DIGITALNA FORENZIKA I NJENA PRIMJENA

Bogut, Filip

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Stručni diplomski studij Elektrotehnika

FILIP BOGUT

Z A V R Š N I R A D

DIGITALNA FORENZIKA I NJENA PRIMJENA

Split, veljača 2024.

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Stručni diplomski studij Elektrotehnika

Predmet: Sigurnost mreža i usluga

Z A V R Š N I R A D

Kandidat: Filip Bogut

Naslov rada: Digitalna forenzika i njena primjena

Mentor: dr.sc. Tonko Kovačević, prof. st.

Split, veljača 2024.

Sadržaj

Digitalna forenzika i njena primjena

Sažetak:

U ovom radu je obrađena tema digitalne forenzike, grane znanosti koja je u sve većem razvitku i susreće se sa stalnim izazovima. Ukratko su objašnjene tri vrste digitalne forenzike. Sukladno tome, odrađeni su i neki konkretni primjeri uz pomoć forenzičkih alata. Korišteni programi su Wireshark, Autopsy, PhotoME i OSForensics.

Ključne riječi: Digitalna forenzika, Wireshark, Autopsy, PhotoME, OSForensics

Digital forensics and its application

Summary:

This paper deals with the topic of digital forensics, a branch of science that is constantly developing and faces constant challenges. Three types of digital forensics are briefly explained. Accordingly, some concrete examples were worked out with the help of related forensics tools. Wireshark, Autopsy, PhotoME and OSForensics programs were used.

Key words: Digital forensics, Wireshark, Autopsy, PhotoME, OSForensics

1. UVOD U DIGITALNU FORENZIKU

Uz forenziku najčešće vežemo pojmove: otisci prstiju, tragovi oružja, DNK. Forenzika podrazumijeva određivanje redoslijeda tragova kao i dodjeljivanje vremena, mjesta i osobe pronađenom tragu. Sve od navedenog je u cilju otkrivanja nečeg ne očitog, onog što nije vidljivo na prvi pogled.

Svjedoci smo svakodnevnog i neprekidnog razvoja tehnologije. Možemo je shvatiti kao moćno oružje u našim rukama, međutim može biti usmjerena i protiv nas. Razvoj nam donosi niz prednosti i olakšava razne situacije. S druge strane, povećana je i stopa digitalnog kriminala. Danas je teško pronaći bilo kakvu istragu, a da nije uključena komponenta koja se zove digitalni dokaz. Raste broj slučajeva zlouporabe osobnih i poslovnih računala, računalnih mreža, mobitela, kreditnih kartica itd. Raspon zloupotrebe kreće se od povreda autorskih prava, poslovnih prijevara preko napada na računalne sustave i ilegalnih transakcija pa sve to dječje pornografije.

IT omogućava, ako druga strana nije zaštićena, da se naprave štete velikih razmjera. Uslijed povećanja ovakvog tipa štetnih radnji, a u cilju zaštite, razvila se i digitalna forenzika. Za cilj ima prikupljanje, čuvanje, analizu i dokumentiranje digitalnih dokaza, tj. podataka koji su skladišteni, obrađivani ili prenošeni u digitalnom obliku. Na svjetskoj razini je poznat naziv Cyber kriminal ili u Hrvatskoj računalni kriminal. Pojam digitalne forenzike prvi je put korišten kao sinonim za računalnu forenziku. Međutim, digitalna forenzika je vezana uz istragu bilo kakvog organiziranog kriminala. Ona pomaže tako da otkrije komunikaciju među ljudima. Znanstvenici, ali i ostali stručnjaci iz područja sigurnosti, smatraju kako je upravo ova vrsta kriminala najbrže rastuća prijetnja.

Prvi napad na sigurnost hrvatskog interneta je zabilježen 1994. god. Sukladno tome, godinu iza, osniva se CERT (*eng. Computer Emergency Response Team*) koji je odjel Hrvatske akademske i istraživačke mreže (CARNET). Osnovni zadatak je obrada računalno – sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u Republici Hrvatskoj.

Tvrtke se okreću digitalnom poslovnom modelu. Sukladno tome, rapidno je u porastu količina podataka koja se razmjenjuje i generira među organizacijama, kupcima i partnerima. Povećana je vrijednost digitalnih podataka, koji se smatraju okosnicom međusobnog partnerstva, kako za organizacije, tako i za kriminalne skupine. U toj priči bitnu ulogu ima kibernetička sigurnost. Može se reći da je kibernetička sigurnost zapravo umijeće zaštite raznih sustava od zlonamjernih napada, kao i prijetnji koje nisu uzrokovane ljudskim čimbenikom. Za potpuno razumijevanje ovog koncepta potrebe su godine iskustva, a osnovni cilj državnih vrhova je uputiti stanovništvo u osnove kako bi mogli zaštititi svoj digitalni svijet. Smatra se da su ljudi zapravo najslabija karika kibernetičke sigurnosti. Mnogi napadači favoriziraju manipulaciju ljudima. Drugim riječima, do izražaja dolazi iskorištavanje socijalnog inženjeringa, odnosno iskorištavanja ljudskih pogrešaka za izvođenje napada. U prošlosti, usluge temeljene na oblacima (eng. cloud) bile su korištene samo od strane velikih organizacija. Danas takav pristup imaju i manje tvrtke, što također izaziva dodatne rizike iz perspektive slabije zaštite. Što je sustav složeniji, veća je mogućnost ljudske pogreške. U takvim okolnostima, bitno je definiranje tko ima pristup kakvom sustavu, kao i opoziv pristupa.

Republika Hrvatska je dokumentom naziva „ Nacionalna strategija kibernetičke sigurnosti“ započela planiranje aktivnosti u svrhu zaštite svih korisