datoteke mogu se pregledavati u izvornom formatu, aplikacijama (npr., MS Word, PowerPoint itd.) ili pomoću preglednika datoteka iz sustava za slikanje*" (Odgers, 2015., 416.)

## 2.3. Poslovno komuniciranje

„*Komunikacija je jedna od temeljnih funkcija ureda, te proces koji je bitan za sve oblike poslovanja.*" (Chopa, Gauri, 2015., 333.)

Poslovno komuniciranje u užem smislu može se gledati kao dvosmjerni kanal za odašiljanje i primanje ideja, planova, naredbi, izvještaja, prijedloga koje se odnose na poslovnu organizaciju i njene ciljeve, a moguće ga je podijeliti na unutarnju komunikaciju i vanjsku komunikaciju. Unutarnja komunikacija odnosi se na komunikaciju radi menadžmenta, koordinacije, integracije, motivacije i treninga. Bez ključnih unutarnjih komunikacija organizacija ne može pravilno izvoditi svoje aktivnosti. Vanjska komunikacija odnosi se na prenošenje informacija prema ljudima izvan organizacije koji mogu imati ulogu potrošača, investitora, dobavljača, i slično, a može se izvoditi radi povezivanja s okruženjem, konkurencija i javnih odnosa.

Slika 2. - Uloga komunikacije i funkcije


Izvor: autor

„*Učinkovito obavljanje uredski zadataka zahtijeva redovitu razmjenu informacija i poruka između pojedinih rukovoditelja, različitih odjela i unutar istog odjela.*" (Chopa, Gauri, 2015., 337.)

Kako bi poslovno komuniciranje bilo efikasno, u uredu se koriste razni alati, komunikacijski sustavi koju pridonose lakšem komuniciranju između zaposlenika, odjela pa čak i postrojenja koji se nalaze na raznim lokacijama. Prilikom određivanja alata za komunikaciju potrebno je u obzir uzeti brzinu izvođenja komunikacije, udaljenost, točnost, tajnost komunikacijskog kanala, kvalitetu veze, mogućnost snimanja itd..

„*U gotovo svakoj organizaciji, komunikacija teče u različitim smjerovima: prema dole, prema gore i unakrsno.*" (Chopa, Gauri, 2015., 339.)

Komunikacija se unutar organizacije može odvijati prema dole kada se radi o promjenama, naredbama, instrukcijama, razgovorima, sastancima, pismima i sličnom, dok se komunikacija prema gore odnosi na prenošenje informacija od strane zaposlenika prema nadređeni osobama. Komunikacija prema gore može se odnositi na sugestije, pritužbe, grupne sastanke itd., a jedna je od ključnih čimbenika za viši menadžment koji ovom komunikacijom dobiva korisne informacije o radu zaposlenih, stanju tržišta i financijskim podacima. Unakrsna komunikacija odnosi se na horizontalnu komunikaciju između zaposlenika na istom organizacijskoj razini, te dijagonalnom protoku podataka između zaposlenika na različitim organizacijskim razinama. Nerijetko se u organizacijama ne slijedi organizacijska hijerarhija kada se želi ubrzati komunikacija, poboljšati suradnja među zaposlenicima i postići brža koordinacija zaposlenika kako bi se efikasnije postigli ciljevi organizacije.

Unutarnju komunikaciju moguće je izvršavati licem u lice ili preko mehaničkih uređaja, a smatra se jednom od najvažnijih metoda efektivnog komuniciranja iz razloga što omogućuje kontakt između nadređenih i zaposlenika na dnevnoj bazi. Ovom metodom nadređeni imaju mogućnost brzo i jednostavno objasniti svoje stajalište. Telefoni su uobičajeni i efektivni mehanički uređaji za komunikaciju. Zavisno od veličine organizacije i njezine strukture telefonski sustav mora biti pomno isplaniran kako bi podržao funkcije organizacije bez poteškoća. Potrebno je prilikom postavljanja sustava obratiti pozornost na nabavu potrebnog

broja telefona s upravljačkom pločom za prebacivanje poziva kojima se smanjuje čekanje na linijama. Ploče za prebacivanje poziva ne smiju biti zastarjele, te osoblje koje ih koristi treba biti educirano kako ne bi došlo do gubljenja vremena i odgađanja komunikacije.

Pismena komunikacija može se u organizacijama sresti u oblicima pisma, memoranduma, izvještaja, ali i formalnim oblicima kao što su razne ponude.

„*Uobičajeni problemi u pismenim komunikacijama su loši zaključci ili je zakopan u izvještaju, previše su opširni, koriste kompliciranе rečenice i imaju pravopisne pogreške.*" (Chopa, Gauri, 2015., 350.)

Kako bi se pismena komunikacija poboljšala i bila razumljivija, preporučuje se korištenje jednostavnih riječi i fraza, poznatih izraza, slika i grafikona, te je poželjno izbjegavati nepotrebne riječi. Neke od prednosti pisane komunikacije su preciznije i točnije poruke, mogućnost većeg broja detalja, ozbiljnost odnosno formalnost pisanih poruka je veća, a pismena komunikacija prisutna je i dostupna za odašiljanje u bilo kojem dijelu svijeta. Neke od vrsta pisane komunikacije su pošiljateljski servis koji uključuje osobu zaduženu za preuzimanje, pošiljanje, dostavljanje i prijenos pošiljki unutar firme ili odjela. Unutrašnji servis računalne pošte znatno je unaprjeđenje nad pošiljateljskim servisom, a omogućava jednostavno prikupljanje poruka od strane zaposlenika i odjeljenja koje se zatim dostavljaju zaposlenicima. Ovaj sustav ako je dobro namješten i pravilno reguliran može biti najekonomičnije rješenje za pisanu komunikaciju.

„*Tvrtke širom svijeta koriste aplikacije za računalnu poštu kako bi unaprijedile način poslovanja. Sada se poruke mogu prenijeti po djeliću prije normalnih troškova.*" (Chopa, Gauri, 2015., 359.)

Danas, kako bi organizacije koristile sve prednosti koje donosi računalna pošta moraju imati pristup računalu i internetskoj vezi. Računalna pošta uz pomoć razvijenih programa omogućuje jednostavnu distribuciju digitalnih informacija do zaposlenika, dobavljača i korisnika.

Mehanička komunikacija podrazumijeva pisane poruke koje se mehanički dostavljaju osobama za koje su informacije namijenjene. Današnji mehanički uređaji koji su spoj više uređaja poput faksa, printera i kopirke, predstavljaju kompletno uredsko rješenje. Ovakvi uređaji omogućili su odašiljanje digitalnih dokumenata s jednog mjesta na drugi vrlo jednostavnim. Proširene mogućnosti za slanje slika, crteža, napisanog teksta predstavljaju samo neke od prednosti koje se postižu raznim mehaničkim uređajima. Danas se koriste i video servisi koji omogućavaju razmjenu videa i zvuka koristeći danas uobičajenu informatičku opremu koju je moguće pronaći na gotovom svakom uredskom stolu.

Osobni „pametni“ telefoni omogućuju nesmetanu komunikaciju neovisno o lokaciji osobe, a smatraju se jednim od najbitnijih telekomunikacijskih dostignuća. Ovi uređaji omogućuju bez ograničavanja kretanja pristup elektroničkoj pošti, porukama, pristup faksu ali i internet servisima, privatnim i javnim bazama podataka.

Internet također predstavlja jedan od načina na koji korisnici diljem svijeta dijele svoje informacije. Mnoge organizacije smatraju internet jedan od najvažnijih načina za oglašavanje i predstavljanje svojih proizvoda, funkcija i djelatnosti dok u isto vrijeme omogućavaju prodaju i primanje povratnih informacija o proizvodu od velike skupine korisnika.

„...*World Wide Web (WWW) je najpopularnije sredstvo tvrtke koje je sada dostupno na internetu. To je posrednik preko kojeg tvrtke mogu predstavljati svoj posao, proizvod i uslugu golemoj i brzo rastućoj bazi korisnika diljem svijeta.*“ (Chopa, Gauri, 2015., 363.)

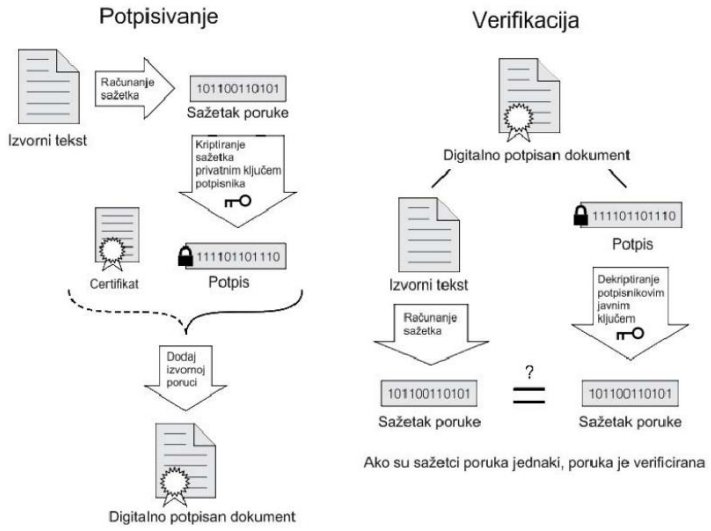
## 2.4. Zaštita uredskih dokumenata

U digitalnom dobu u kojem su dokumenti i razni podaci dostupni velikom broju korisnika koji imaju mogućnost s jednostavnim akcijama podijeliti iste, prema svojim kolegama, vrlo lako može doći do nezakonite ili radi nepažnje, do kršenja autorskih prava i intelektualnog vlasništva. Kako bi se nezakonito dijeljenje podataka u uredskom poslovanju smanjilo, potrebno je dokumente zaštiti. U uredskom poslovanju zaštitu dokumenata moguće je podijeliti na fizičku i elektroničku.

Fizička zaštita dokumenata odnosi se na postupke koji onemogućavaju neautorizirani pristup i dijeljenje fizičkih dokumenata, najčešće u pisanom obliku na papiru. Fizička zaštita dokumenata obuhvaća sustave za zaštitu po pristupa neautoriziranih osoba, kontrolu pristupa, video nadzor ali i sustave za uzbunu i zaštitu prilikom požara, curenje plina i eksplozija. Danas su uredi i poslovni prostori opremljeni velikim brojem uređaja, čitačima za identifikaciju i zabranu pristupa fizičkim dokumentima kao i uređajima koji služe za prevenciju uništavanju dokumenata u slučaju neželjenih događaja.

Elektronička zaštita podataka odnosi se na zaštitu svih digitalnih dokumenata u poslovnim organizacijama. Zaštita digitalnih dokumenata može se odnositi na njihov integritet, autentičnost, odgovornost, tajnost, te izvornost dokumenata. U računalno podržanom uredu postoje razne metode za zaštitu dokumenata kao što su elektronički potpis, kriptiranje, digitalni vodeni žigovi i lozinke. Digitalni potpisi služe kao zamijene za tradicionalni potpis rukom kojim je moguće utvrditi autentičnost dokumenata poput elektroničke pošte, web sjedišta, slika i sličnog. Sama vjerodostojnost potpisanih dokumenata izvršava se upotrebom kriptografije a sastoji se od izračunavanja algoritma i kriptiranja sažetka poruke. Digitalnim potpisom zaštićuje se dokumentna autentičnost, integritet i neporecivost.

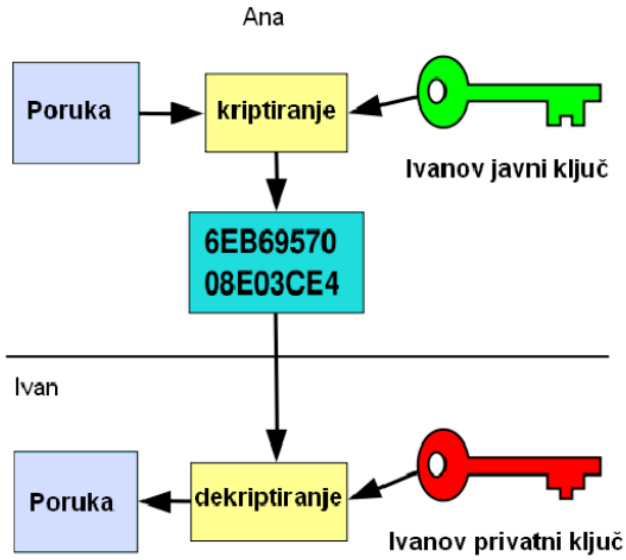
Slika 3. - Proces digitalnog potpisivanja dokumenata




Izvor: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-04-296.pdf (27.5.2018.)

Kriptiranje je jedna od najsigurnijih i najrasprostranjenijih metoda za zaštitu dokumenata na raznim tipovima medija za pohranu digitalnih podataka. Ova metoda vrlo jednostavno omogućuje prebacivanje čitljivog teksta u nejasan, pomoću ključa koji je dostupan samo određenim pojedincima čime se ograničuje pristup osjetljivim podacima. Kriptiranje je također prisutno u porukama, te modernim računalnim operacijskim sustavima koji u većini slučajeva imaju tvornički ugrađene mehanizme za kriptiranje sadržaja. Kriptiranje se može podijeliti prema dva principa rada, simetrični kriptosustav koji za šifriranje i dešifriranje podataka koriste isti ključ, te asimetrični kriptosustav koji se sastoji od ključa koji je korišten za šifriranje sadržaja i javnog ključa.

Slika 4. - Prikaz asimetričnog kriptosustava



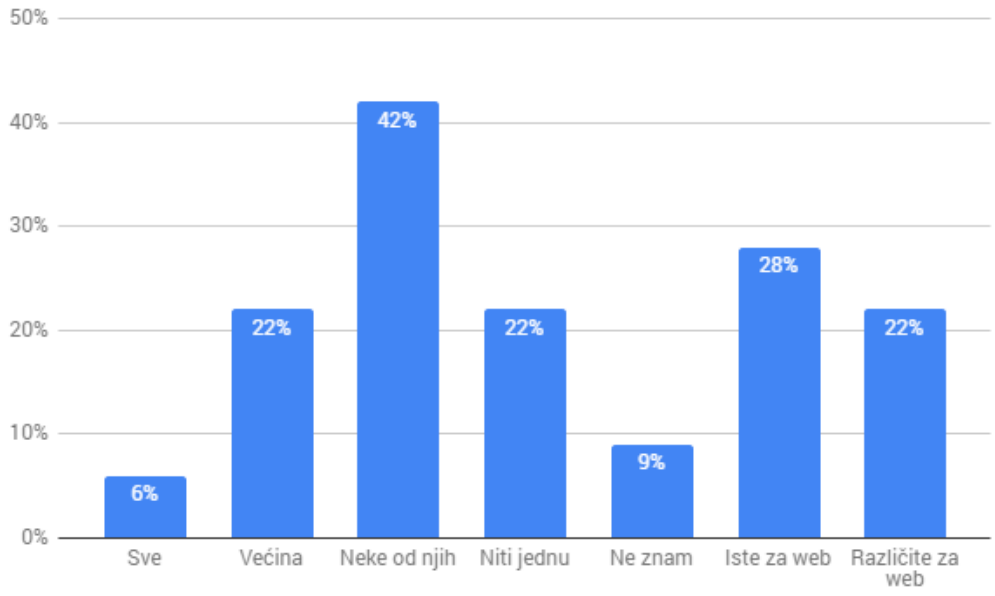

Izvor: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-04-296.pdf (27.05.2018.)

Kako bi organizacije zaštitile svoje podatke ali i potrošače, danas su na snazi razne odredbe i zakoni koji definiraju na koji način je potrebno zaštiti razne podatke koje organizacije čuvaju. Zadnji takva odredba postavljena je od strane Europske Unije, nazvana GDPR (*General Data Protection Regulation*) koja je u primjenu stupila od 25. svibnja 2018. godine. Iako je ova regulativa primarno fokusirana na zaštitu osobnih podataka, također definira elektroničku, fizičku zaštitu podataka i pristupanje prilikom problema curenja podatka.

Prema GDPR-u (European Union, 2018., 3-4.) ako se podaci spremaju u informatičkom sustavu, potrebno je ograničiti pristup datotekama koje ih sadrže, te se preporučuje redovito ažuriranje sigurnosnih postavki sustava. U slučaju fizičkih podataka koji sadrže osobne podatke a pohranjuju se u tvrtki, potrebno je onemogućiti pristup neautoriziranom osoblju koristeći fizičko osiguranje u obliku sefa ili ormara s bravama.

Zaporke predstavljaju još jednu metodu zaštite dokumenata u uredskom poslovanju koje mogu biti postavljene nad određenim dokumentima i pristupnim točkama prema njima. Zaporku je moguće sastaviti od kombinacije raznovrsnih znakova poput slova, brojeva, simbola i sličnog, koje računalo pohranjuje kako bi moglo prepoznati podudaranje, te zatim dozvoliti pristup dokumentima. Zavisno o kombinaciji gore navedenih elemenata zaporke mogu biti vrlo kompliciranе i teške za pogoditi ali i vrlo jednostavne ako ih se ne shvati ozbiljno, čime je moguće ugroziti organizaciju i njene podatke.

Slika 5. - Broj istih zaporki na različitim online računima u 2017. godini

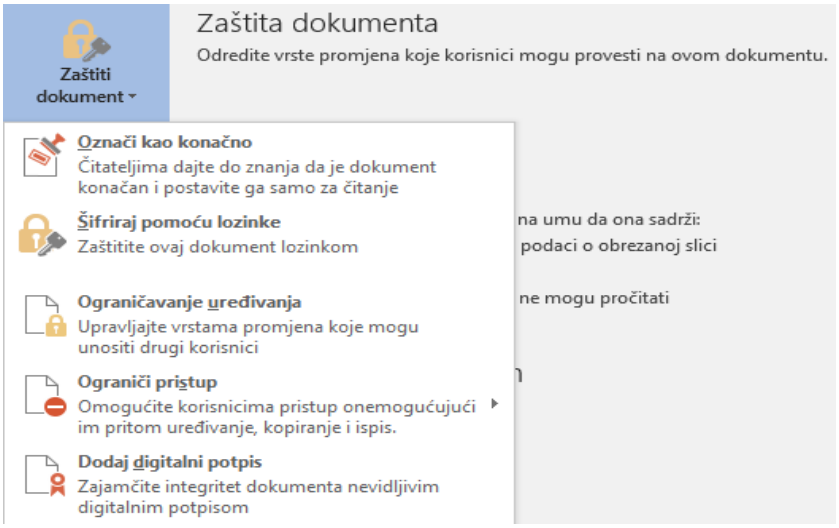



Izvor: obrada autora prema https://www.statista.com/statistics/763091/us-use-of-same-online-passwords/ (27.5.2018.)

Osim prije navedenim zasebnim mehanizmima koje je moguće postaviti nad raznim dokumentima, postoje i programski paketi poput Microsoft Office i Open Office-a koji među

svojim ugrađenim funkcionalnostima omogućuju zaštitu dokumenata pomoću enkripcije, zaporke za ograničavanje izmjene i digitalnih potpisa. Programski paketi ovoga tipa upravo se najviše koriste za obradu podataka i dokumenata u uredskom poslovanja. Upravo ovakvi paketi koriste se u najrasprostranjenijem operacijskom sustavu Windows koji se koristi diljem svijeta u uredskom poslovanju.

Slika 6. - Zaštita Word 2016 dokumenta




Izvor: autor

Uz Microsoft Office alate, PDF (*Portable Document Format*) dokumenti spadaju pod jedne od najraširenijih i korištenijih formata za spremanje dokumenata, a sadrži funkcionalnosti poput zaštite dokumenata od kopiranja teksta i njegovog uređivanja. Specifičnost PDF datoteka proizlazi iz svojstva kriptiranja sadržaja dokumenta prilikom kojega se provjerava skupina oznaka koje određuju pravila tj. mogućnosti manipulacije sadržajem. PDF koristi asimetričan kriptosustav s dva ključa.

Danas uz sve poznate mehanizme zaštite dokumenata i podataka, i dalje nerijetko zbog ljudskih pogrešaka dolazi do slučajnog ili namjernog curenja podataka u javnost, te kako bi se takvi slučajevi smanjili, treba koristiti razne ili više raznih mehanizama za zaštitu digitalnih dokumenata kao i savijete stručnjaka za zaštitu podataka.

# 3. Digitalna forenzika

Digitalna forenzika jedan je od grana forenzičkih znanosti koja se bavi identifikacijom, prikupljanjem i analizom računalnih tj. digitalnih dokaza tako da budu valjani za prezentaciju na sudu.

*„Computer Forensic is about evidence from computers that is sufficiently reliable to stand up in court and be convincing.“* (River, 2005., 3.)

Riječ forenzika potječe iz latinskog pridjeva „*forensi*“ koje ima značenje „pred forumom“ odnosno „pred sudom“, a u literaturi danas moguće je naići na nazive poput računalne forenzičke analize, elektroničke istrage, digitalne forenzike, digitalne analize i sličnog. Velika raznolikost naziva nastala je kao posljedica nagle digitalizacije i informatizacije svih grana društva. Razvoj računalne forenzike započeo je 1980-tih godina kada je FBI (*The Federal Bureau of Investigation*) osnovao CART (*Computer Analysis and Response Team*) ured. Njegova uloga je bila prikupljanje digitalnih dokaza i obrada istih iz raznih istraga koje su uključivale računala, odnosno digitalne dokaze. (Mohay et al., 2003., 114.)

Danas se zbog korištenja računala u kriminalne svrhe digitalna forenzika znatno razvila i proširila. Razvitak udruga i zajednica, te pojava specijaliziranih programa i komponenti omogućili su nagli razvoj ove znanosti kako bi se računalni kriminal mogao otkriti i kazniti. Kada se govori o granama forenzike postoje mnoge podijele ove znanosti u stručnoj literaturi, a razvoj novih tehnologija dodatno proširuje postavljeni skupu grana. (River, 2005., 4.; CERT, 2010.; Volonino, Anzaldua, 2008., 151.)

Računalnu forenziku tako je moguće podijeliti na četiri osnovne grane koje su uzajamno povezane:

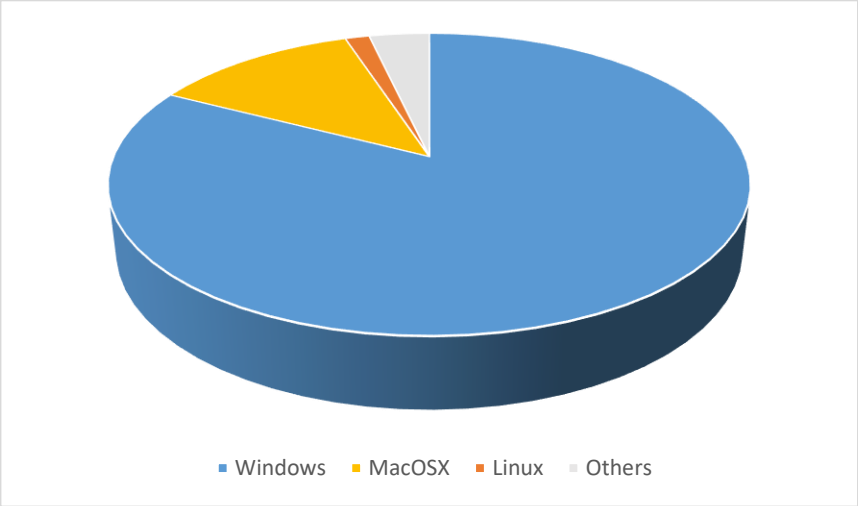
- Forenziku podataka
- Mrežnu forenziku
- Forenziku mobilnih uređaja
- Forenziku računalne pošte

## 3.1. Forenzika podataka

Forenzika podataka odnosi se na sve radnje kojima je cilj prikupiti i analizirati podatke koji su izgubljeni ili skriveni. U Windows operacijski sustavi kroz godine razvoja integrirani su razni alati i podsustavi koji bilježe i spremaju određene podatke kako bi korisnik imao bolje iskustvo prilikom korištenja ovog operacijskog sustava. Osim navedenog razni mediji za pohranu podataka sadrže mehanizme koji im omogućavaju pravilno funkcioniranje i spremanje podataka. Ovakvi korisniku prikriveni podaci jedni su od načina na koji digitalni forenzičari prikupljaju dokaze protiv kriminalnih radnji. Iskustvom i poznavanjem operacijskih sustava i njegovih mehanizama forenzičari imaju mogućnost da prikupe digitalne dokaze, pretražuju i povrate izbrisane podatke, pregledaju neodijeljen prostor, radnu memoriju, te razne druge artefakte.

Windows operacijski sustav najčešće se upotrebljavaju od strane korisnika radi svojeg jednostavnog sučelja i interakcije, a isto vrijedi i za slučaj uredskog poslovanja. Poznavanjem ovog operacijskog sustava omogućava forenzičarima pronalazak različitih podataka i dokumenata iz uredskog poslovanja i popratnih alata.

Slika 7. - Svjetski tržišni udio operacijskih sustava za siječanj 2018. godine




Izvor: obrada autora prema https://www.statista.com/statistics/218089/global-market-share-of-windows-7/ (29.5.2018.)

Podaci koje Windows operacijski sustav sprema, a prati radi unaprijeđena korisničkog iskustva i pravilnog rada u svijetu računalne forenzike nazivaju se Windows artefakti.

„...*Windows artefakti, u računalnoj forenzici, su dokazni podaci koje automatski sprema operacijski sustav Windows kao rezultat interakcije s računalom.*“ (IACIS, 2017., 444.)

Na prvi pogled izbrisane datoteke mogu se nalaziti u košu za smeće, te u priručnoj memoriji. Analizom neodijeljenog prostora, koji se smatra praznim za zapisi novih podataka od strane sustava, moguće je otkriti i povratiti podatke koji su preostali u ovom prostoru nakon brisanja. Izbrisani podatke moguće je naći i u prostorima pojedinih klastera na medijima za spremanje podataka. U slučaju NTFS (*New Technology File System*) datotečnog sustava minimalna veličina klastera iznosi 4 kilobajta, te ako se radi o zapisivanju datoteke koja ne popunjava cijeli klaster, postoji šansa da ostatak službeno slobodnog prostora sadrži stare neobrisane podatke. Ovaj specifični slučaj omogućen je načinom na koji NTFS radi, odnosno običnim brisanjem podataka, oni se zapravo ne brišu već se mijenja atribut koji definira zauzet i slobodan prostor. Stvarni podaci i dalje se nalaze na mediju ali sustav sljedeći put ima dozvolu da preko postojećih podataka zapiše nove. (Microsoft, 2015.; CIS, 2015.; IACIS, 2017., 458-465.)

Kada se govori o nedostupnom prostoru, pod njime se podrazumijeva svaki prostor kojem operacijski sustav poput Windowsa, nema pristup. Ovakav prostor većinom je zauzet ključnim mehanizmima koji omogućuju rad samih uređaja poput tvrdog diska. Uz pomoć posebnih forenzičkih programa ovakvom prostoru i njegovim podacima moguće je pristupiti.

U slučaju kada je računalo koje se analizira upaljeno, potrebno je prije isključivanja poduzeti sve mjere opreza kako bi podaci u radnoj memoriji bili sačuvani. Hvatanje odnosno kopiranje radne memorije jedan je od prvih koraka koje je prilikom upaljenog računala potrebno izvršiti iz razloga što se svi podaci iz ove memorije brišu u trenutku gašenja računala ili gubitka struje. Ovakvi podaci tako su limitirani samo na podatke od zadnjeg gašenja ali danas sve većim kapacitetom radne memorije moguće je prikupiti veliki broj podataka koji mogu pojednostavniti istragu u slučaju enkripcije ili drugih sigurnosnih metoda.

Windows registri predstavljaju bazu podatka u kojima se nalaze razne informacije koje operacijski sustav čuva kako bi personalizirao sustav određenom korisniku.

„*Središnja hijerarhijska baza podataka koja se koristi u Microsoftu... koristi se za pohranu podataka potrebnih za konfiguriranje sustava za jednog ili više korisnika, aplikacija i komponenti uređaja.*“ (IACIS, 2017., 566.)

U ovoj bazi moguće je pronaći sistemske postavke, informacije o komponentama, lozinke, aplikacijske podatke i mnoge druge. U registrima se mogu naći zapisi o korisničkim radnjama poput upisanih URL (*Uniform Resource Locator*) adresa, MRU (*Most Recently Used*) lista, lozinke i druge korisne informacije. Ova baza također sprema i specifične sistemske informacije poput mrežnih postavki, vremenske zone, registriranog vlasnika uređaja, vremena zadnjeg gašenja i informacija o komponentama. Sa strane aplikacija također se spremaju specifične informacije kao što su njihove lokacije u sustavu, koliko su puta pokrenute, kada su prvi puta prepoznate na sustavu i slično. (CIS, 2015.; IACIS, 2017., 566.)

Jedan od problema danas je veliki broj raznovrsnih verzija operacijskih sustava koji mogu predstavljati problem prilikom istrage ili korištenja specifičnih alata. Različite verzije sustava poput Windows XP, Viste, 7, 8, 8.1 i 10 na prvi pogled možda ne izgledaju toliko različito, no način funkcioniranja i spremanja određenih podataka je promijenjen kroz ove operacijske sustave čime može doći do krivog tumačenja ili ne pronalaska određenih podataka s alatima koji nisu redovno ažurirani. Prije svake forenzičke istrage nužno je testirati forenzičke alate u poznatom okruženju kako bi se utvrdilo da alati rade kako bi trebali.

„*U području digitalne forenzike validacija je postupak potvrde da nešto funkcionira kako se očekuje da će funkcionirati. U svakom djelu svog rada računalni forenzičar mora voditi brigu da osobno ispita i potvrdi.*“ (IACIS, 2017., 382.)

## 3.2. Mrežna forenzika

„*Mrežna forenzika općenito se odnosi na prikupljanje, spajanje i analizu informacija na mrežama*.“ (Mohay et al., 2003., 322.)

Mrežna forenzika uključuje analizu mrežne infrastrukture za koju postoji mogućnost da je iskorištena za kriminalnu radnju. Prilikom izvođenja forenzičke analize na mrežnoj infrastrukturi, forenzičari nerijetko nailaze na probleme višestrukih vremenskih zona i nadležnosti. Problem nastaje kada istražitelj treba prikupiti dokaze s različitih mjesta, odnosno država koji nemaju iste zakone.

„*Mreže su veze velike propusnosti, što mrežnu forenziku čini izazovom. Pronalaženje odgovarajućeg mrežnog forenzičkog alata za specifičnu situaciju može biti teško, ali nije nemoguće ako imate dobre smjernice.*“ (Volonino, Antaldua, 2008., 241.)

Programi kojima se prikupljaju digitalni dokazi u trenutnom vremenu nemaju mogućnost obrade velike količine podataka. Također postoji i izazov praćenja osobe koja napad izvršava putem IP adrese, te praćenja kretnji putem specijaliziranih programa za mapiranje lokacija s kojih se napadalo. (Mohay et al., 2003., 322-323.)

Kako bi forenzičar prikupio što više dokaza mora dobro poznavati mrežnu opremu, princip na kojem ona radi, te na kojim se mrežnim uređajima mogu naći određeni dokazi. Mrežna oprema koja se analizira je računalo domaćin na kojem je moguće pronaći dokaze forenzikom podataka tvrdog diska, radne memorije i ostalih artefakata. Usmjeritelj sprema podatke o greškama koje su se desile prilikom usmjerivanja, te sumnjive aktivnosti. Usmjeriteljev primarni zadatak je pomicanje podataka između mreža, te je na njemu moguće pronaći zapise o pogreškama i detaljima statusa komponenti. Ovaj uređaj također čuva tablice s IP i MAC (*Media Access Control*) adresama. Vatrozid pohranjuje detaljne zapise aktivnosti sustava kao i zapise prepoznatih napada, ispalih paketa i programa kojima je dopuštena komunikacija preko vatrozida. Također vatrozid zapisuje sve sumnjive aktivnosti i potencijalne napade. U CAM (*Content Addressavbe Memory*) memoriji preklopnika mogu se pronaći podaci o MAC adresama koji su povezani za određene portove, kao i informacije o

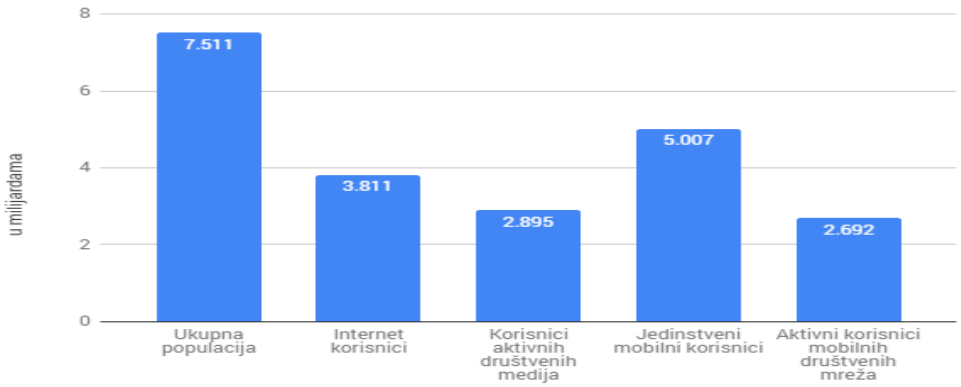
virtualnim lokalnim mrežama. Preklopnici nemaju procesnu snagu niti puno memorije ali su korisna platforma za kopiranje mrežnog prometa u istom trenutku koji spada pod jednu od ključnih zadataka mrežne forenzike. (CIS, 2015.; Volonino, Antaldua, 2008. 242-244.)

### 3.3. Forenzika mobilnih uređaja

Forenzika mobilnih uređaja obuhvaća bežične prenosive uređaje kao što su mobiteli, pametni mobiteli, auti, digitalne kamere, GPS (*Global Positioning System*) uređaji, tableti ali i mrežne tehnologije koje se danas na ovim uređajima upotrebljavaju. Ovi uređaji ne moraju uvijek biti direktno korišteni u kriminalnim radnjama već se mogu koristiti za planiranje i komunikaciju između sudionika. Prilikom analize ovakvih uređaja forenzičari nailaze na još veću raznolikost uređaja nego u slučaju osobnih računala. Uz to nailaze na probleme jer forenzički alati ne mogu uvijek izvući sve podatke i ne podržavaju sve mobitele. Priključak za punjenje mobitela, operacijski sustav, funkcionalnosti mobitela, nepodržani znakovi i slično mogu predstavljati neprebrodiv izazov za forenzičare ako nisu prilagođeni za specifični model mobitela nad kojim je potrebno izvršiti analizu.

Kao i osobna računala, današnji mobiteli također imaju operacijske sustave poput Androida i iOS-a koji omogućuju veliki broj funkcionalnosti. Ovi sustavi također spremaju razne korisničke podatke kako bi personalizirali i poboljšali korisnikovo iskustvo.

Slika 8. - Pregled korištenja mobitela u svijetu




Izvor: obrada autora prema https://thenextweb.com/contributors/2017/06/14/global-digital-stats-june-2017-facebook-active-users-decline-mobile-usage-hits-5-billion/ (30.5.2018.)

Kako bi se raznovrsni pametni mobiteli i mobilna tehnologija mogli koristiti i spojiti na sustav GSM-a (*Global System for Mobile communications*) potrebno je zadovoljiti uvijete za spajanje. Jedan od takvih uvjeta je i ICC-ID (*Integrated Circuit Card Identifier*) broj koji je programiran prilikom proizvodnje od strane proizvođača. Ovaj jedinstveni broj omogućuje forenzičarima da otkriju pozivni broj zemlje, pružatelja usluge i serijski broj. Još jedan takav broj je IMSI (*International Mobile Subscriber Identity*) koji predstavlja identifikacijski broj pretplatnika na GSM mreži, a nalazi se na SIM (*Subscriber Identity Modul*) kartici gdje je zaštićen PIN (*Personal Identification Number*) brojem. IMEI (*International Mobile Equipment Identity*) predstavlja jedinstveni broj koji ima svaki GSM mobitel, a postavljen je od strane proizvođača. U trenutku prvog paljenja mobitela, ovaj broj je proslijeđen pružatelju mobilnih usluga gdje se broj provjerava u registru. IMEI broj u sebi sadrži informacije poput internacionalnog pozivnog broja, proizvođačevog finalnog identifikacijskog koda, serijskog broja uređaja i softverske verzije. Ovakvi podaci koji su prisutni na svakom mobilnom uređaji znatno pomažu prilikom forenzičke analize tako da je njima moguće utvrditi početne informacije o uređaju. (Metropolitan Police, 2015., 11-14.)

Neke od mjera koje forenzičari trebaju poduzet kako bi zaštitili podatke na mobilnim uređajima su uključivanje zrakoplovnog rada, odnosno isključivanje mrežnih podataka kako udaljeni pristup uređaju i brisanje podataka ne bi moglo biti pokrenuto. Ako je mobilni uređaj uključen, a opciju za uključivanje zrakoplovnog rada nije dostupna, forenzičari što prije moraju izolirati uređaj pomoću posebnih vreća i torba koje blokiraju komunikaciju s uređajem. Da bi se sačuvao pristup mobitelu u slučaju nepoznate zaporke, moguće ga je s prijenosnom baterijom zadržati upaljeno prilikom transporta do adekvatne opreme u laboratoriju.

### 3.4. E-mail forenzika

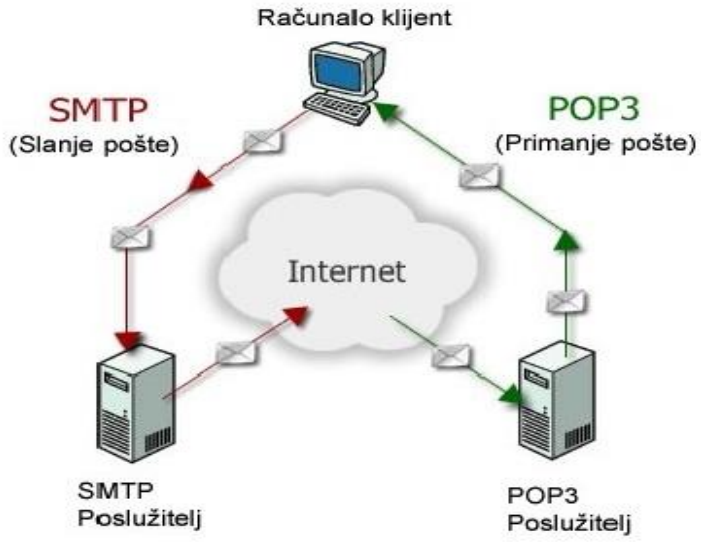
Računalna pošta danas predstavlja jedno od glavnih tehnologija za komuniciranje u svakodnevnom privatnom ali i poslovnom životu ljudi pružajući forenzičarima veliki broj mogućih dokaza putem artefakata nastalim iza računalne pošte i web preglednika.

U slučajevima poput prijetnji, napastovanja i prijevara računalna pošta može biti primarni dokazni materijal, dok se u nekim slučajevima može koristiti kao komunikacijsko sredstvo ili sredstvo potpore drugih dokaza u slučaju hvaljenja o kriminalnoj radnji ili planiranju. Dokazi sadržani u računalnoj pošti moguće je zbog svoje prirode naći na raznovrsnim lokacijama kao što su lokalni uređaji, lokalni serveri na LAN-u (*Local Area Network*), mobilnim uređajima, PDA (*Personal Digital Assistant*) uređajima, kao i na serverima poslužitelja.

„*Forenzički istražitelj mora moći identificirati računalnu poštu kao važan čimbenik u istrazi, utvrditi gdje se nalaze dokazi, kako se dokumenti pohranjuju, koji su alati potrebni za pregled i izvoz dokaza i kako ih predstaviti osobi zaduženoj za slučaj*.“ (IACIS, 2017., 957.)

Računalna pošta je format elektroničke poruke poslan s jednog računala na drugi koristeći više protokola za uspješno pristizanje poruke. SMTP (*Simple Mail Transfer Protocol*) jedan je od protokola koji šalje računalnu poštu s korisnikovog klijenta prema serveru pružatelja internet usluge. Ovaj proces odvija se preko mreže sa SMTP protokolom koji postavlja pravila komunikacije između svih točaka. Završni stanica je prijamnikov email server koji pohranjuje elektroničku poštu dok nije preuzeta, te zatim POP (*Post Office Protocol*) preuzima kontrolu nad posljednjim dijelom. (IACIS, 2017., 958.)

Slika 9. - Proces slanja računalne pošte




Izvor: https://image.slidesharecdn.com/smtppope-mailprotokol-091207150155-phpapp01/95/email-protokol-9-728.jpg?cb=1260198145 (05.5.2018.)

Ovaj protokol omogućuje korisničkom sustavu da pristupi i preuzme elektroničku poštu sa servera. Umjesto POP protokola danas se također koristiti i IMAP (*Internet Message Access Protocol*) protokol koji omogućuje klijentu da pristupa i manipulira elektroničkom poštom na serveru. Ovaj protokol ima prednosti poput kreiranja mapa za pohranu i prebacivanje poruka. Za razliku od POP-a poruke ostaju na serveru dok ih korisnik ne izbriše. IMAP također podržava i izvanmrežni način rada koji omogućuje rad s elektroničkim porukama iako klijent na računalu nije povezan sa serverom. U trenutku kada se veza uspostavi, sve promjene su s klijenta prenose se na serversku stranu. (IACIS, 2017., 959.)

Korisnici interneta danas svojoj računalnoj pošti mogu pristupiti i putem web-a koristeći neki od danas popularnih web preglednika kao što su Internet Explorer, Firefox, Mozilla i Google Chrome. Poslane poruke i dalje će slijediti SMTP procedure, a većina web računalnih računa dopuštaju korištenje POP i/ili IMAP-a za pristup izvan servera. Korištenje web preglednika za pristupa računalnoj pošti ostavlja razne podatke na računalu korisnika. Preglednici u operacijskom sustavu Windows pohranjuju razne datoteke, te i sam sustav prati određene aktivnosti. Uz navedeno i server pohranjuje razne zapise o korisnicima i računalnoj pošti koji mogu biti vrijedni dokazi ako se uspostavi pravovremeni kontakt s poslužiteljem, te se dokazi sačuvaju. (IACIS, 2017., 959.; CIS, 2015.)

# 4. Forenzička istraga

Cilj istražitelja koji izvodi forenzičku istragu je da prikupi, analizira i po potrebi, na sudu, prezentira svoje pronalaske. Pošto je svaki slučaj drugačiji i može se razlikovati prema prirodi kriminalnog dijela, jedinstveni princip i model za sve slučajeve ne postoji već je potrebno napraviti pripremu i analizu prilagođenu za pojedinačni slučaj. Zavisno od slučaja mogu se pronaći raznovrsni kriminalni elementi i podaci pohranjeni na različite načine ovisno o uređajima i operacijskim sustavima prisutnim kod počinjenja kaznenog dijela.

„*Cilj bilo koje istrage je otkrivanje i predstavljanje istine.*“ (Eoghan Casey, 2011., 187.)

Kako bi forenzička istraga mogla započeti potrebno je prvo doći do počinjenja kriminalne radnje, te netko treba slučaj i prijaviti. Tek tada forenzički istražitelji mogu započeti s detaljnom forenzičkom istragom.

Slika 10. - Faze računalne forenzike


Izvor: autor

Jedno od ključnih koraka prilikom svake forenzičke analize je proces zapisivanja koraka provedenih prilikom istrage. Prilikom svih navedenih faza forenzičke istrage istražitelj se mora zapitati i zabilježiti:

- Što sam promatralo?
- Koje korake sam napravio?
- Kada sam ih napravio?
- Zašto sam ih napravio?

Ključno pitanje koje se postavlja je zašto se određeni korak napravio, kako bi se u slučaju preispitivanja istražitelja na sudu, mogli opravdati postupci. Prilikom prezentacije dokaza na

sudu, sudac i porota mogu preispitati određene postupke, te na postavljena pitanja treba dati opravdani odgovor kako bi dokazi bili uvaženi od strane suda.

„*Suđenje može nastupiti mjesecima, ako ne i godinama nakon što izvršite forenzičku istragu.*“ (IACIS, 2017., 1041.)

Uz navedeno, detaljne zabilješke rade se kako bi se određeni postupci mogli ponoviti. Zabilješke moraju biti dovoljno detaljne kako bi drugi forenzičari mogli, koristeći iste postupke, programe i podatke, dobiti jednake rezultate. Nemogućnost rekonstrukcije forenzičke istrage u najgorem slučaju mogu dovesti do odbacivanja prikupljenih dokaza na sudu.

Kao pomoć pri pravilnom postupanju s digitalnim dokazima prilikom forenzičke istrage, danas se koriste mnogi vodiči za istražitelje, te su definirana četiri ključna načela prilikom rada s digitalnim dokazima:

- Načelo 1: Sve radnje od strane provoditelja zakona nad dokazima ne smiju izmijeniti prikupljene podatke koji bi mogli biti korišteni na sudu.
- Načelo 2: U trenucima kada je potrebno pristupiti izvornim podacima, osoba koja izvršava ovaj postupak mora biti iskusna i sposobna obrazložiti svoje radnje.
- Načelo 3: Zapisi ili snimke svih provedenih radnji nad digitalnim dokazima moraju biti sačuvani. Treća neovisna strana mora mogući rekonstruirati proces istrage i dobiti iste rezultate.
- Načelo 4: Osoba zadužena za vođenje istrage ima sveukupnu odgovornost za provođenje istrage u skladu s ovim načelima i zakonima.

### 4.1. Priprema za forenzičku istragu

Upravo zato što ne postoje dva jednaka slučaja, faza pripreme za forenzičku istragu ključni je prvi korak koji istražitelj mora napraviti. Istražitelj prvo mora prikupiti informacije o slučaju, kakve digitalne dokaze je moguće pronaći, kakva su legalna ograničenja, te tko su sumnjivci i kakva je njihova uloga. Razgovor s policijskim detektivom, policijski izvještaji,

informatičko osoblje i slike dostupni su izvor informacija koji će biti korisni za razumijevanje slučaja.

Slika 11. - Dio standardne forenzičke oprema


Izvor: autor

Istražitelj također mora biti upoznat s nalogom i važećim zakonima za oduzimanje dokaza, pod čijom nadležnosti se oduzimanje izvršava, te kojim podacima istražitelj smije pristupiti. U Republici Hrvatskoj zakonom o kaznenom postupku definiran je elektronički digitalni dokaz, te pravilno postupanje s takvom vrstom dokaza.

„*Pretraga pokretnih stvari obuhvaća i pretragu računala i s njim povezanih uređaja, drugih uređaja koji služe prikupljanju, pohranjivanju i prijenosu podataka, telefonskim, računalnim i drugim komunikacijama i nositelja podataka. Na zahtjev tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu ili drugom uređaju ili nositelju podataka, te davatelj telekomunikacijskih usluga, dužni su omogućiti pristup računalu, uređaju ili nositelju podataka, te dati potrebne obavijesti za nesmetanu uporabu i ostvarenje ciljeva pretrage.*“ (NN, 2017.)

Jedna od pozitivnih navika prije početka svake istrage je pregledavanje naloga za slučaj. Nalozi mogu sadržavati razna ograničenja prilikom pretraživanja dokaza koji ako se prekrše mogu dovesti do odbacivanja dokaza na sudu. Forenzičar mora biti u stanju, ukoliko naiđe na ograničenja u nalogu, razviti strategiju kako raditi unutar njih i izvršiti istragu. Prilikom pripreme za istragu istražitelj koji izvršava forenzičku analizu može utvrditi vremenski okvir

počinjenja kriminalnog dijela iz prikupljenih informacija čime se nerelevantni podaci mogu isključiti iz istrage i time uštedjeti dragocjeno vrijeme. Prikupljene informacije mogu se koristiti i za postavljanje specifičnih filtera nad podacima i tipovima podataka kako bi se ponovno isključile datoteke koje nisu u okviru slučaja. Vrlo veliku vrijednost imaju korisnička imena i lozinke koje je moguće dobiti od sumnjivca ili pronaći na mjestu zločina na raznim oblicima za zapisivanje informacija. (IACIS, 2017.)

„*Morate znati postoje li neka ograničenja koja vam je sud nametnuo kao što je samo mogućnost gledanja slika, a ne dokumenata ili tablica, te ispituje li se samo jedan korisnički račun.*“ (IACIS, 2017., 338.)

Forenzičar mora biti u stanju prema svojim sposobnostima i iskustvu procijeniti svoju kompetentnost za obavljanje istrage. Snalažljivost i različiti pristupi rješavanju slučaja omogućuju forenzičarima da riješe i najkompliciranije zločine koristeći raznovrsna forenzička pomagala, te time prikupe dokaze potrebne za sudski proces.

### 4.2. Identifikacija dokaza

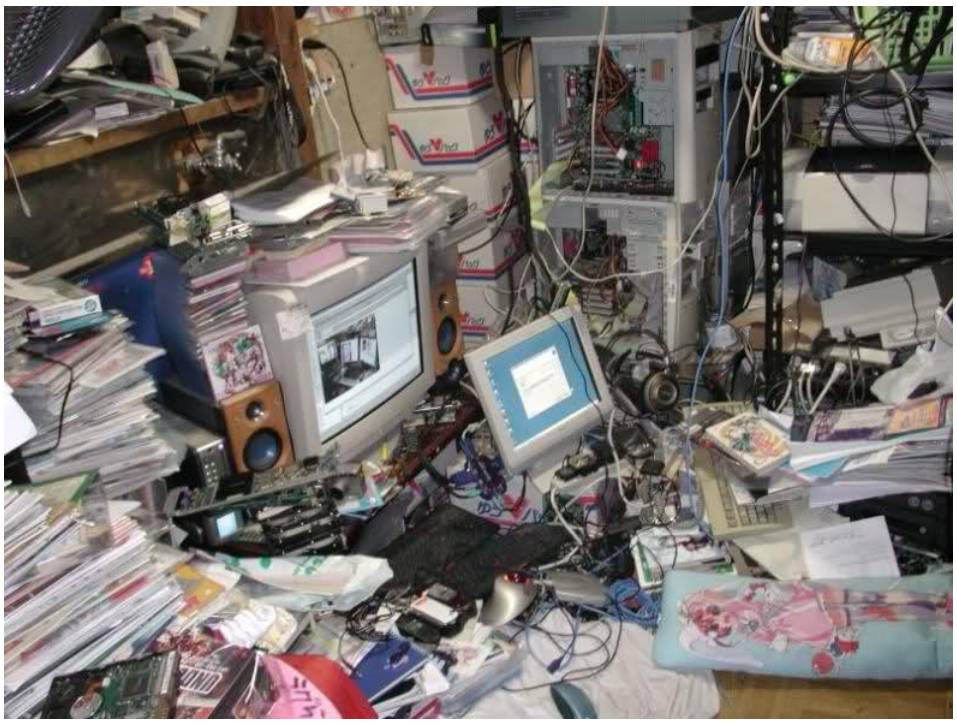
Ključno je da forenzičari prilikom dolaska na mjesto zločina utvrde koji računalni uređaji mogu biti izvor potencijalno korisnih dokaza. Pogreške prilikom ovog korak omogućuju obrani da prilikom sudskog procesa napadnu slučaj na tehničkoj bazi i preispitaju način na koji je forenzička istraga izvršena. Samo mjesto zločina ili prostor u kojem se izvršava istraga može biti vrlo neuredan i kompliciran zavisno o tipu slučaja. Prikupljanjem svih propisanih dopuštenja, istraga može uključivati privatne prostore sumnjivca ali i poslovni prostor. (Eoghan Casey, 2011.)

„*Povećanje broja digitalnih uređaja i napredak u digitalnoj komunikaciji znače da su digitalni dokazi sada prisutni ili potencijalno prisutni u gotovo svakom zločinu.*“ (ACPO, 2012., 7.)

Danas je digitalne dokaze moguće pronaći u gotovo svakom računalnom uređaju. Lociranje i poznavanje takvih uređaja omogućuje forenzičarima da pravilno i detaljno

pretraže prostor u potrazi za takvim uređajima. Digitalne dokaze moguće je pronaći na raznim lokacijama kao što su potrošački uređaji poput osobnog računala, mobitela, pametnog mobitela, GPS sustava, USB (*Universal Serial Bus*) uređaja, digitalne kamere i sličnog. Osim na fizičkim uređajima, dokaze je moguće naći na web sjedištima i socijalnim mrežama, forumima i grupama za vijesti kada se radi o javnim vanjskim resursima, te u slučaju privatnih vanjskih resursa u zapisima internet poslužitelja, korisničkim aktivnostima, pozivima i računalnoj pošti. Za pristup vanjskim resursima je potrebno imati odgovarajući nalog čime su pružatelji ovakvih usluga dužni omogućiti pristup potrebnim podacima. Sve popularnije lokacija digitalnih dokaza trenutno su pametni mobilni uređaji koji mogu sadržavati mobilne poruke, pozive, računalne poruke i internetske razgovore. Upravo zbog povećanja prisutnosti digitalnih dokaza, od strane agencija i policije razvijaju se standardne procedure za pristupanja mjestu zločina s digitalnim dokazima, te vodiči kako njima postupati. (Williams, 2012., 25.)

Slika 12. - Izazovi identificiranja digitalnih dokaza



Izvor: http://cdn2.hubspot.net/hub/189007/file-969200778-jpg/online-storage-will-be-nice.jpg (05.6.2018.)

Prilikom dolaska na mjesto počinjenja kriminalne radnje ili lokacije mogućih dokaza moguće je naići na računala u tri različita stanja. Ako je računalo isključeno, istražitelj ga ne smije paliti jer bi paljenje ugašenog računala izmijenilo više različitih podataka u datotekama koje sustav sprema. Forenzičar u ovom slučaju treba isključiti priključak za struju sa zadnje strane računala, a ne iz zida. Drugo stanje računala izgleda kao da je isključeno, no zapravo je u stanju mirovanja ili npr. ekran nije spojen. Uvijek je potrebno detaljno provjeriti u kojem se stanju računalo nalazi pomoću signalizacijskih svjetla, vanjske periferije, zvuka ventilatora i slično. Kako bi se sa sigurnošću utvrdilo da računalo nije u stanju mirovanja, forenzičari pomicanjem miša ili pritiskom na tipku „Shift" mogu provjeriti da li je računalo stvarno isključeno. Prilikom zadnjeg stanja u kojem je računalo uključeno, prvi korak je udaljavanje svih ljudi iz blizine računala, te često zatim slijedi slikanje svega prisutnog na zaslonu. Kod ovog stanja moguće je izvršiti tehniku prikupljanja dokaza s upaljenog računala s minimalnim izmjenama koja se zove *triage*. U bilo kojem stanju računala, odgovornost prvog istražitelja je udaljavanje svih prisutnih od računala i njegovo osiguravanje. Nerijetko se unazad par godina mogu naći primjeri nepažnje istražitelja gdje su osumnjičenici pokušali i uspjeli izbrisati dokaze na računalu, isključiti struju a time i računalo ili uništiti medije za spremanje podataka. (Volonino, Anzaldua, 2008.; R. Vacca, 2005., CERT, 2015.; IACIS, 2017., 320-321.)

Korištenje standardnih operacijskih procedura u digitalnoj forenzici daje istražiteljima smjernice kako identificirati, prikupiti i analizirati određene uređaje, te kako sačuvati dokaze tako da budu prihvaćeni u sudskom procesu.

### 4.3. Prikupljanje i očuvanje dokaza

„*Kako bi se sačuvali podaci i prikupili najbolji dokazi, ovi predmeti moraju se na odgovarajući način obrađivati i zaplijeniti, te ih trebati tretirati jednako pažljivo kao i svaku drugu stavku koja se mora forenzički ispitati.*" (Williams, 2012., 30.)

Prilikom prikupljanja dokaza forenzičari moraju koristiti odgovarajuće tehnike za uspješno prikupljanje dokaza bez izmjenjivanja i njihovog uništavanja. Računalo je potrebno isključiti s mreža kako ne bi došlo do vanjske komunikacije i promjene podataka. Uz

navedeno potrebno je zabilježiti i locirati položaj svih kablova, prikupiti informacije o proizvođaču, modelu i serijskom broju sistema. Prikupljanje fizičkih dokaza također je ključno za istragu. Pronađene zabilješke, papiri i upute za korištenje mogu sadržavati korisne informacije za istragu.

„*Nemojte samo uzeti kućište računala i ostaviti monitor, tipkovnicu i ostalu periferiju. Ta smiješna kutija pokraj računala može biti vanjski uređaj za pohranu koji je bitan za ponovno rekonstruiranje računala i dokazivanje kasnije.*“ (IACIS, 2017., 328.)

Ako je potrebno forenzičari s mjesta zločina mogu uzeti i popratne uređaje za čitanje danas ne standardnih medija poput disketa i magnetskih vrpci. Sve oduzete elektroničke uređaje potrebno je obilježiti kako bi se prilikom dolaska u forenzički laboratorij moglo izvršiti rekonstruiranje sustava, ako je to potrebno. Prilikom pakiranja za prijevoz, dokazi moraju biti pravilno zaštićeni kako ne bi došlo do oštećenja. Mjere opreza poput dodatnog pakiranja i zaštitnih slojeva prilikom prevoženja monitora, tvrdog diska, računala i drugih popratnih komponenti dio su standardne procedure. Fizičko oštećenje osjetljivih mehaničkih komponenti npr. tvrdog diska najvjerojatnije će rezultirati uništavanjem svih dokaza na njemu. Osim fizičkih oštećenja dokaze treba zaštiti od vlage, elektromagnetskih valova, ekstremno niskih ili visokih temperatura i štetnika. Za spremanje elektroničkih uređaja potrebno je koristiti isključivo papirnate vrećice, kartonske kutije ili anti-statične torbe. (IACIS, 2017., 328-329.)

„*Ne možete raditi s izvornim materijalom, tako da morate stvoriti točan fizički duplikat. Stvaranje forenzičke kopije naziva se akvizicija.*“ (IACIS, 2017., 330.)

Forenzička kopija predstavlja identičnu kopiju tvrdog diska ili nekog drugog medija pošto nastaje kopiranjem bita po bita s originalnog dokaza na čisti forenzički sterilan medij. Dobra praksa je izrada minimalno dvije kopije originalnog medija. Prva kopija koristi se za forenzičku analizu dok se druga najčešće odmah pohranjuje u arhivu. Prilikom izrade ovakvih kopija koriste se uređaji nazvani *write-blocker*s kojima se omogućuje samo čitanje podataka. Korištenjem ovih uređaja fizički je onemogućena namjerna ili slučajna izmjena dokaza, a danas se smatraju standardnom forenzičkom opremom.

Slika 13. - Uređaja za onemogućavanje zapisivanja


Izvor:
https://bounga.sg/sites/bounga.sg/files/styles/semi_large__360x360_/public/field/image/tableau-t9-1.png?itok=vhb6bCgS (05.6.2018.)

Ove uređaje danas je moguće naći u raznim oblicima izrađenim od strane kompanija specijaliziranih za forenzičku opremu, no validacija svih alata i uređaja koji će se možda morati koristiti u istrazi treba biti izvršena u laboratoriju. Osim fizičkih uređaja za onemogućavanje zapisivanja, forenzički alati pružaju i programsku podršku za način rada bez zapisivanja ili izmjene podataka. Ovisno o izboru forenzičara uz obaveznu validaciju moguće je koristiti oba načina zaštite dokaza prilikom forenzičkog kopiranja.

„*When you handle e-evidence, always follow the three Cs of evidence: care, control, and chain of custody.*“ (Volonino, Anzaldua, 2008., 56.)

Prilikom prikupljanja i očuvanja dokaza forenzičari trebaju biti vrlo oprezni i poštovati ,ako situacija to omogućuje, sve postavljene procedure, načela, zakone i ograničenja naloga kako bi svi prikupljeni dokazi prilikom prezentacije imali neosporivu vrijednost u sudskom procesu dokazivanja krivnje.

## 4.4. Analiza prikupljenih dokaza

Svi koraci napravljeni do sada bili su priprema za analizu prikupljenih dokaza i njihovo tumačenje.

„*Kopanje kroz podatke osumnjičenog, dokumente, bilješke, računalnu poštu, izravne poruke, internet povijest, financijske zapise, fotografije i druge informacije je ono što većina ljudi misli kada čuje pojam digitalna forenzika - i iz dobrog razloga.*“ (Volonino, Anzaldua, 2008., 117.)

Nakon što su pripremljene forenzičke kopije, forenzičari se mogu susresti s velikom količinom podataka od kojih je samo dio relevantan za slučaj. Prvi korak koji bi forenzičari trebali napraviti je ponovni pregled cijelog slučaja. Pod time se podrazumijeva pregled evidencije preuzimanja dokaza, laboratorijskog zahtjeva, pregled naloga i drugi administrativni zadatci. Forenzičari posebno trebaju obratiti pozornost na povijest slučaja, prigovore, informacije o osumnjičenom ili žrtvi, te drugim informacijama prikupljenim kroz ispitivanja u trenutku istrage. Svaka informacija koja može dati odgovor na pitanje od kuda krenuti s istragom i gdje postoji najveća vjerojatnost za pronalazak dokaza, imat će veliku vrijednost forenzičaru. Informacije o vrsti uređaja, korisniku i mjestu pronalaska pomaže forenzičarima da odrede prioritet analiziranja elektroničkih uređaja. (IACIS, 2017.)

„*...hoćeš li najprije ispitati računalo pronađeno pod osumnjičenim krevetom ili računalo priključeno na televiziju u obiteljskoj sobi?*“ (IACIS, 2017., 1024.)

Nakon prikupljanja i pregleda informacija o slučaju forenzičar može pristupiti pripremi plana za analizu prikupljenih dokaza. Uobičajeno je da forenzičar u ovome trenutku utvrdi prema prikupljenim podacima koji artefakti su od posebnog interesa za slučaj. U slučaju prijetnji preko računalne pošte, forenzičar će se najvjerojatnije fokusirati upravo na nju. Ako se radi o slučaju preuzimanje nedozvoljenog slikovnog sadržaja s interneta, forenzičar će kao prioritet postaviti pretraživanje svih grafičkih datoteka. Za svaki slučaj moguće je postaviti listu općih riječi, u slučaju prodaje opojnih droga pretraga poznatih uličnih naziva za droge može znatno ubrzati i olakšati posao forenzičaru.

Kako bi se ubrzali procesi analize danas forenzičari na raspolaganju imaju veliki broj automatiziranih forenzičkih alata. Ovakvi alati su potrebni za bržu provedbu analize, no njihove rezultate bi trebalo detaljno provjeriti. Rezultati automatiziranih alata mogu znatno pridonijeti istrazi pronalaskom novih općih riječi i tragova za daljnju analizu.

„*Cilj je započeti s popisom dostupnih artefakata, te dopustiti da vas podaci vode do drugih dokaza*.“ (IACIS, 2017., 1044.)

Forenzički alati omogućuju istražiteljima da znatno ubrzaju analizu velikog broja podataka koje je danas moguće pronaći na računalima zahvaljujući razvoju medija za pohranu podataka i povećanju njihovog kapaciteta. Funkcionalnosti alata poput predefinirani filtera i mogućnost kreiranja vlastitih, ubrzavaju proces analize. Neki od uobičajenih kriterija za filtriranje u digitalnoj forenzici su imena datoteka, vremenski rasponi, filtriranje prema tipu i veličini datoteka, te mnogi drugi zavisno o vrsti slučaja i dostupnim informacijama. Pretraživanje ključnih riječi jedan je od načina kako pronaći datoteke i sektore koje bi drugačije mogli biti preskočeni. Ključne riječi moguće je podijeliti na opće i prema slučaju specifične riječi. Listu općih riječi za razne vrste slučajeva moguće je preuzeti na internetu sa stranica agencija za suzbijanje kriminala. Iako su opće liste vrlo korisne forenzičari kroz proces analize prikupljaju razne informacije o osumnjičenom i njegovim navikama. Ovakve informacije pomažu forenzičaru da sastavi vlastiti, slučaju specifičnu, listu riječi. Liste za specifične slučajeve mogu sadržavati imena osoba, korisnička imena, adrese, telefonske brojeve, upisane URL-ove, nazive dokumenata i mnoge druge informacije prikupljene prije i za vrijeme analize.

GREP (*Globally search a Regular Expression and Print*) izrazi zamjena su ili dodatno sredstvo za pretraživanje dokaza prilikom analize. Ključne riječi imaju jednu kritičnu manu, a ona je da se pretraživanjem određene riječi može pronaći samo ta identična riječ. Tako se prilikom pretraživanja mobilnog broja „555-555-5555“ može naći taj identični izraz, ali neće se pronaći drugi mogući oblici poput 555.555.5555, (555) 555 5555 ili 5555555555. Upravo iz ovog razloga koriste se poznati uzorci za pretraživanje podataka za koje se ne zna u kojem će se obliku pojaviti. (IACIS, 2017., 1044-1047.)

Tablica 1. - Primjer GREP izraza

| Uzorak | Primjeri |
|---|---|
| Ivić [DB] Ivan | Ivić D Ivan ili Ivić B Ivan |
| ivic_ivan[0-9]{3} | Korisničko ime ivic_ivan, s bilo kojom kombinacijom tri znamenke |
| https?://.+.\.(com\|net\|org\|hr) | Svi URL-ovi koji započinju s http ili https a završavaju s .com, .net, .org, .hr |

Izvor: autor

Ovako postavljeni pretraživanja omogućuju forenzičarima da pretražuju dokaze prema određenim oblicima odnosno poznatim uzorcima. Iako ovi izrazi u forenzičkim programima nisu uvijek isti, potrebno je vrlo malo vremena za prilagodbu ovakvih izraza specifičnom forenzičkom alatu.

*Hashing* je još jedna od tehnika koji forenzičari koriste prilikom analize prikupljenih dokaza. *Hashing* je matematička reprezentacija podatka, datoteke, sektora, teksta, particija i sličnog jedinstvenom oznakom. Rezultat ove tehnike je dobivanje jedinstvenog seta znamenki.

„*Dvije datoteke s identičnim uzorcima bita trebale bi imati istu hash vrijednost koristeći isti algoritam za hash-iranje.*“ (IACIS, 2017., 342.)

Danas je sve popularnija usporedba *hashing*-a s otiskom prsta pošto svaki podataka ima svoj vlastiti jedinstveni set znamenki. Forenzičari koriste razne vrste *hasing* algoritama poput CRC (*Cyclic Redundancy Check*), MD5 (*Message Digest 5*) i SHA (*Secure Hash Algorithm*) algoritma. Ova tehnika koristi se u digitalnoj forenzici za verifikaciju podataka odnosno kao potvrda da dokazi nisu bili izmijenjeni. *Hashing* algoritam Checksum 64 koristi se kao potvrda da je kreiran forenzički sterilan medij odnosno medij potpuno prebrisan s poznatom vrijednosti nula. Razloga zašto se koristi upravo ovaj *hashing* algoritam je što njegov rezultat prilikom forenzički prebrisanog medija iznosi nula. Uz navedeno postoje poznate baze setova *hash* vrijednosti čime je moguće određene datoteke izdvojiti jer nisu opasne ili opaziti jer se vrijednosti poklapaju s crnim ili sivim *hashing* setovima. Ako se izvršava forenzička analiza

nad više različitih uređaja, moguće je pomoću *hashing* vrijednosti utvrditi da li se potpuno iste datoteke nalaze na različitim uređajima, a time i utvrditi npr. povezanost više sudionika. (IACIS, 2017. 342-345.)

Kako bi se jednostavnije pretražile slikovne datoteke forenzički alati imaju mogućnost za detekciju površine kože, za jednostavniji pronalazak pornografskog sadržaja. Također alati posjeduju mogućnosti za pretraživanje poznatih baza nedozvoljenih slika, kreiranje vremenskih crta prema poznatim vremenima i provjere entropije kojom je moguće utvrditi postojanje enkripcije.

Analiza prikupljenih dokaza završava kada se obavi kompletna analiza svih prikupljenih dokaza ili pronađu dokazi za određenu radnju. Potrebno je pronaći sredinu između pregledavanja svih podataka i traćenja vremena. Na kraju forenzičar koji je izvršio analizu mora stati pred suca i odgovoriti na pitanje je li ili nije izvršio potpunu analizu dokaza. Forenzičar mora biti u stanju odrediti koje forenzički alati su mu potrebni, provjeriti njihov rad i napraviti plan kojim će prikupiti digitalne dokaze.

### 4.5. Izvještaj istrage

„*Osim provođenja temeljite i cjelovite analize računalnih podataka, od ključne je važnosti da forenzički istražitelj može jasno objasniti svoje nalaze i detalje o tome kako su dobiveni, kao i njihovu relevantnost za istragu.“* (IACIS, 2017., 1054.)

Većina vodećih forenzičkih alata posjeduje integrirane funkcionalnosti za kreiranje izvještaja. Za izradu takvih izvještaja moguće je koristiti već predefinirane obrasce ili vlastoručno kreirati izvještaj. Ovaj proces izvodi se tako da forenzički program sam postavlja prije označene ključne dokaze u izvještaj. Generalno bi se iz izvještaja trebalo moći vidjeti što se analiziralo, po čijem odobrenju se analiza radila, koje metode su korištene u analizi, popis relevantnih dokaza i njihovo objašnjenje.

Izvještaj je moguće dostaviti u papirnatom obliku gdje bi se zatim trebala dodati tablica sadržaja i jasno označiti poglavlja, te u digitalnom obliku. Kreiranje izvještaja u papirnatom

obliku može predstavljati izazov prilikom prezentiranja snimki, baza podataka, dijelova dokumenta i sličnog. Digitalni izvještaji danas se sve više koriste pošto je organizacija različitih tipova podataka i dokaza znatno lakša. Problem koji može nastati prilikom digitalnog izvještaja je neposjedovanje programske podrške za njegov pregled od svih strana uključenih u sudski proces. Najnoviji trend su HTML (*Hyper Text Markup Language*) i web bazirani izvještaji koji imaju mogućnosti za povezivanje i označavanje određenih stavki čime se upućuje čitaoca na pojedinačne dijelove. Svaka od ovih metoda posjeduju prednosti i mane, te se često može vidjeti kombinacija ili izrada više vrsta izvještaja za što bolje prezentiranja dokaza.

Prilikom izrade izvještaja u obzir treba uzeti sudionike sudskog procesa koji možda ne posjeduje osnovno ili napredno znanje iz informatike i korištene terminologije. Sudac, porota, obrana i drugi sudionici možda neće imati potrebno iskustvo za poznavanje tehničkih pojmova i određenih dijelova izvještaja, te forenzičar u takvim situacijama mora biti spreman objasniti svoje pronalaske na svim sudionicima razumljiv način. Kako bi si forenzičari pomogli prilikom takvih situacija, mogu pripremiti dodatne materijale u obliku prezentacije koje objašnjavaj opće koncepte rada pojedinih tehnologija koje se danas koriste. Osim prezentacija za prikazivanje dokaza moguće je koristiti i snimke zaslona prikazanih dokumenata koji sadrže relevantne dokaze. (IACIS, 2017., 1055-1056.)

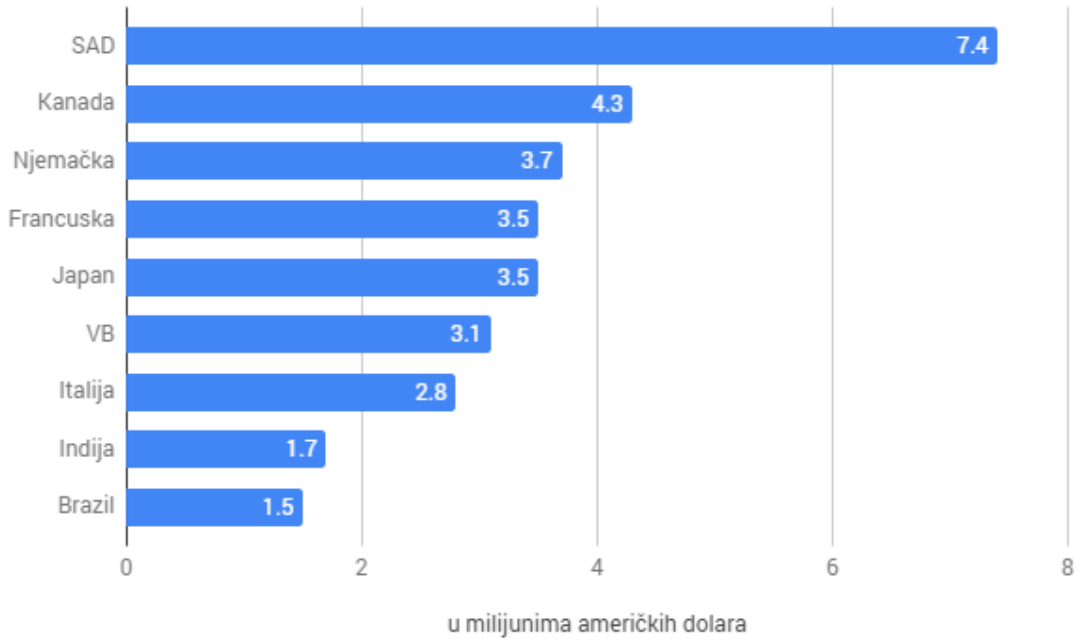
Zavisno o vrsti slučaja i dokazima forenzičari danas na raspolaganju imaju programsku podršku za kreiranje i prilagođavanje izvještaja. Razumijevanje forenzičara za svoje pronalaske i sudionike ključno je kako bi svi bez poteškoća razumjeli rezultate forenzičke analize. Loše prezentiranje dokaza i loša objašnjenja mogu prouzročiti preispitivanje dokaza i stručnosti forenzičara čime može doći do komplikacija u cijelom sudskom procesu, a u najgorem slučaju i do odbacivanja prikupljenih digitalnih dokaza.

# 5. Digitalna forenzika prilikom ilegalnog izvlačenja uredskih podataka

U nastavku rada prikazat će se postupak izvođenja računalne forenzike u slučaju izvlačenja uredskih podatka. Objasnit će se proces analize prikupljenih dokaza, rad u forenzičkom alatu otvorenog koda i komercijalnom alatu, te će se usporediti dobiveni rezultati i funkcionalnosti korištenih alata.

Ilegalno izvlačenja uredskih podataka odnosi se na pristup, kopiranje i iznošenje ili slanje povjerljivih uredskih podataka, namjernim ili slučajnim radnjama, u nepouzdanu okolinu. Nadalje kada se govori o uredskim podacima od ovoga trenutka mislit će se isključivo o digitalnim podacima i datotekama koje je moguće pronaći na Windows operacijskim sustavima u uredskom poslovanju.

Slika 14. - Šteta prouzročena u 2017. godini izvlačenjem podataka iz organizacija




Izvor: obrada autora prema https://www.statista.com/chart/9918/the-price-tag-attached-to-data-breaches/ (07.6.2018)

Nerijetko forenzičar koji izvršava identifikaciju i prikupljanje elektroničkih dokaza nije osoba koja izvršava forenzičku analizu u laboratoriju. U ovome radu pristupit će se forenzičkoj istrazi upravo na navedeni način.

Forenzičari prilikom dolaska u laboratorij ponovno proučavaju sve prikupljene informacije kao pripremu za forenzičku analizu. U ovom specifičnom slučaju radi se o Iaman Informant-u, menadžeru razvojnog odjela poznate kompanije koja razvija nove tehnologije i uređaje. Menadžer je zaustavljen na sigurnosnoj provjeri prilikom izlaska iz kompanije, te su kod njega pronađeni razni mediji za pohranu podataka. Mediji su kratko pregledani prilikom sigurnosne provjere, te je u tom procesu korišten uređaj za zabranu zapisivanja. Iako nisu pronađeni dokazi o izvlačenju osjetljivih podataka kompanije, mediji za pohranu podataka odmah su zbog kršenja sigurnosnih pravila poslani u forenzički laboratorij na daljnju analizu.

Sigurnosna pravila kompanije sadrže sljedeće stavke:

- Povjerljivi elektroničke datoteke trebaju biti pohranjene u autoriziranim eksternim medijima i sigurnim mrežnim mjestima
- Povjerljivi papirnati dokumenti i elektronički podaci mogu se pristupati samo unutra razdoblja od 10 do 16 sati s odgovarajućim dopuštenjima
- Neautorizirani elektronički uređaji poput prijenosnih računala, medija za pohranu podatka i pametnih uređaja ne smiju biti uneseni u kompaniju
- Svi zaposlenici moraju proći kroz sigurnosnu provjeru
- Svi mediji za pohranu poput tvrdog diska, USB uređaja i optičkih medija su zabranjeni prema pravilima sigurnosne provjere

Naknadno su dobivene informacije da navedena kompanija posjeduje sigurnosne mehanizme DRM (*Digital Rights Management*) i DLP (*Data Loss Prevention*) kako bi zaštitila svoj informacijski sustav. Također je utvrđeno da je kao menadžer u kompaniji Iaman Informant imao dovoljna prava za zaobilaženje ovih mehanizama, bio vrlo zainteresiran za informacijsku tehnologiju, te posjeduje osnovno znanje o računalnoj forenzici.

Tablica 2. - Elektronički uređaji prikupljeni na sigurnosnoj provjeri

| Prikupljeni uređaji | Memorija |
|---|---|
| Osobno (virtualno) računalo | HDD 20 GB + 2,048 MB RAM |
| Autoriziran USB mediji | 4 GB (S/N: 4C530012450531101593) |
| USB mediji | 4 GB (S/N: 4C530012550531106501) |
| CD-R mediji | 700 MB |

Izvor: autor

Od strane vlasnika kompanije dobiven je zahtjev za pronalazak bilo kakvih dokaza koji ukazuju da su navedeni mediji za pohranu podataka korišteni za izvlačenje osjetljivih podataka kompanije.

## 5.1. Digitalna forenzika korištenjem Autopsy alata otvorenog koda

Autopsy je forenzička platforma, grafičko sučelje za TSK (*The Sleuth Kit*®) i druge forenzičke alata koji omogućuju analiziranje forenzičkih kopija diska. TSK je knjižnica i kolekcija alata za naredbeni redak koji omogućuju analiziranje forenzičkih kopija. Ovaj besplatni alat danas je vrlo popularan, a koriste ga odvjetnici, vojska i korporativni istražitelji za analiziranje događaja na računalima.

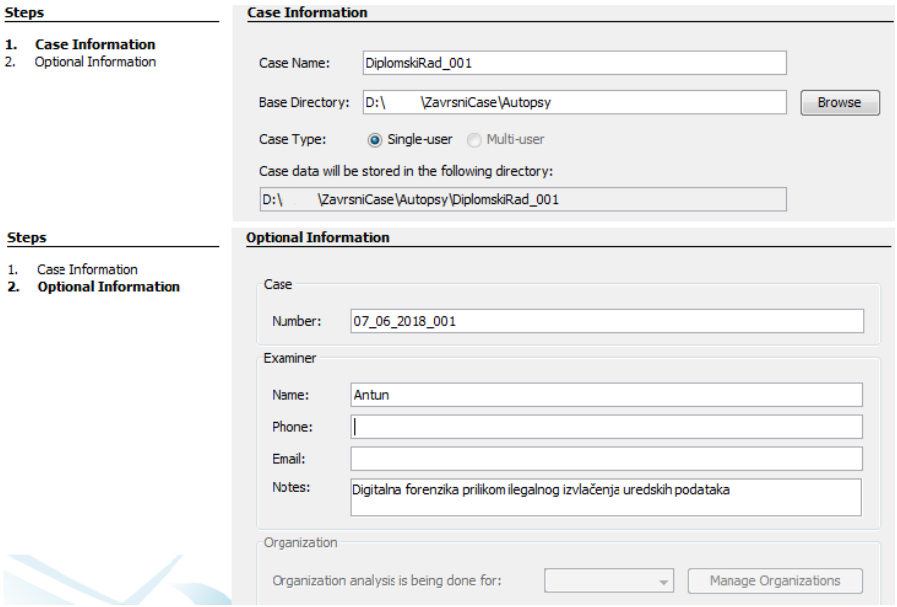
„*Autopy je Windows bazirani digitalni forenzički alat koji je besplatan, otvorenog koda i ima sve značajke koje biste inače pronašli u komercijalnim forenzičkim alatima.*“ (Basis Technology, 2018.)

Prednosti koje nudi ovaj forenzički alat su intuitivni dizajn, jednostavna instalacija i preglednost analiziranih podataka. Ovaj alat napravljen je kao platforma koja dolazi s modulima za vremenske linije, sortiranja *hash* vrijednosti, pretraživanja ključnih riječi, izvlačenja web artefakta, vračanja izbrisanih datoteka, te mogućnosti za dodavanje modula izrađenih od trećih strana. Uz navedeno alat ima mogućnosti pokretanja paralelnih pozadinskih zadataka kako bi analiza bila brža, a verzija alata koja se koristila za forenzičku analizu u ovom radu je Autopsy 4.7.0.

### 5.1.1. Otvaranje novog slučaja

Prvim pokretanjem Autopsy forenzičkog alata, forenzičaru se pojavljuje jednostavni izbornik u kojem je omogućeno otvaranje novog, nedavno otvorenog ili otvaranje prije kreiranog slučaja. Prilikom kreiranja novog slučaja forenzičar ima mogućnost unijeti različite informacije o slučaju, osobi koja izvršava forenzičku analizu, odabira jednokorisničkog ili više korisničkog načina rada, te odabira lokacije spremanja rezultata i osnovnog direktorija. Uz navedeno također je omogućeno dodavanje neobaveznih informacija poput imena, telefona, adrese računalne pošte i zabilješka forenzičara.

Slika 15. - Proces otvaranja novog slučaja




Izvor: autor

### 5.1.2. Dodavanje dokaza

Proces dodavanja prikupljenih dokaza moguće je napraviti neposredno nakon otvaranja slučaja ili naknadnim dodavanjem putem izbornika. Prilikom dodavanja dokaznog materijala, Autopsy nudi forenzičarima opcije za odabir različitih izvora podataka. Neki od ponuđenih opcija su učitavanje slike diska ili datoteke virtualnih računala, lokalnog diska, logičkih datoteka i slike neodijeljenog prostora. Svaka od ovih opcija podržava razne, forenzički

uobičajene, formate poput *.dd (*DiskDoubler Archive files*), *.raw (*Raw Image Data*), *.E01 (*Encase Image File Format*) i *.vmdk (*Virtual Machine Disk*).

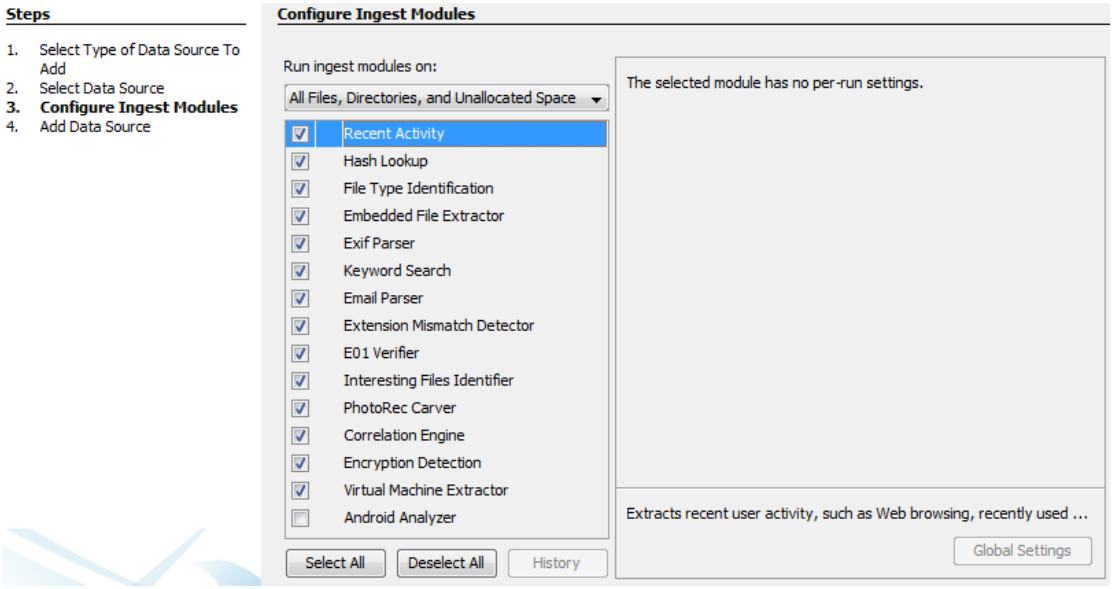
U ovom slučaju svi pristigli dokazi nalaze se u *.E01 formatu, izumljenom od strane jedne od vodećih forenzičkih marki EnCase. Prednost korištenja ovog formata je automatsko rezanje slike nakon dostignutih 640 MB prilikom kojega ne dolazi do promjena unutarnje strukture datoteke. Uz navedeno ovaj format u naslovu sadrži informacije o slučaju dok svaki skup podataka ima ugrađeni CRC *hash* zapis kako bi se mogle provjeriti bilo kakve nastale pogreške.

Slika 16. - Proces dodavanja forenzičkih slika


Izvor: autor

Dodavanje forenzičkih kopija dokaza vrlo je jednostavno i intuitivno. Pažnju u ovom procesu treba obratiti na ulaznom vremenu, a odnosi se na vremensku zonu prikupljenih dokaza, a ne forenzičkog računala na kojem se izvršava analiza.

Slika 17. - Lista modula




Izvor: autor

Nakon dodavanja dokaza u forenzičkom alatu Autopsy, slijedi odabir i konfiguracija dostupnih modula za analiziranje specifičnih dijelova sustava i raščlanjivanje podataka. Zavisno o vrsti elektroničkih uređaja i dokaza forenzičar određene module može isključiti kako bi uštedio na vremenu. U ovom slučaju isključen je modul za Android analizu pošto među prikupljenim dokazima nema mobilnih uređaja s navedenim operacijskim sustavom.

### 5.1.3. Forenzička analiza

Ovaj proces započinje pokretanjem Autopsy modula ako su odabrani jedan ili više dostupnih izbora. Moduli se izvršavaju u pozadini s mogućnosti izvršavanja određenih modula paralelno odnosno u isto vrijeme. Ove module moguće je pokrenuti i naknadno kroz samo sučelje alata. Moduli su napravljeni da omoguće vrlo brzi pronalazak relevantnog sadržaja, a prilikom izvođenja paralelnih modula, zadaci se grupiraju, te ih je moguće usporediti s „cijevima“ kroz koje prolaze datoteke koje se analiziraju.

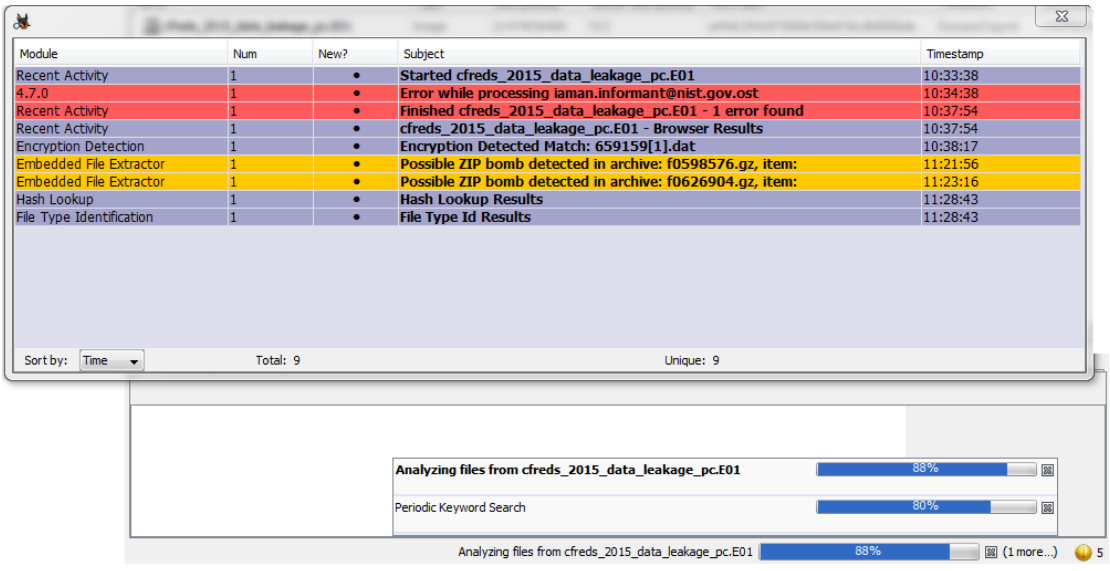
Slika 18. - Prikaz “cijevi” modula


Izvor: obrada autora prema http://sleuthkit.org/autopsy/docs/user-docs/4.3/ingest_page.html (07.06.2018.)

Ovisno o jačini upravljačke jedinice, tj. broju jezgri koju posjeduje forenzičko računalo na kojem se izvršava analiza, moguće je konfigurirati broj „cijevi“ kroz koje se podaci analiziraju. Autopsy prioritizira korisnički sadržaj prije drugih tipova dokumenata, tako da će kroz analizu prvo proći podaci iz npr. „Documents and Settings“, a ne „Windows“ direktorija.

Kako bi u svakom trenutku forenzičar znao kako njegova analiza napreduje, na raspolaganju u donjem desnom kutu ima statusnu traku cijele analize učitanih dokaza i zasebnih modula koji se trenutno izvršavaju ili su završeni.

Slika 19. - Status analize s upozorenjima, greškama I izvršenim zadacima

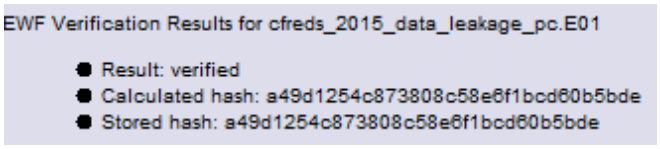



Izvor: autor

Prema odabiru forenzičara u procesu analize moguće je dodavati nove izvore dokaza, ručno pregledavati analizirane dokumente ili pričekati da se trenutna analiza završi. Zbog opsežnosti i „težine“ modula na upravljačku jedinicu u ovom slučaju pričekat će se s dodavanjem novih izvora dokaza kako ne bi došlo do usporavanja zadataka koji se trenutno izvršavaju.

Zadnji modul koji se izvršava je verifikacija *.E01 forenzičke slike, tako da se uspoređuje, izračunata *hash* vrijednost prilikom prikupljanja dokaza i ponovno izračunata vrijednost nakon provedene analize. Ako se ove dvije vrijednosti podudaraju možemo sa sigurnošću reći da nije došlo do promjene prikupljenih dokaza.

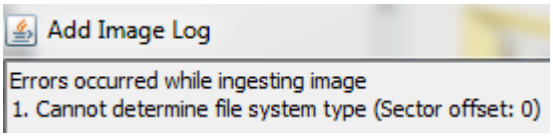
Slika 20. - Prikaz rezultata verifikacije *hash* vrijednosti




Izvor: autor

Proces dodavanja i automatske analize ponovljen je za ostale tri forenzičke slike kako bi svi, moguće relevantni dokazi, bili prisutni prilikom ručne analize. Prilikom dodavanja zadnje četvrte forenzičkih slike alat Autopsy prikazuje skočni prozor s greškom. Zadnja forenzička slika je slika CD-R (*Compact Disc-Recordable*) medija s datotečnim sustavom tipa UDF (*Universal Disk Format*) koji prema dokumentaciji nije podržan od strane Autopsy alata, te je potrebno koristiti drugačiji pristup prilikom analiziranja navedene forenzičke slike.

Slika 21. - Prikaz pogreške prilikom dodavanja posljednje forenzičke slike

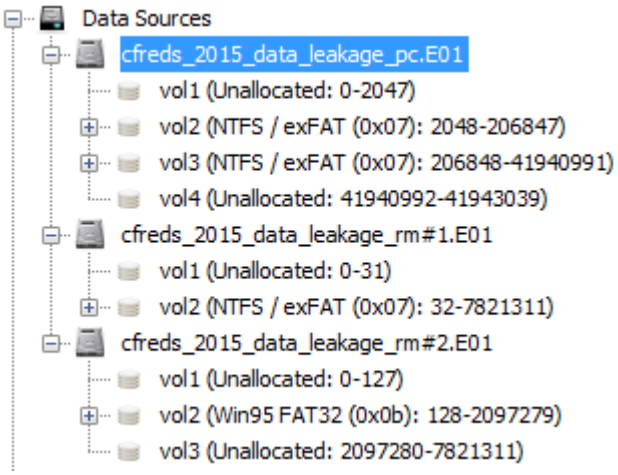



Izvor: autor

Nakon što su izvršeni Autopsy moduli, te su sortirane i raščlanjene datoteke, forenzičar koji izvršava analizu često se može susresti, ovisno o količini prikupljenih podataka, s vrlo

velikim brojem rezultata. Sljedeći korak je detaljna analiza rezultata i pretraživanje za relevantnim dokazima. U ovoj fazi forenzičar mora pokazati svoju stručnost prilikom pretraživanja sadržaja rezultata i snalažljivost.

Slika 22. - Prikaz particija prikupljeni uređaja




Izvor: autor

U razgranatom pregledniku alata Autopsy moguće je pregledati sve prepoznate particije, direktorije i njihov sadržaj. Na samom početku analize traže se informacije o svojstvima sustava. Pregledom dokaza utvrđeno je da je računalo ima dvije dodijeljene particije NTFS datotečnog sustava od kojih druga particija sadrži Windows sistemske datoteke. Pregledom rezultata Windows registra, točnije „SOFTWARE“ ogranka, moguće je vidjeti neke od osnovnih podataka o Windows sustavu instaliranom na uređaju.

Tablica 3. - Opće informacije o sustavu

| | |
|---|---|
| Naziv sustava | Windows 7 Ultimate |
| Datum instaliranja sustava | Sun Mar 22 14:34:26 2015 (GTM) |
| Registriran vlasnik | informant |
| Početni direktorij | C:\Windows |
| Identifikacijska oznaka proizvoda | 00426-292-0000007-85262 |
| Lokacija informacija | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion |

Izvor: autor

Kako bi se mogli koristiti zapisi o vremenu pojedinih datoteka potrebno je utvrditi vremensku zonu sustava. Informacije o vremenskoj zoni, odnosno *bias* vrijednost, koja je vremenska razlika u minutama od UTC-a (*Coordinated Universal Time*) nalazi se u „SYSTEM“ ogranku Windows registra.

Tablica 4. - Informacije o vremenskoj zoni sustava

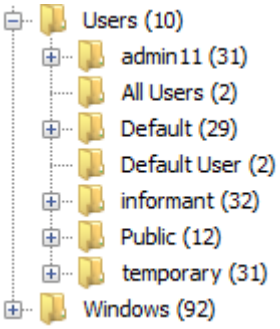
| | |
|---|---|
| *Bias* vrijednost | 300 (u minutama) |
| Naziv vremenske zone | Eastern Standard Time (UTC -5) |
| Lokacija informacija | HTLM\SYSTEM\ControlSet###\Control\TimeZoneInformation |

Izvor: autor

Iz navedenog ogranka Windows registra također je moguće utvrditi da je naziv oduzetog računala „INFORMANT-PC“ koji se nalazi u „*\Control\ComputeName\“ ključu registra.

Pregledom Windows particije i direktorija „Users“ moguće je vidjeti korisničke račune jer ovaj operacijski sustav za svakog korisnika kreira specifični poddirektorij, te se nazivaju prema korisničkom imenu. Uz uobičajene Windows profile poput „Default“ i „Public“ prisutni su i korisnički računi „admin11“, „informant“ i „temporary“.

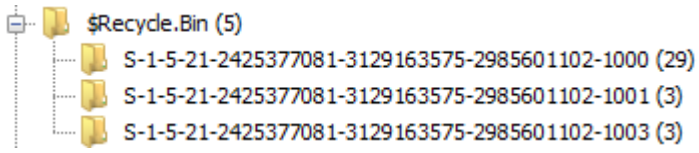
Slika 23. - Prikaz korisničkih direktorija




Izvor: autor

Podaci korisničkih računa nalaze se i u Windows registru, ogranku „HKLM\SAM“, te je uz to moguće iste pregledati u sistemskom direktoriju „$Recycle.Bin“ pošto se za svakoga korisnika kreira njemu specifični „koš za smeće“ direktorij predstavljen SID (*Security Identifier*) brojem.

Slika 24. - Prikaz SID brojeva korisničkih računa




Izvor: autor

SID brojevi sastavljeni su od više informacija od kojih je jedna RID (*Relative ID*). RID je uvijek odnosi na zadnje znamenke odvojene crtom, te su ovi brojevi dodijeljeni redom. U ovom slučaju preskočen je RID „1002“, te je potrebno potvrditi korisničke račune iz drugoga izvora. Pregledom Windows ogranka SAM utvrđeno je da korisnički račun pod RID brojem „1002“ ima naziv „ITechTeam“ te je moguće da je sumnjivac pomoću specijaliziranih programa isti direktorij izbrisao kako bi prekrio tragove. Informacije koje se nalaze u SAM ogranku uz navedene su i broj prijave za pojedinačni račun, zadnja promjena lozinke i neuspješne prijave. Autopsy za čitanje SAM ogranka koristi program otvorenog koda RegRipper u obliku dodatka s kojim dolazi prilikom instalacije.

Tablica 5. - Prikaz informacija o korisničkim računima

| Korisnik | RID | Admin | Broj prijava | Zadnja prijava |
|---|---|---|---|---|
| informant | 1000 | Da | 10 | Wed Mar 25 14:45:59 2015 (UTC) |
| admin11 | 1001 | Da | 2 | Sun Mar 22 15:57:02 2015 (UTC) |
| ITechTeam | 1002 | Da | 0 | Never |
| temporary | 1003 | Ne | 1 | Sun Mar 22 15:55:57 2015 (UTC) |

Izvor: autor

Prema prikupljenim podacima zaključeno je da je zadnji korisnički račun prijavljen na računalu bio „informant“.

Kako bi pregledali korisničku aktivnost, odnosno koje programe je korisnik najviše koristio, potrebno je analizirati Windows *Prefetch* artefakt. Ovaj artefakt dio je Windows sustava kojem je cilj ubrzavanje često pokretanih programa kako bi korisnici imali bolje iskustvo. Ovaj artefakt sadrži podatke o pokrenutim programima, približnom broju pokretanja i vremenu zadnjeg pokretanja.

Slika 25. - Prikaz *Prefetch* zapisa o sumnjivim programima

| Source File | Prefetch File Name | Actual File Name | Program Number Runs | PF Execution DTTM 1 |
|---|---|---|---|---|
| CCLEANER64.EXE-779BD542.pf | CCLEANER64.EXE-779BD542.pf | CCLEANER64.EXE | 2 | 2015-03-25 15:15:50 GMT |
| ERASER.EXE-CE61944A.pf | ERASER.EXE-CE61944A.pf | ERASER.EXE | 2 | 2015-03-25 15:13:30 GMT |

Izvor: autor

Prilikom analiziranja *Prefetch* zapisa uočeni su programi koji sadrže funkcionalnosti za brisanje podataka i promjenu Windows registra. Program Eraser koji je bio pokrenut služi za prebrisavanje podataka. Korištenje ovakvih programa za brisanje dokaza o nedozvoljenim radnjama u forenzičkim krugovima nazivaju se i korištenje anti-forenzičkih metoda. Pregledom *Prefetch* zapisa također je utvrđeno da je korisnik često koristio internet preglednike Chrome i Internet Explorer.

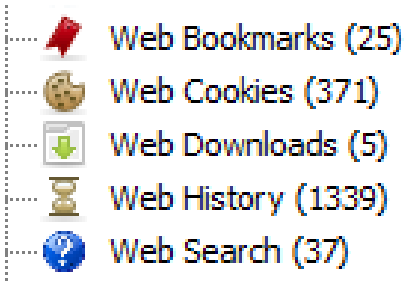
Slika 26. - Prikaz *Prefetch* zapisa o preglednicima

| Source File | Prefetch File Name | Actual File Name | Program Number Runs | PF Execution DTTM 1 |
|---|---|---|---|---|
| CHROME.EXE-D999B1BA.pf | CHROME.EXE-D999B1BA.pf | CHROME.EXE | 71 | 2015-03-24 21:05:38 GMT |
| IEXPLORE.EXE-4B6C9213.pf | IEXPLORE.EXE-4B6C9213.pf | IEXPLORE.EXE | 14 | 2015-03-25 15:22:07 GMT |
| IEXPLORE.EXE-908C99F8.pf | IEXPLORE.EXE-908C99F8.pf | IEXPLORE.EXE | 2 | 2015-03-25 15:22:06 GMT |

Izvor: autor

Autopsy dolazi s ugrađenim modulima za prepoznavanje i sortiranje različitih datoteka kreiranih od strane preglednika. U razgranatom prikazu rezultata prikazani su u kategorijama kolačići, povijest posjećenih web stranica i pretraživanja, preuzimanja, te spremljene oznake.

Slika 27. - Razgranati prikaz artefakata preglednika

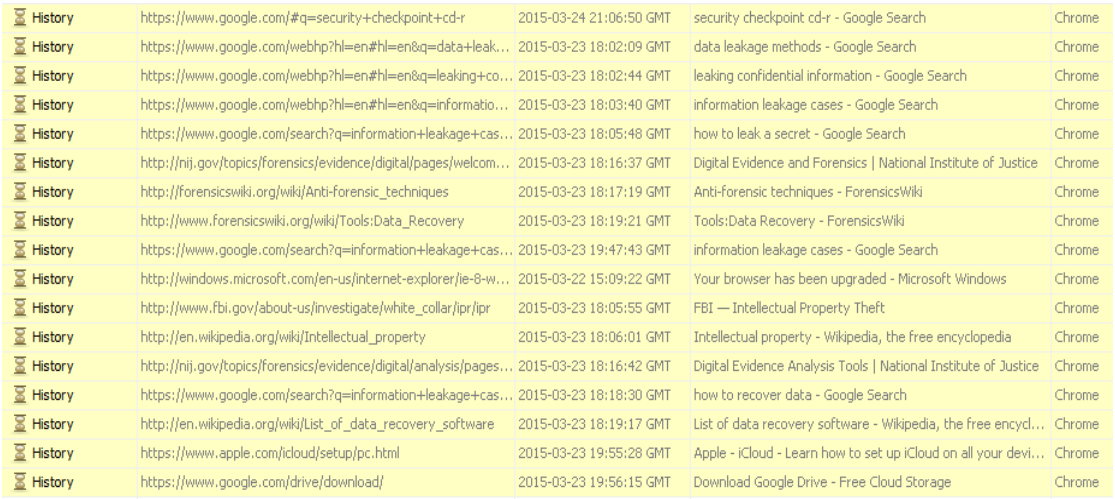



Izvor: autor

U sekciji preuzimanja vidljivo je da je korisnik „informant“ preuzeo izvršne datoteke za instaliranje oblačnih servisa iCloud i Google Drive. Analiza povijesti pretraživanja odličan je

način za profiliranje korisnika i otkrivanja njegovih interesa, a menadžer „informant“ posjećivao je stranice koje sadrže informacije o intelektualnom vlasništvu, alatima za oporavak podataka, anti-forenzičkim metodama i slično. Pregledom pretraživanih pojmova potvrdilo je zainteresiranost sumnjivca za prije navedenim temama. Uz navedeno korisnik je prema pretraživanim pojmovima i posječenim stranicama bio vrlo zainteresiran za novosti o tehnologiji.

Slika 28. - Povijest posječenih stranica i pretraženih pojmova



| | | | | |
|---|---|---|---|---|
| History | https://www.google.com/#q=security+checkpoint+cd-r | 2015-03-24 21:06:50 GMT | security checkpoint cd-r - Google Search | Chrome |
| History | https://www.google.com/webhp?hl=en#hl=en&q=data+leak… | 2015-03-23 18:02:09 GMT | data leakage methods - Google Search | Chrome |
| History | https://www.google.com/webhp?hl=en#hl=en&q=leaking+co… | 2015-03-23 18:02:44 GMT | leaking confidential information - Google Search | Chrome |
| History | https://www.google.com/webhp?hl=en#hl=en&q=informatio… | 2015-03-23 18:03:40 GMT | information leakage cases - Google Search | Chrome |
| History | https://www.google.com/search?q=information+leakage+cas… | 2015-03-23 18:05:48 GMT | how to leak a secret - Google Search | Chrome |
| History | http://nij.gov/topics/forensics/evidence/digital/pages/welcom… | 2015-03-23 18:16:37 GMT | Digital Evidence and Forensics \| National Institute of Justice | Chrome |
| History | http://forensicswiki.org/wiki/Anti-forensic_techniques | 2015-03-23 18:17:19 GMT | Anti-forensic techniques - ForensicsWiki | Chrome |
| History | http://www.forensicswiki.org/wiki/Tools:Data_Recovery | 2015-03-23 18:19:21 GMT | Tools:Data Recovery - ForensicsWiki | Chrome |
| History | https://www.google.com/search?q=information+leakage+cas… | 2015-03-23 19:47:43 GMT | information leakage cases - Google Search | Chrome |
| History | http://windows.microsoft.com/en-us/internet-explorer/ie-8-w… | 2015-03-22 15:09:22 GMT | Your browser has been upgraded - Microsoft Windows | Chrome |
| History | http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr | 2015-03-23 18:05:55 GMT | FBI — Intellectual Property Theft | Chrome |
| History | http://en.wikipedia.org/wiki/Intellectual_property | 2015-03-23 18:06:01 GMT | Intellectual property - Wikipedia, the free encyclopedia | Chrome |
| History | http://nij.gov/topics/forensics/evidence/digital/analysis/pages… | 2015-03-23 18:16:42 GMT | Digital Evidence Analysis Tools \| National Institute of Justice | Chrome |
| History | https://www.google.com/search?q=information+leakage+cas… | 2015-03-23 18:18:30 GMT | how to recover data - Google Search | Chrome |
| History | http://en.wikipedia.org/wiki/List_of_data_recovery_software | 2015-03-23 18:19:17 GMT | List of data recovery software - Wikipedia, the free encycl… | Chrome |
| History | https://www.apple.com/icloud/setup/pc.html | 2015-03-23 19:55:28 GMT | Apple - iCloud - Learn how to set up iCloud on all your devi… | Chrome |
| History | https://www.google.com/drive/download/ | 2015-03-23 19:56:15 GMT | Download Google Drive - Free Cloud Storage | Chrome |

Izvor: autor

Iako alat Autopsy kroz svoje module nije prepoznao računalnu poštu pregledom *Prefetch* zapisa pronađena je „Outlook.exe“ izvršna datoteka. Provjerom uobičajenih aplikacijskih direktorija korisnika „informant“ vidljivo je da je klijent za računalnu poštu prisutan. U Windows registru „SOFTWARE“ i „NTUSER“ također su pronađeni zapisi o klijentima računalne pošte.

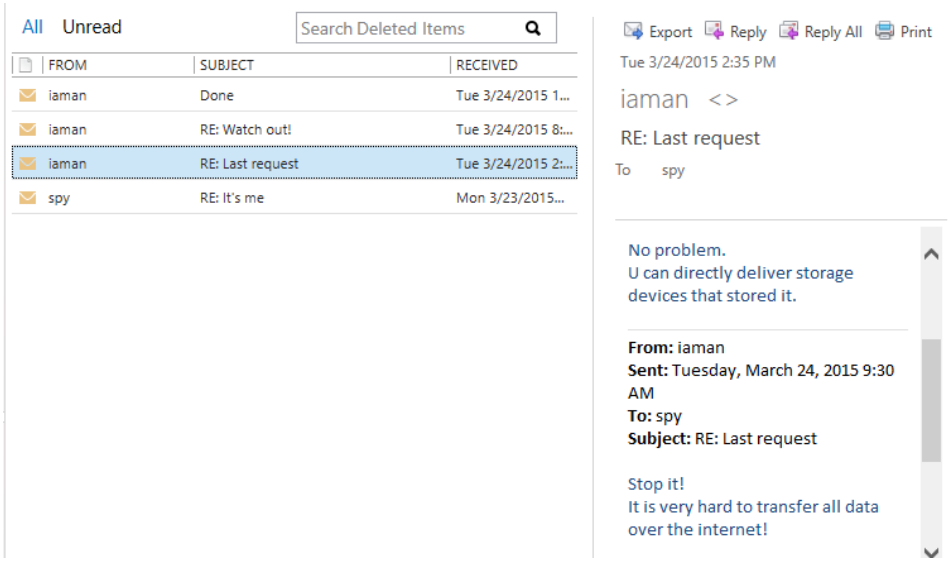
Tablica 6. - Prikaz informacija o klijentu računalne pošte

| | |
|---|---|
| Microsoft Office paket | Office 15 |
| Klijent računalne pošte | Outlook 2013 |
| Lokacija | HKLM\SOFTWARE\Clients\Mail\Microsoft Outlook |
| | NTUSER.DAT\Software\Microsoft\Office\15.0\Outlook |

Izvor: autor

Pregledom „Outlook“ direktorija aplikacijskih podataka pronađena je „iaman.informan@nist.gov.ost“ datoteka koja je izvanmrežna baza poruka koja omogućuje korisniku da pristupa prisutnim računalnim porukama. Iz ove datoteke vidljiva je i adresa računalne pošte, te OST (*Offline Outlook Data File*) datoteka sadrži poruke elektroničke poruke. Autopsy ne podržava otvaranje OST datoteke, te je za pregled poruka korišten program OST PST Viewer.

Slika 29. - Pregled računalne pošte u OST PST Viewer-u




Izvor: autor

Korištenjem GREP izraza Autopsy izlistava 17 datoteka u kojima se nalazi korisnički račun računalne pošte „iaman.informant@nist.gov“ od kojih je jedna i prije navedena OST datoteka. Pregledom datoteke različitim tipovima prikaza poput heksadecimalnog, *string* i indeks prikaza ne omogućuje nam čitanje poruka, te će se u nastavku morati koristiti prije navedeni OST preglednik.

Tablica 7. - Prikaz izmijenjenih poruka između sumnjivca

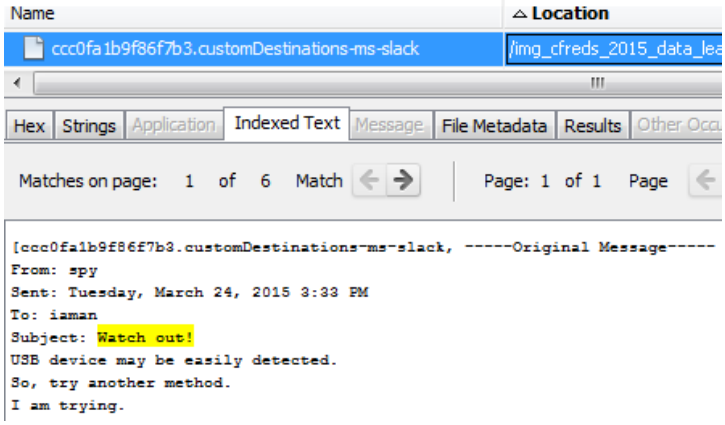
| Vrijeme (UTC -5) | spy.conspirator@nist.gov → iaman.informant@nist.gov |
|---|---|
| 23/03/2015 1:29 PM | How are you doing? |
| | Iaman.informant@nist.gov → spy.conspirator@nist.gov |
| 23/03/2015 2:44 PM | Successfully secured. |

| | |
|---|---|
| | Spy.conspirator@nist.gov → iaman.informant@nist.gov |
| 23/03/2015 3:15 PM | Good, job. I need a more detailed data about this business. |
| | Iaman.informant@nist.gov → spy.conspirator@nist.gov |
| 23/03/2015 3:19 PM | This is a sample. |
| | Spy.conspirator@nist.gov → iaman.informant@nist.gov |
| 23/03/2015 3:20 PM | Okay, I got it. I'll be in touch. |
| | Spy.conspirator@nist.gov → iaman.informant@nist.gov |
| 23/03/2015 3:26 PM | I confirm it. But, I need a more data. Do your best. |
| | Iaman.informant@nist.gov → spy.conspirator@nist.gov |
| 23/03/2015 3:27 PM | Umm..... I need time to think. |
| | Iaman.informant@nist.gov → spy.conspirator@nist.gov |
| 23/03/2015 4:39 PM | Use links below,<br>https://drive.google.com/file/d/<br>0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing<br><br>https://drive.google.com/file/d/<br>0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing |
| | spy.conspirator@nist.gov → iaman.informant@nist.gov |
| 23/03/2015 4:41 PM | I got it. |
| | Spy.conspirator@nist.gov → iaman.informant@nist.gov |
| 24/03/2015 9:26 AM | This is the last request. I want to get the remaining data. |
| | Iaman.informant@nist.gov → spy.conspirator@nist.gov |
| 24/03/2015 9:30 AM | Stop it! It is very hard to transfer all data over the internet! |
| | Spy.conspirator@nist.gov → iaman.informant@nist.gov |
| 24/03/2015 9:34 AM | No problem. U can directly deliver storage devices that stored it. |
| | Iaman.informant@nist.gov → spy.conspirator@nist.gov |
| 24/03/2015 9:35 AM | This is the last time.. |
| | iaman.informant@nist.gov → spy.conspirator@nist.gov |
| 24/03/2015 15:34 AM | (nema sadržaja poruke) |
| | iaman.informant@nist.gov → spy.conspirator@nist.gov |
| 24/03/2015 15:05 PM | It's done. See you tomorrow. |

Izvor: autor

Iz prikazane tablice računalnih poruka moguće je vidjeti da u predzadnjoj poruci nema sadržaja poruke. OST PST Viewer ne može prikazati sadržaj poruke ali je vidljiv naslov razgovora. Unosom naziva razgovora „Watch out!“ u pretraživanje pojmova, Autopsy pronalazi podudaranje naziva u datoteci „ccc0fa1b9f86f7b3.customDestination-ms-slack“. Ova datoteka je Windows artefakt *Jump List* koji nastaje otvaranjem ili pokušajem otvaranja datoteke putem specifičnog programa.

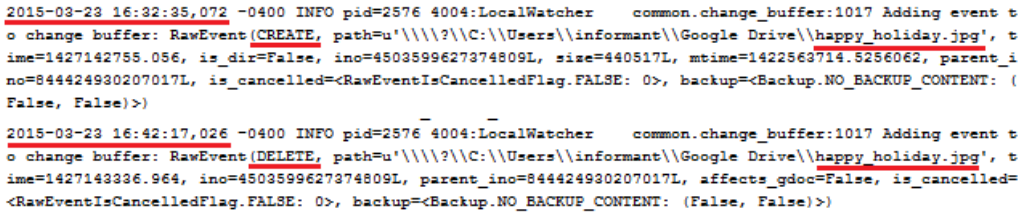
Slika 30. - Prikaz pronalaska u *Jump List* datoteci




Izvor: autor

Iz navedenih poruka jasno je vidljivo da se komunikacija odvija radi prenošenja podataka iz firme. U porukama se nalaze linkovi za Google Drive, te prijedlozi kako iznijeti informacije izvan organizacije. Pošto se u porukama spominje Google Drive provjerit će se transakcijski zapisi ovog programa koji se nalaze u datoteci „sync_log.log“.

Slika 31. - Prikaz transakcijskog zapisa kreiranja i brisanja datoteke




Izvor: autor

U transakcijskim zapisima moguće je vidjeti vrijeme postavljanja i brisanja datoteka koji odgovaraju vremenu slanja poruka odnosno postavljanje datoteke izvršeno je neposredno prije

slanja poveznica sumnjivcu, te su iste datoteke izbrisane neposredno nakon potvrde sumnjivca da ih je dobio.

Pošto su prilikom sigurnosne provjeri u posjedu menadžera pronađeni razni mediji za prenošenje podataka, u ogranku „SYSTEM“ Windows registra provjeravamo podudaraju li se zapisi o spojenim USB uređajima na računalu s uređajima koji su pronađeni kod sumnjivca.

Slika 32. - Zapisi o priključenim USB uređajima

```
Disk&Ven_SanDisk&Prod_Cruzer_Fit&Rev_2.01 [Tue Mar 24 13:58:32 2015]
  S/N: 4C530012450531101593&0 [Tue Mar 24 13:38:00 2015]
  Device Parameters LastWrite: [Mon Mar 23 18:31:11 2015]
  LogConf LastWrite          : [Mon Mar 23 18:31:10 2015]
  Properties LastWrite       : [Mon Mar 23 18:31:11 2015]
    FriendlyName    : SanDisk Cruzer Fit USB Device
    InstallDate     : Mon Mar 23 18:31:11 2015 UTC
    FirstInstallDate: Mon Mar 23 18:31:11 2015 UTC
  S/N: 4C530012550531106501&0 [Tue Mar 24 13:58:33 2015]
  Device Parameters LastWrite: [Tue Mar 24 13:58:33 2015]
  LogConf LastWrite          : [Tue Mar 24 13:58:32 2015]
  Properties LastWrite       : [Tue Mar 24 13:58:33 2015]
    FriendlyName    : SanDisk Cruzer Fit USB Device
    InstallDate     : Tue Mar 24 13:58:33 2015 UTC
    FirstInstallDate: Tue Mar 24 13:58:33 2015 UTC
```

Izvor: autor

Usporedbom prikupljenih serijskih brojeva USB uređaja od strane zaposlenika koji su obavljali sigurnosnu provjeru utvrđenoj je da se serijski brojevi podudaraju, te ovime dokazujemo da su navedeni uređaji bili spojeni na računalo.

Pregledom radne površine pronađeno je pismo ostavke menadžera izrađenog prema podacima .docx datoteke 24.03.2015. godine.

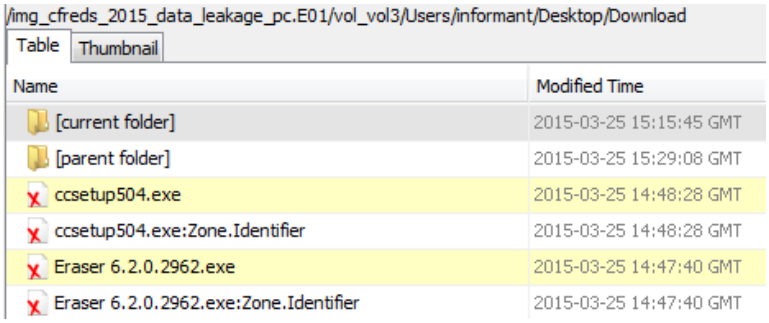
Slika 33. - Sadržaj pisma ostavke

```
RESIGNATION LETTER

March 25, 2015

Dear Mr. Manager,

This letter serves as official notification of my resignation from the company OOO, effective today. Than
k you for your guidance and support while working as your Development Manager.

.....

I would like to thank you for your support and the fine years I spent with your organization. I wish you
continued success.

Sincerely,

Iaman Informant
```

Izvor: autor

Uz navedeno pismo na radnoj površini se također nalazi i „Download“ direktorij koji sadrži s korisničke strane izbrisane izvršne datoteke programa CCleaner i Eraser čime se dodatno potvrđuju nalasci iz *Prefetch* Windows artefakata.

Slika 34. - Prikaz izbrisanih izvršnih datoteka




Izvor: autor

Pregledom Windows artefakta *$UsnJrnl* (*Update Sequence Number Journal*) koji zapisuje promjene na datotekama i direktorijima u NTFS particijama moguće je pronaći zapise o kreiranju, brisanju, sažimanju, kriptiranju, prebrisavanju i sličnom. Prema zapisima *$UsnJrnl* menadžer je preimenovao više datoteka.

Tablica 8. - Prikaz djela datoteka s promijenjenim nazivom

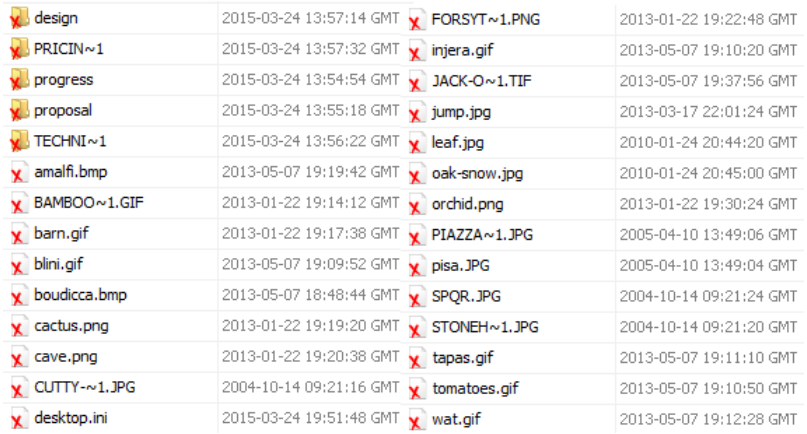
| Stari naziv | Novi naziv |
|---|---|
| [secret_project]_detailed_proposal.docx | landscape.png |
| [secret_project]_design_concept.ppt | space_and_earth.mp4 |
| [secret_project]_detailed_design.pptx | winter_whether_advisory.zip |
| (secret_project)_pricing_decision.xlsx | happy_holiday.jpg |
| (secret_project)_price_analysis_#2.xls | my_favorite_cars.db |
| (secret_project)_price_analysis_#1.xlsx | my_favorite_movies.7z |
| (secret_project)_market_shares.xls | super_bowl.avi |
| (secret_project)_market_analysis.xlsx | new_years_day.jpg |
| [secret_project]_final_meeting.pptx | do_u_wanna_build_a_snow_man.mp3 |
| [secret_project]_technical_review_#1.docx | diary_#1d.txt |
| [secret_project]_technical_review_#1.pptx | diary_#1p.txt |

| | |
|---|---|
| [secret_project]_technical_review_#2.docx | diary_#2d.txt |
| [secret_project]_technical_review_#2.ppt | diary_#2p.txt |
| [secret_project]_technical_review_#3.doc | diary_#3d.txt |
| [secret_project]_technical_review_#3.ppt | diary_#3p.txt |
| ... | ... |

Izvor: autor

U ovom trenutku nastavlja se s analiziranjem, ne prvog autoriziranog USB uređaja, već drugog kako bi se utvrdilo da li se prilikom priključka istog u računalo kopirali osjetljivi podaci firme. Sami dokazi da su podaci kopirani na neautorizirani USB uređaj moguće je utvrditi pronalaskom podataka na USB uređaju. Pregledom USB uređaja RM#2 otkriveno je više izbrisanih direktorija i razne datoteke.

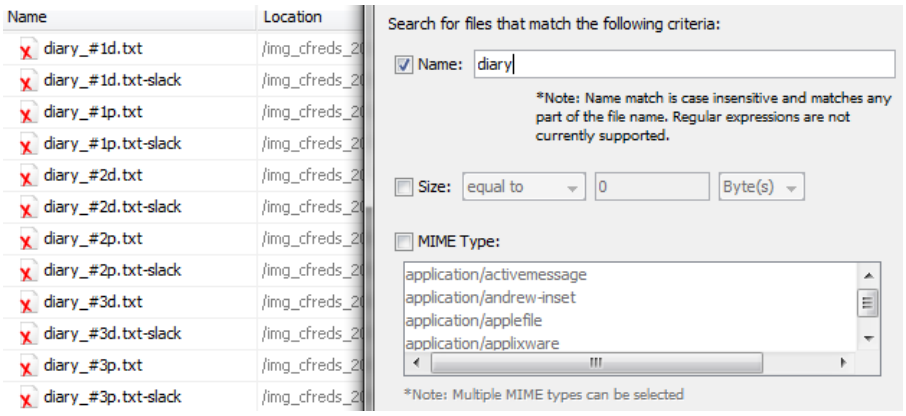
Slika 35. - Prikaz direktorija i datoteka na RM#2 USB uređaju




Izvor: autor

Iako izbrisane datoteke na prvi pogled mogu izgledati sumnjivo, utvrđeno je da većina datoteka koje se nalaze u početnom direktoriju nisu sumnjivi podaci već razni, za ovaj slučaj, nebitni podaci. Zahvaljujući prije uočenim preimenovanjima specifičnih datoteka, s lakoćom je moguće pretražiti USB uređaj.

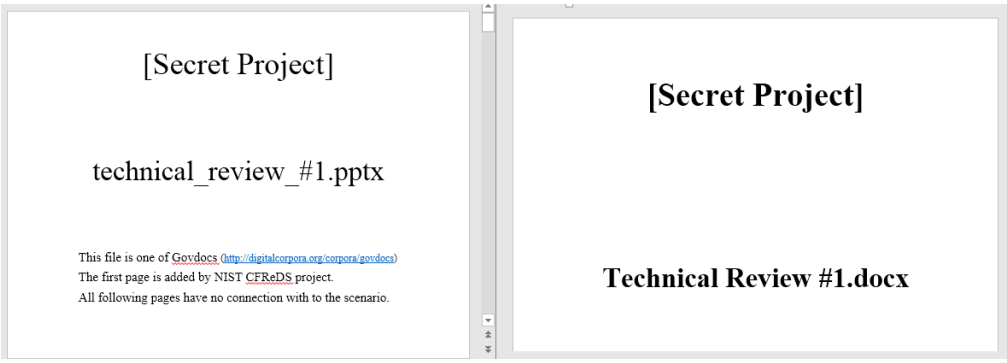
Slika 36. - Prikaz rezultata pretraživanja po nazivu “diary”




Izvor: autor

Iako Autopsy može i izbrisane datoteke prikazati u svojem sučelju, te je moguće prikazati njihov sadržaj, Autopsy također omogućuje izvoz ovih datoteka u forenzički sistem kako bi mogli promijeniti tip datoteke i pogledati ih u originalnom formatu.

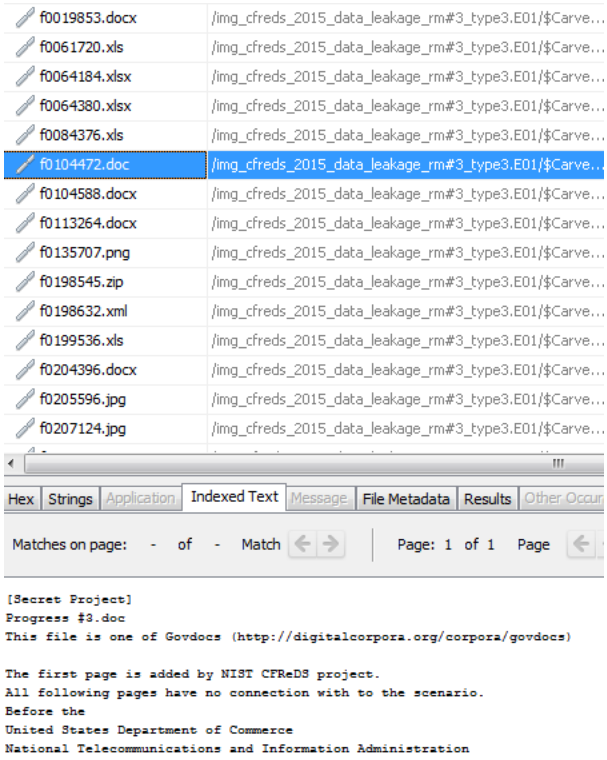
Slika 37. - Prikaz osjetljivih podataka organizacije




Izvor: autor

Posljednji medij koji je bilo potrebno analizirati je CD-R optički mediji. Ovaj mediji je morao biti u Autopsy učitan kao nedodijeljen prostor. Autopsy ovakav prostor analizira i pronalazi tragove datoteka koje je zatim moguće izdvojiti, otvoriti i slično.

Slika 38. - Prikaz prepoznatih datoteka iz nedodijeljenog prostora



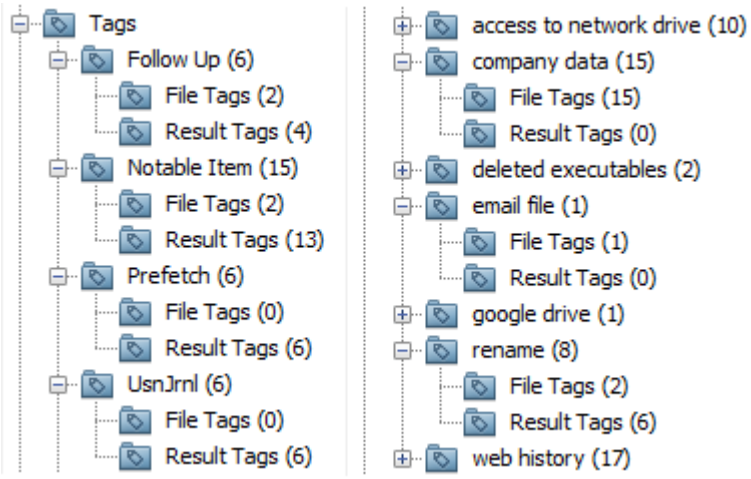

Izvor: autor

Ove datoteke također je uz pomoć Autopsy-a izvući na forenzičko računalo, te tako pregledati sadržaj u originalnom obliku.

### 5.1.4. Izrada izvještaja analize

Kroz proces cijele analize u Autopsy-u su označene informacije koji su relevantne za slučaj. Forenzičari imaju mogućnost korištenja predefiniranih oznaka ili kreiranja vlastiti s mogućnosti dodavanja komentara. Označivanje je moguće za datoteku ili rezultate, zavisno o potrebama.

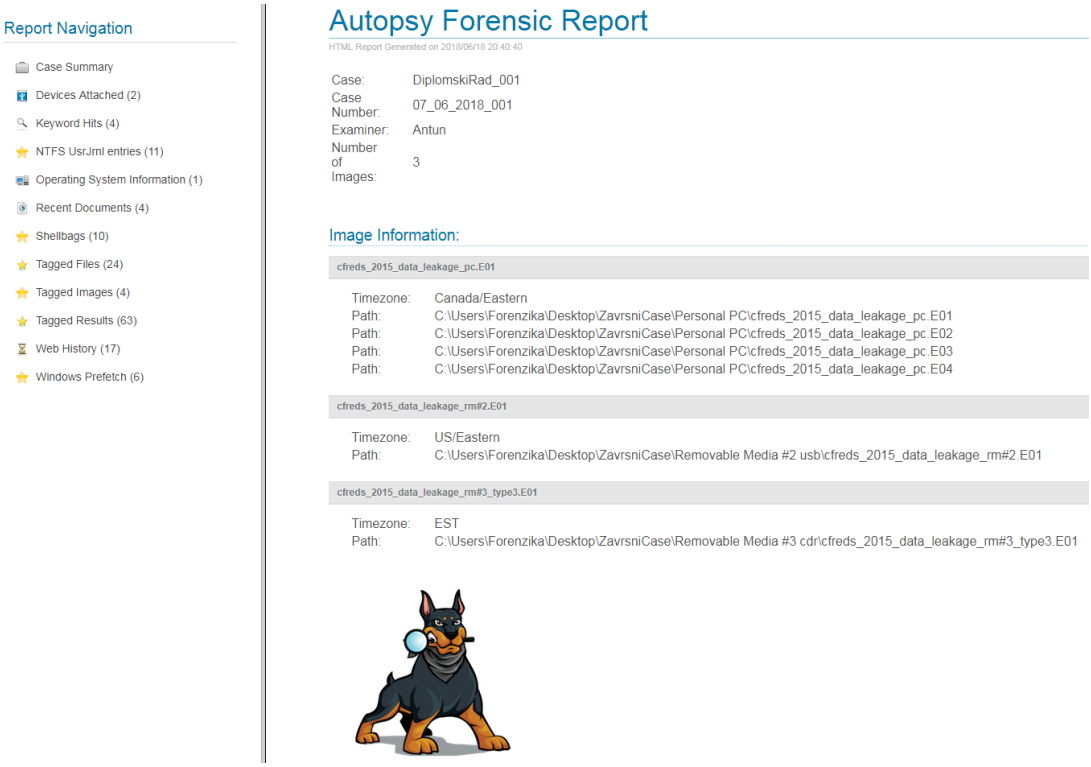
Slika 39. - Prikaz oznaka




Izvor: autor

Prilikom generiranja izvještaja oznake se koriste kao sadržaj za izvještaj. Forenzičar tako u procesu analize mora za dobivanje izvještaja redovito obilježavati oznakama svoje pronalaske.

Slika 40. - Prikaz generiranog izvještaja u HTML obliku




Izvor: autor

## 5.2. Digitalna forenzika korištenjem komercijalnog alata Forensic Explorer

Forensic Explorer je forenzički alat za očuvanje, analizu i prezentaciju elektroničkih dokaza primarno korišten od službenika za provođenje zakona, vlada, vojske i korporativnih istražitelja. Ovaj alat kombinira grafičko sučelje s naprednim funkcionalnostima za sortiranje, pretraživanje ključnih riječi, pregledavanje i pisanje skripti. Tako ovaj alat omogućuje forenzičarima analiziranje velike količine podataka s više elektroničkih medija, pristup i analiziranje svih prikupljenih podataka uključujući i skrivene i sistemske datoteke, izbrisane datoteke i neodijeljenog prostora. Forensic Explorer posjeduje i funkcionalnosti za generiranje detaljnih izvještaja, te može služiti kao platforma za pregledavanje dokaza od strane sudionika sudskih procesa koji ne posjeduju forenzičko znanje.

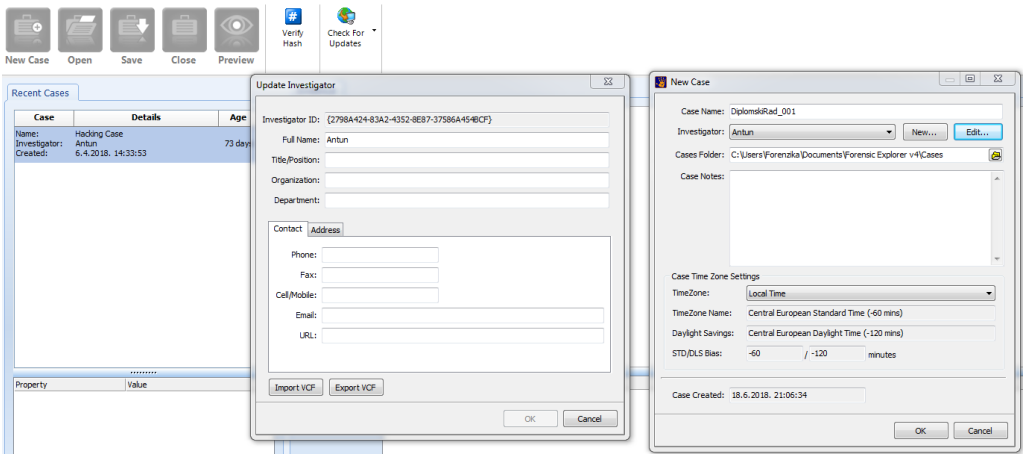
„*Fleksibilno grafičko sučelje s naprednim sortiranjem, filtriranjem, pretraživanjem ključnih riječi, pregledavanjem i skriptnim tehnologijama.“* (Forensic Explorer, 2018.)

Neke od prednosti ovog forenzičkog alata su intuitivno i prilagodljivo sučelje, mogućnost pisanja Delphi, Pascal i Basic skripti, analiza računalne pošte i Windows registra, te mnoge druge. Mana ovakvih specijaliziranih alata koji se plaćaju je cijena koja za navedeni forenzički alat iznosi 1695 američkih dolara.

### 5.2.1. Otvaranje novog slučaja

Pokretanjem forenzičkog alata otvara se njegovo grafičko sučelje u kojem je moguće pregledati prije kreirane slučajeve, otvoriti novi slučaj ali i samo pregledati određene datoteke koje su odabrane za učitavanje. Pritiskom na tipku izrade novog slučaja otvara se skočni prozor u kojem je potrebno upisati opće informacije o slučaju, osobi koja vodi istragu i slično. Ovaj alat traži od istražitelja da upiše svoje informacije, te ih sprema u lokalnu bazu forenzičkih istražitelja. Ove podatke moguće je izvesti ili uvesti, te je time pojednostavljeno unošenje podataka o istražiteljima između slučaja.

Slika 41. - Otvaranje slučaja u Forensic Explorer-u



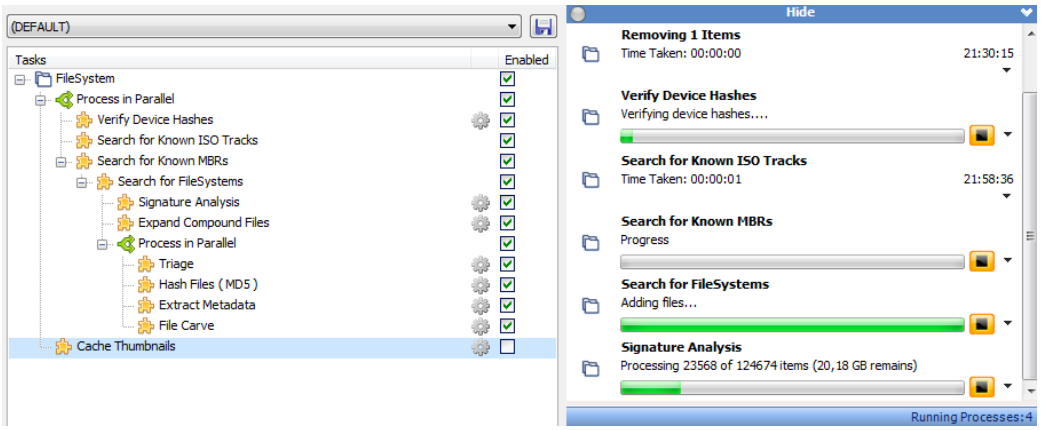

Izvor: autor

### 5.2.2. Dodavanje dokaza

U trenutku kada je otvoren slučaj, forenzičar ima mogućnost odabira između dodavanja raznih vrsta datoteka. Ovaj alat omogućuje dodavanje montiranih uređaja, forenzičkih slika, pojedinačnih datoteka, mrežnih mjesta, mapa i grupa. Za svaki od navedenih, podržani su uobičajeni tipovi podataka forenzičkih slika poput *.dd, *.raw, *.E01, *.vmdk i slične. Uz navedene alat podržava i formate drugih forenzičkih alata odnosno tvrtki poput *.mfs (*NUIX*), *.crt (*Xway Container*), *.eve (*ProDiscover*) i druge. U ovom slučaju sve forenzičke slike dokaza su *.E01 formatu.

Odabirom forenzičke slike kao vrste datoteke otvara se prozor za navigaciju do tražene datoteke na forenzičkom računalu, te se odabirom otvara skočni prozor za procesiranje prikupljenih dokaza. Određeni zadaci u procesoru imaju dodatne postavke koje omogućuju istražitelju da ih prilagodi svojim potrebama i vrsti slučaja za koji se izvršava forenzička analiza. Ako je odabrano više zadataka, oni se izvršavaju paralelno kako bi se uštedjelo na vremenu izvršavanja. Ovaj proces izvršen je za sve forenzičke slike koje su prikupljene prilikom sigurnosne provjere na izlasku iz kompanije. Kako svaki put forenzičar ne bi trebao ponovno označivati i postavljati zadatke koje želi da se izvrše alat posjeduje funkciju spremanja odabira modula za ponovno korištenje.

Slika 42. - Prikaz procesora dokaza i njihovog izvršavanja




Izvor: autor

Nakon izvršenja zadataka u procesnom modulu za svaku forenzičku sliku izračunava se verifikacijska *hash* oznaka koja se treba podudarati s oznakom napravljenom prilikom prikupljanja dokaza.

Slika 43. - Prikaz podudaranja *hash* oznaka

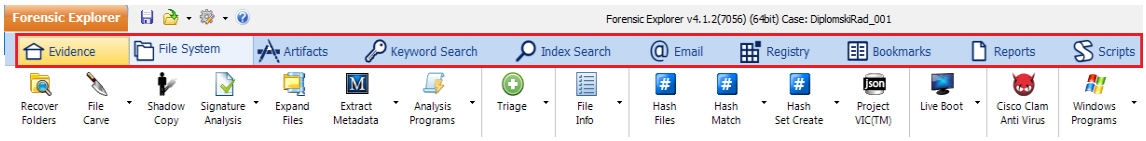
| | |
|---|---|
| Acquisition Hash (MD5) | a49d1254c873808c58e6f1bcd60b5bde |
| Acquisition Hash (SHA1) | afe5c9ab487bd47a8a9856b1371c2384d44fd785 |
| Verification Hash (MD5) | a49d1254c873808c58e6f1bcd60b5bde |
| Acquisition Hash (MD5) | b4644902acab4583a1d0f9f1a08faa77 |
| Acquisition Hash (SHA1) | 04896 1a85ca3eced8cc73f1517442d31d4dca0a3 |
| Verification Hash (MD5) | b4644902acab4583a1d0f9f1a08faa77 |
| Acquisition Hash (MD5) | df914108fb3d86744eb688eba482fbdf |
| Acquisition Hash (SHA1) | 7f3c2eb1f1e2db97be6e963625402a0e362a532c |
| Verification Hash (MD5) | df914108fb3d86744eb688eba482fbdf |

Izvor: autor

### 5.2.3. Forenzička analiza

Nakon što je procesor dokaza završio sa zadacima, forenzičar može započeti s forenzičkom analizom prikupljenih dokaza. Forensic Explorer svoje grafičko sučelje ima podijeljeno u više modula od kojih svaki sadrži prilagođene procesne radnje i preglede za specifične dijelove analize. Alat sadrži module za datotečni sustav, artefakte, traženje ključnih riječi, traženje prema indeksima, modul za računalnu poštu, registre, oznake, izvještaj i skripte. Iako su ovi moduli odvojeni, istražitelj može iz početnog podatkovnog modula izvoziti odabrane datoteke u druge.

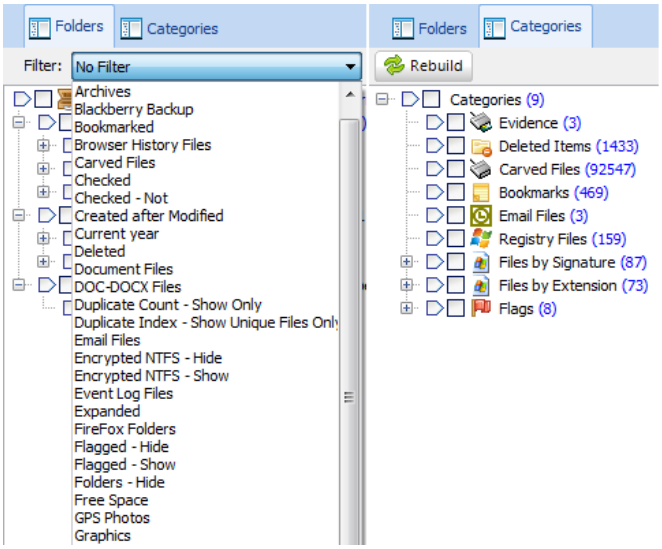
Slika 44. - Prikaz modula




Izvor: autor

U modulu datotečnog sustava s lijeve strane nalazi se struktura svih prikupljenih uređaja od particija do datoteka koje se nalaze u njima. Ovu strukturu direktorija moguće je filtrirati prema predefiniranim kategorijama čime se znatno može uštedjeti vrijeme pronalazak specifičnih datoteka. Uz navedeno FEX (*Forensic Explorer*) automatski kategorizira datoteke koje su prepoznate prilikom procesiranja dokaza.

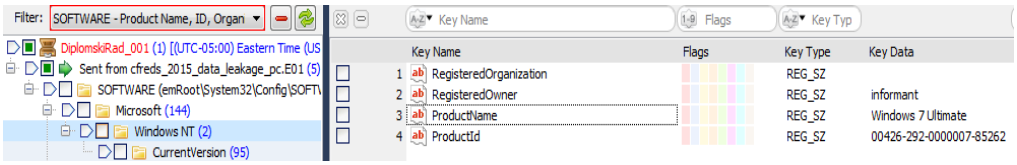
Slika 45. - Filtriranje i kategoriziranje




Izvor: autor

Na samom početku forenzičke analize tražit će se informacije o sustavu koje se nalaze u Windows registru „SOFTWARE“. Jednostavnom primjenom filtriranja direktorija odabirom datoteka registra prikazuju nam se samo direktoriji koji sadrže iste. Kako bi se ove datoteke prebacile u modul registra potrebno ih je označiti, te odabrati opcije slanje u modul registra. Odabirom modula registra može se vidjeti originalna struktura Windows registra i svi poslani ogranci.

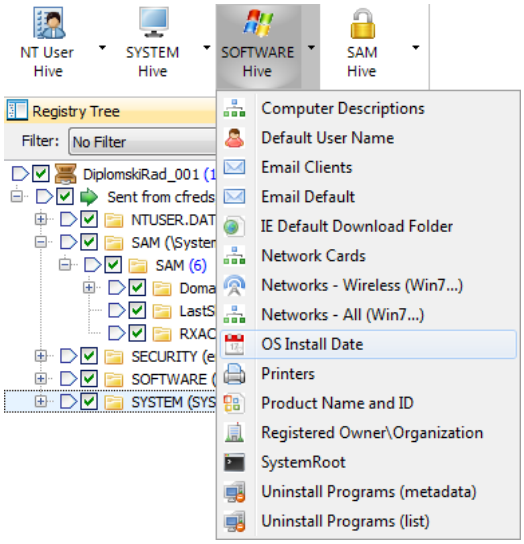
Slika 46. - Prikaz informacija o sustavu iz registra




Izvor: autor

Osim ovakvog pristupa traženju podataka, ovaj alat također omogućuje forenzičaru da pokrene integrirane skripte koje raščlanjuju informacije iz odabranih ogranka registra.

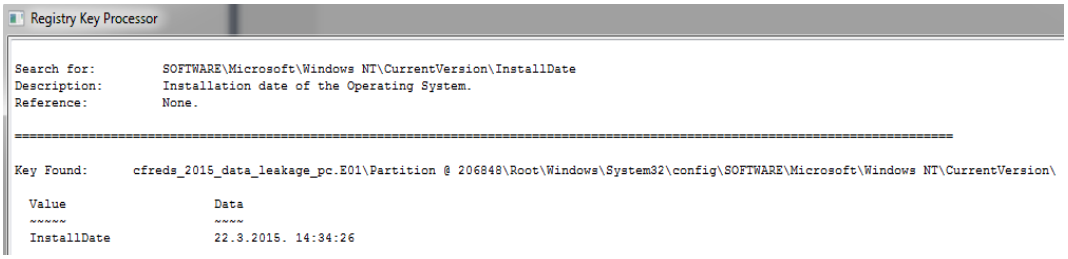
Slika 47. - Prikaz mogućnosti za raščlanjivanje registra




Izvor: autor

Nakon što se zadatak izvrši u FEX-u se pojavljuje skočni prozor s rezultatom, te je kreiran zapis o izvršenom zadatku i rezultatu.

Slika 48. - Prikaz zapisa s rezultatima




Izvor: autor

U nastavku će se raščlaniti ključni podaci iz poslanih ogranak registra za koje ovaj alat sadrži integrirane skripte. Zavisno o jačini forenzičke stanice ovi zadaci mogu se odvijati paralelno.

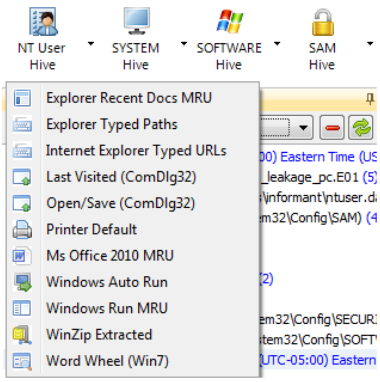
Tablica 9. - Prikaz informacija o sustavu iz registra

| | |
|---|---|
| Disk sustava | C:\Windows |
| Naziv sustava | Windows 7 Ultimate |
| Identifikacijska oznaka proizvoda | 00426-292-0000007-85262 |
| Registrirani vlasnik | informant |
| Datum instaliranja | 22.3.2015. 14:34:26 (GTM) |
| Naziv mrežne kartice | Intel(R) PRO/1000 MT Network Connection |
| Klijent računalne pošte | Microsoft Outlook |
| Vremenska zona | Eastern Standard Time |
| Naziv računala | INFORMANT-PC |
| Posljednje gašenje sustava | 25.3.2015. 15:31:05 (GMT) |
| Zadnji prijavljeni korisnik | informant |
| Broj prijava korisnika „informant“ | 10 |

Izvor: autor

U modulu registra također postoje procesi za raščlanjivanje NTUSER ogranka. Neki od procesa koji su forenzičaru na izboru su analiziranje često korištenih aplikacija, upisanih adresa u Internet Explorer-u, posječene Windows Explorer putanje i slično.

Slika 49. - Mogućnosti za raščlanjivanje NTUSER ogranka registra




Izvor: autor

Raščlanjivanjem nedavno otvorenih dokumenata i direktorija moguće je vidjeti da je menadžer Iaman Informant nedavno otvarao osjetljive dokumente firme, te da je pristupao optičkom mediju.

Tablica 10. - Prikaz nedavno otvorenih datoteka i direktorija

| |
|---|
| [secret_project]_proposal.docx |
| [secret_project]_design_concept.ppt |
| (secret_project)_pricing_decision.xlsx |
| pricing decision |
| [secret_project]_final_meeting.pptx |
| winter_whether_advisory.zip |
| BD-RE Drive (D:) |
| Penguins.jpg |
| Koala.jpg |
| Tulips.jpg |
| BD-RE Drive (D:) IAMAN CD |
| Resignation_Letter_(Iaman_Informant).xps |
| Resignation_Letter_(Iaman_Informant).docx |

Izvor: autor

U modulu artefakta na izboru forenzičar ima razne mehanizme za raščlanjivanje podataka o preglednicima, razgovorima, artefakata mobilnih uređaja, operacijskom sustavu, socijalnim mrežama i sličnog. Forenzičar ima mogućnost odabira zasebnih mehanizama ili pokretanje svih u isto vrijeme.

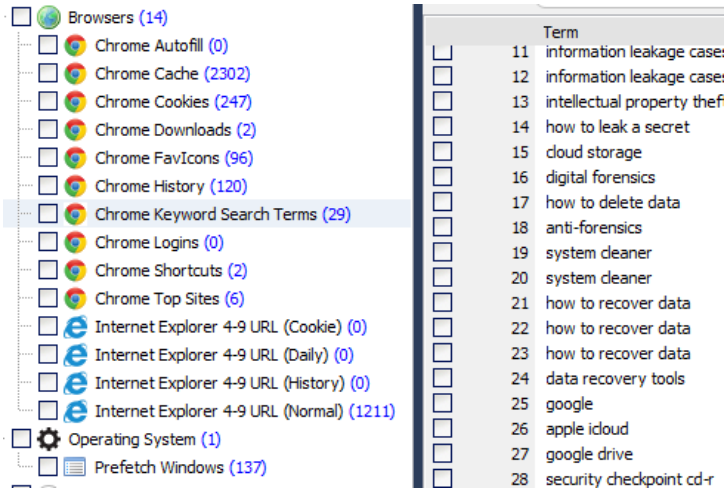
Slika 50. - Prikaz mogućnosti modula za artefakte


Izvor: autor

Korištenjem ovakvog pristupa vrlo je jednostavno i brzo isključiti aplikacije koje nisu bile korištene na sustavu pošto ne postoji zapis o istima. Rezultatima ove analize zaključeno je da

korisnik računala „informant“ nije koristio aplikacije za socijalne mreže, te da nije koristio aplikacije za razgovore. Rezultati su također pokazali ostatke Gmail servisa u nedodijeljenom prostoru, te su pronađeni dokazi o korištenju preglednika Internet Explorer i Google Chrome. Svi rezultati prikazani su sortirano u razgranatom prikazu FEX alata, te je iz navedenih rezultata moguće pregledati uobičajene artefakte koji za sobom ostavljaju preglednici.

Slika 51. - Prikaz pretraživanja iz artefakta preglednika




Izvor: autor

Analizom artefakta operacijskog sustava ovim modulom dobiveni su si rezultati često pokrenutih aplikacija iz *Prefetch* artefakta Windows sustava. Na ovaj način možemo utvrditi korištenje prije navedenih preglednika ali i specijaliziranih alata za prebrisavanje podataka koji se često koriste za skrivanje dokaza.

Slika 52. - Prikaz “Prefetch” zapisa o pokrenutim programima

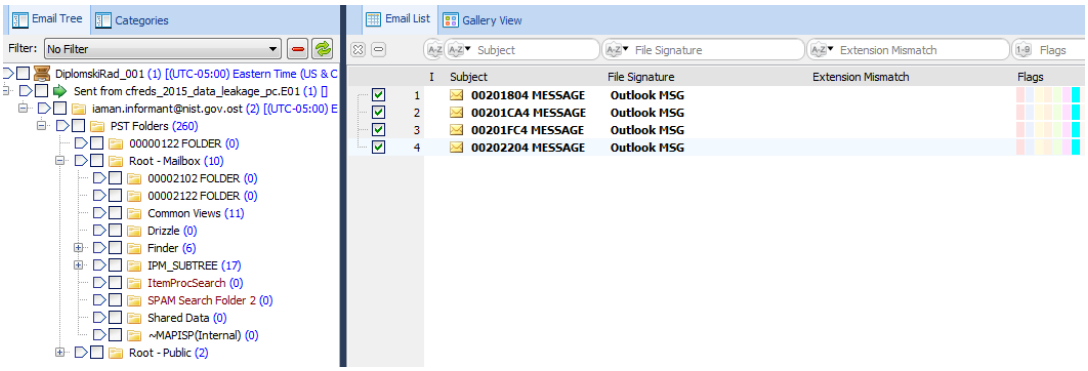
| | Windows Prefetch Filename | Windows Prefetch... | Flags | Windows Prefetch Exe... | Windows Prefetch Execution Count |
|---|---|---|---|---|---|
| 1 | CHROME.EXE | D999B1BA | 8 | | 71 |
| 2 | IEXPLORE.EXE | 4B6C9213 | 8 | | 12 |
| 3 | ERASER.EXE | CE61944A | 8 | | 2 |
| 4 | CCLEANER64.EXE | 779BD542 | 8 | | 2 |

Izvor: autor

Povratkom u modul datotečnog sustava i odabirom predefiniranog filtera za pronalaženje datoteka računalne pošte kao dobiveni rezultat je prikazana „iaman.informant@nist.gov.ost“

datoteka. Odabirom ove datoteke, te njenim slanjem u modul računalne pošte moguće je otvoriti sam sadržaj u ovom forenzičkom alatu ali ne i prikazati same poruke na ovaj način.

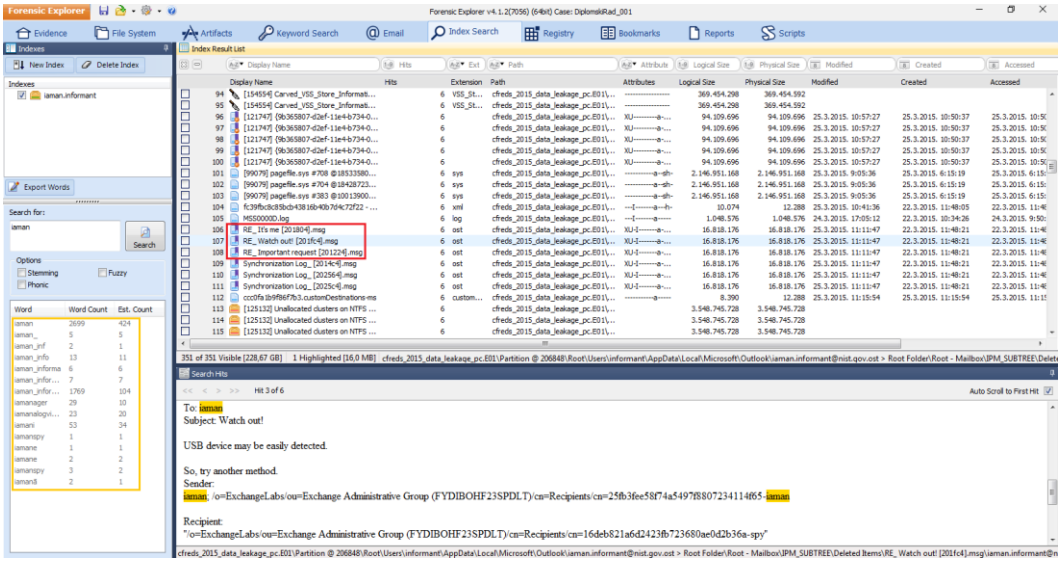
Slika 53. - Prikaz otvorene *.ost datoteke i njene strukture




Izvor: autor

Forensic Explorer posjeduje mehanizme za pretraživanje putem indeksa, odnosno odabirom ove opcije i dokaza, kreira se baza podataka svih riječi koji se nalaze u dokazu. Jednom kada je kreirana ovakva baza pretraživanje riječi gotovo je trenutačno. Ovim mehanizmom vrlo je jednostavno pretražiti sve dokaze s ključnim riječima slučaja. Na navedeni način upisom imena „iaman“ pronađene su poruke računalne pošte između sumnjivca.

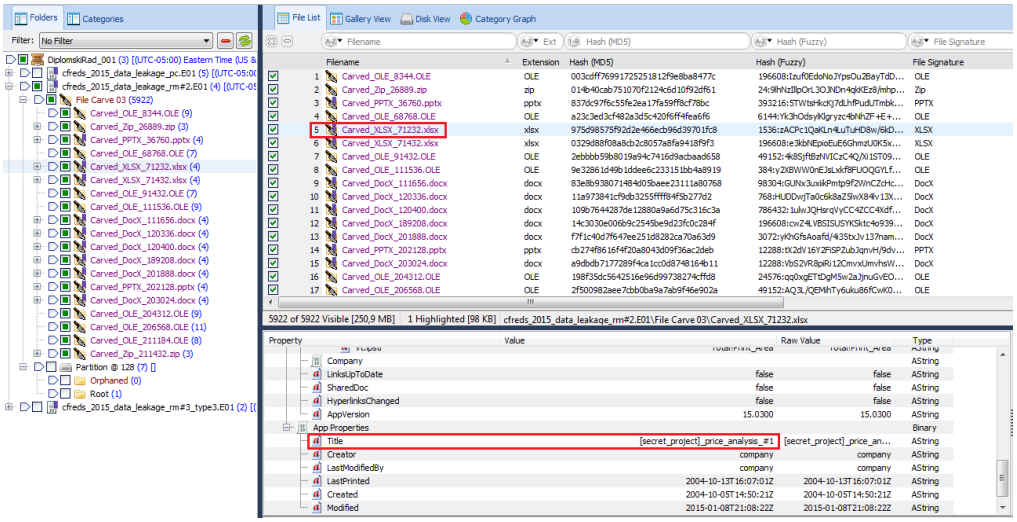
Slika 54. - Prikaz pretraživanja putem indeksa




Izvor: autor

U nastavku analize, na USB uređaju RM#2 i optičkom mediju RM#3 pronađene su tragovi izbrisanih datoteka. Iako ovi dokumenti nemaju iste nazive, uobičajeni formati Microsoft Office paketa uz sam sadržaj podataka sadrže i podatke o podacima. FEX alat je prepoznao njihovu strukturu, te podatke o podacima koji su pohranjeni uz njih. Ako podaci o podacima nisu izbrisani iz njih je moguće vidjeti originalne nazive dokumenata.

Slika 55. - Prikaz osjetljivih firminih datoteka na USB uređaju



Izvor: autor

Dodatno FEX alat sadrži mehanizme za uspoređivanje *hash* vrijednosti, ali pošto je vidljivo da je sumnjivac izmijenio nazive i tipove podataka, *hash* vrijednosti su također promijenjene jer se promjenom jednog bita mijenja *hash* vrijednost. Upravo iz ovog razloga koristi se *Fuzzy Hash* metoda kojom se uspoređuje sličnost između datoteka.

Slika 56. - Prikaz rezultata podudaranja *Fuzzy Hash*-a

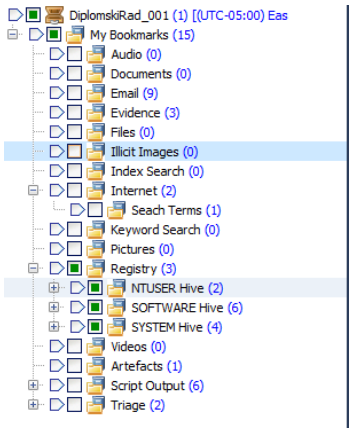
```
SOURCE FILE:  27       === BATES: 236033    cfreds_2015_data_leakage_rm#2.E01\File Carve 03\Carved_PPTX_36760.pptx
 Score = 100 --> Bates: 238521    Carved_PPTX_29724.pptx

--------------------------------------------------------------------------------------------------------------------------------
SOURCE FILE:  29       === BATES: 236047    cfreds_2015_data_leakage_rm#2.E01\File Carve 03\Carved_XLSX_71232.xlsx
 Score = 100 --> Bates: 238523    Carved_XLSX_64184.xlsx

--------------------------------------------------------------------------------------------------------------------------------
SOURCE FILE:  30       === BATES: 236048    cfreds_2015_data_leakage_rm#2.E01\File Carve 03\Carved_XLSX_71432.xlsx
 Score = 100 --> Bates: 238524    Carved_XLSX_64380.xlsx

--------------------------------------------------------------------------------------------------------------------------------
SOURCE FILE:  37       === BATES: 238521    cfreds_2015_data_leakage_rm#3_type3.E01\File Carve 04\Carved_PPTX_29724.pptx
 Score = 100 --> Bates: 236033    Carved_PPTX_36760.pptx

--------------------------------------------------------------------------------------------------------------------------------
SOURCE FILE:  38       === BATES: 238523    cfreds_2015_data_leakage_rm#3_type3.E01\File Carve 04\Carved_XLSX_64184.xlsx
 Score = 100 --> Bates: 236047    Carved_XLSX_71232.xlsx

--------------------------------------------------------------------------------------------------------------------------------
SOURCE FILE:  39       === BATES: 238524    cfreds_2015_data_leakage_rm#3_type3.E01\File Carve 04\Carved_XLSX_64380.xlsx
 Score = 100 --> Bates: 236048    Carved_XLSX_71432.xlsx
```

Izvor: autor

### 5.2.4. Izrada izvještaja analize

Kroz cijeli proces forenzičke analize forenzičar u Forensic Explorer alatu ima mogućnosti obilježavanja relevantnih dokaza. Kao izbor ima označivanje „zastavama“ u raznim bojama te postavljanje oznaka nad određenim datotekama. Alat sadrži već predefinirane oznake ali i mogućnost kreiranja novih, slučaju prilagođenih oznaka, koje je moguće sortirati u mape.

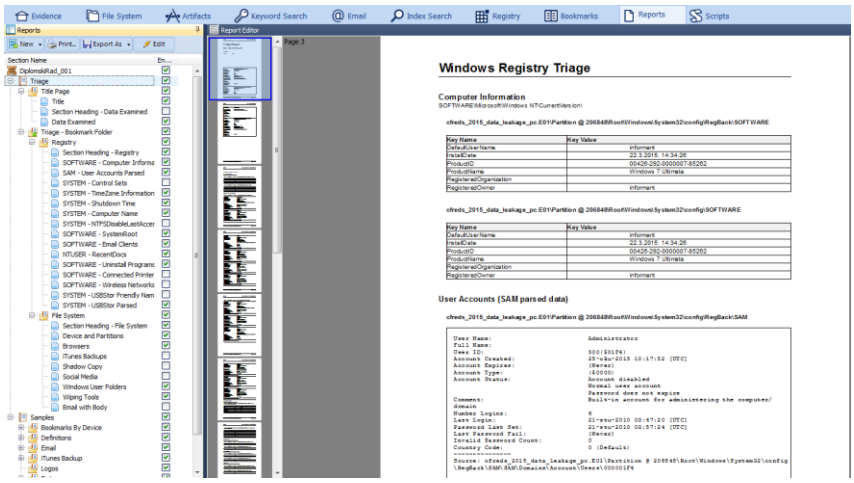
Slika 57. - Prikaz oznaka u modulu oznaka




Izvor: autor

Oznake se osim za lakše snalaženje tijekom analize koriste za formiranje izvještaja forenzičke analize. FEX u modulu izvještaja omogućuje forenzičaru izradu izvještaja od početka ili putem već predefiniranog izgleda. Uz navedeno alat pruža grafičko sučelje za prilagodbu izvještaja prema specifičnom slučaju.

Slika 58. - Prikaz sučelja za izradu izvještaja




Izvor: autor

## 5.3. Usporedba rezultata forenzičke analize i alata

Oba forenzička alata, Autopsy i Forensic Explorer, omogućili su u ovom specifičnom slučaju ilegalnog izvlačenja uredskih podataka, pretraživanje i identifikaciju ključnih dokaza za otvaranje sudskog proces kojim će biti utvrđena krivnja sumnjivca Iaman Informant-a. Kroz proces analize s oba programa pronađeni su dokazi ilegalnog kopiranja podataka, te njihovo prebacivanje na medije za pohranu podataka koji su zatim pronađeni na sigurnosnoj provjeri prilikom izlaza iz firme. Prema sigurnosnim pravilima iste firme, samo posjedovanje neautoriziranih medija prilikom sigurnosne provjere spada pod kršenje istih, ali utvrđivanje postupaka koji su izvršeni ključno je kako bi se sa sigurnošću moglo zaključiti počinjenje kaznenog dijela.

Svaki od forenzičkih alata koristi drugačije pozadinske mehanizme za sortiranje i filtriranje podataka pa je potrebno napomenuti da broj prepoznatih rezultata za tipove datoteka i artefakata preglednika, pojedinačnih alata, ovisi o principu rada pozadinskih mehanizama. Nadalje, podudaranjem prikupljenih informacija iz pojedinačnih datoteka od strane oba forenzička alata, potvrđuje se njihova ispravnost.

Tablica 11. - Usporedba broja prepoznatih uredskih podataka

| Rezultati prema tipu datoteke | Autopsy | Forensic Explorer |
|---|---|---|
| *.html (*Hypertext Markup Language*) | 437 | 434 |
| *.docx (Microsoft Word) | 17 | 17 |
| *.xls / xlsx (Microsoft Excel) | 19 | 20 |
| *.ppt / pptx (Microsoft Powepoint) | 7 | 10 |
| *.ost (*Offline Outlook Data File*) | 1 | 1 |
| *.rtf (*Rich Text Format*) | 74 | 431 |
| *.pdf (*Portable Document Format*) | 2 | 2 |

Izvor: autor

Tablica 12. - Usporedba broja prepoznatih artefakata preglednika

| Google Chrome | Autopsy | Forensic Explorer |
|---|---|---|
| Kolačići | 245 | 247 |
| Preuzimanja | 2 | 2 |
| Pretraživanja | 23 | 29 |
| Povijest | 124 | 120 |
| Predmemorija | - | 2302 |
| Internet Explorer | Autopsy | Forensic Explorer |
| Povijest | 1215 | 1211 |
| Kolačići | 126 | - |
| Pretraživanja | 14 | - |

Izvor: autor

Kroz postupak forenzičke analize korištena je većina funkcionalnosti navedenih forenzičkih alata koje će se u nastavku rada usporediti kao prednosti i mane pojedinog forenzičkog alata.

Tablica 13. - Popis korištenih funkcionalnosti odabranih forenzičkih alata

| Korištene funkcionalnosti | Autopsy | Forensic Explorer |
|---|---|---|
| Verifikaciju *hash* vrijednosti | Posjeduje | Posjeduje |
| Raščlanjivanje Windows registra | Posjeduje | Posjeduje |
| Prikaz strukture Windows registra | Ne posjeduje | Posjeduje |
| Prepoznavanje *Prefetch* artefakata | Eksterni modul | Posjeduje |
| Prepoznavanje artefakta preglednika | Posjeduje | Posjeduje |
| Izvoz odabranih datoteka | Posjeduje | Posjeduje |
| Raščlanjivanje *.ost tipa datoteke | Ne posjeduje | Posjeduje |
| Prepoznavanje *Jump List* artefakata | Eksterni modul | Posjeduje |
| Prepoznavanje *Shellbags* artefakata | Eksterni modul | Ne posjeduje |
| Prepoznavanje *Shimcache* artefakata | Eksterni modul | Ne posjeduje |
| Prepoznavanje nedavno otvorenih dokumenata | Posjeduje | Posjeduje |
| Pretraživanje po ključnim riječima | Posjeduje | Posjeduje |
| Pretraživanje po indeksima | Posjeduje | Posjeduje |
| Sortiranje prema tipovima datoteka | Posjeduje | Posjeduje |
| Prepoznavanje izbrisanih datoteka | Posjeduje | Posjeduje |
| Prikaz strukture direktorija forenzičke slike | Posjeduje | Posjeduje |
| Označivanje relevantnih dokaza | Posjeduje | Posjeduje |
| Generiranje izvještaja | Posjeduje | Posjeduje |
| Izrada prilagođenog izvještaja | Ne posjeduje | Posjeduje |
| Dodavanje eksternih skripti i modula | Posjeduje | Posjeduje |
| Usporedba MD5 *hash* vrijednosti | Posjeduje | Posjeduje |
| Usporedba putem *Fuzzy Hash* vrijednosti | Ne posjeduje | Posjeduje |

Izvor: autor

Iako oba forenzička alata posjeduju pojedine funkcionalnosti koje u drugome nisu dostupne forenzičari poznavanjem lokacija pojedinih podataka mogu samostalno doći do istih, te kroz razne vrste prikaza mogu pregledati relevantne informacije.

Tablica 14. - Mogućnosti prikaza pojedinih datoteka u forenzičkim alatima

| Vrste prikaza | Autopsy | Forensic Explorer |
|---|---|---|
| Heksadecimalni prikaz | Posjeduje | Posjeduje |
| *String* prikaz | Posjeduje | Posjeduje |
| Aplikacijski prikaz | Posjeduje | Ne posjeduje |
| Indeksiran tekst | Posjeduje | Posjeduje |
| Prikaz podataka o podacima | Posjeduje | Posjeduje |
| Prikaz rezultata | Posjeduje | Ne posjeduje |
| Prikaz *byte* strukture | Ne posjeduje | Posjeduje |
| Zapis datotečnog sustava | Ne posjeduje | Posjeduje |
| Prikaz lokacije na disku | Ne posjeduje | Posjeduje |
| Prikaz vremenske linije | Posjeduje | Posjeduje |
| Galerijski prikaz | Posjeduje | Posjeduje |
| Diskovni prikaz | Ne posjeduje | Posjeduje |
| Kategorijski prikaz | Ne posjeduje | Posjeduje |

Izvor: autor

# 6. Zaključak

Kako bi se uspješno obrađivale sve veće količine podataka, te smanjilo vrijeme za obradu istih, uredsko poslovanje prati trendove digitalizacije i automatizacije. Danas je cilj postići automatizirano uredsko poslovanje i isključiti papirologiju uz pomoć procesa podržanih informacijsko komunikacijskom tehnologijom. Ove trendove prate pojedinci koji žele profitirati i nanijeli štetu organizacijama koristeći pojedine slabosti digitalnih tehnologija. Kako bi se utvrdila kriminalna radnja i pronašli digitalni dokazi u danas sve većoj količini digitalnih podatka, taži se pomoć stručnjaka iz područja digitalne forenzike. Njihov zadatak je identifikacija, pronalazak, očuvanje, analiza i prezentacija digitalnih dokaza počinjenih kriminalnih radnji. Iako su poslovne organizacije sve više svjesne rizika i mogućnosti nastajanja šteta u milijunskim iznosima, pojedinci koji posjeduju znanje iz računalnih tehnologija, mogu kroz korištenje razni programa nanijeti veliku štetu istima. Korištenjem standardnih forenzičkih metoda i specijaliziranih forenzičkih programa digitalni forenzičari mogu u većini slučaja pronaći potrebne dokaze za izvođenje sudskog procesa. Forenzičari na raspolaganju danas imaju raznovrsne komercijalne programe poput Forensic Explorer-a i programe otvorenog koda kao što je Autopsy, koji im omogućavaju analiziranje prikupljenih digitalnih dokaza. Prilikom pokušaja izvlačenja osjetljivih uredskih podataka i prikrivanjem dokaza anti-forenzičkim metodama, uz navedene programe i stručnost forenzičara, moguće je utvrditi postupke sumnjivca za utvrđivanje krivnje pojedinaca u sudskom procesu. Usporedbom korištenih forenzičkih alata prikazane su njihove prednosti i mane, te je utvrđeno da je korištenjem istih moguće prikupiti dokaze koji potvrđuju počinjenje kaznenog dijela ilegalnog izvlačenja osjetljivih uredskih podataka.

# POPIS KRATICA

1. ERP - Enterprise Resource Planning
2. WWW - World Wide Web
3. GDPR - General Data Protection Regulation
4. PDF - Portable Document Format
5. FBI - The Federal Bureau of Investigation
6. CART - Computer Analysis and Response Team
7. NTFS - New Technology File System
8. URL - Uniform Resource Locator
9. MRU - Most Recently Used
10. MAC - Media Acces Control
11. CAM - Content Addressavle Memory
12. GPS - Global Positioning System
13. GSM - Global System for Mobile communications
14. ICC-ID - Integrated Circuit Card Identifier
15. IMSI - International Mobile Subscriber Identity
16. SIM - Subscriber Identity Modul
17. PIN - Personal Identification Number
18. IMEI - International Mobile Equipment Identity
19. LAN - Local Area Network
20. PDA - Personal Digital Assistant
21. SMTP - Simple Mail Transfer Protocol
22. POP - Post Office Protocol
23. IMAP - Internet Message Access Protocol
24. USB - Universal Serial Bus
25. IM - Instant Messages
26. GREP - Globally search a Regular Expression and Print
27. CRC - Cyclic Redundancy Check
28. MD5 - Message Digest 5
29. SHA - Secure Hash Algorithm
30. HTML - Hyper Text Markup Language

31. DRM - Digital Rights Management
32. DLP - Data Loss Prevention
33. TSK - The Sleuth Kit
34. DD - DiskDoubler Archive files
35. RAW - Raw Image Dana
36. E01 - Encase Image File Format
37. VMDK - Virtual Machine Disk
38. CD-R - Compact Disc-Recordable
39. UDF - Universal Disk Format
40. UTC - Coordinated Universal Time
41. SID - Security Identifier
42. RID - Relative ID
43. OST - Offline Outlook Data File
44. $UsnJrnl - Update Sequence Number Journal
45. FEX - Forensic Explorer
46. PDF - Portable Document Format

# POPIS LITERATURE


1. Association of Chief Police Officers, ACPO Good Practice Guide for Digitial Evidence, verzija pet, 2012.
2. CERT, Metode zaštite dokumenata, 2010., https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-04-296.pdf, (27.5.2018.)
3. CIS, Računalna forenzika, 2015., https://www.cis.hr/WikiIS/doku.php?id=forenzika_naslovnica, (29.5.2018.)
4. Eoghan Casey, Digital Evidence and Computer Crime, treće izdanje, Elsevier, Maryland, 2011.
5. International Association of Computer Investigative Specialists, Basic Computer Forensic Examiner, 2017.
6. International Association of Computer Investigative Specialists, Network Forensics, 2014.
7. John R. Vacca, Computer Forensic: Computer Crime Scene Investigation, drugo izdanje, Charles River Media, Boston, 2005.
8. Metropolitan Police, Basic Phone Forensics, 2015.
9. Mohay G. et al, Computer and Intrusion Forensic, Artech House, Boston, 2003.
10. Narodne novine, Zakon o kaznenom postupku (NN 152/2008), https://narodne-novine.nn.hr/clanci/sluzbeni/2008_12_152_4149.html (05.5.2018.)
11. Narodne novine, Uredba o uredskom poslovanju (NN 7/2009), https://narodne-novine.nn.hr/clanci/sluzbeni/2009_01_7_171.html (25.5.2018.)
12. Odgers P., Administrative Office Management, trinaesto izdanje, Cengage Learning, Flagstaff, 2005.
13. Rongala A., The Paperless Office: Document Process Automation is the Way, 2014, https://invensis.net/blog/data-processing/paperless-office-document-process-automation-way/ (25.5.2018.)
14. SleuthKit, Open Source Digital Forensic, 2016., https://www.sleuthkit.org/autopsy/, (07.6.2018.)
15. Volonino L., Anzaldua R., Computer Forensic For Dummies, Wiley Publishing, Hoboken, 2008.

16. Ward S., 3 Steps to Creating a Document Management System, 2018., https://www.thebalancesmb.com/creating-a-document-management-system-2948084 (25.5.2018.)

# POPIS SLIKA

# POPIS TABLICA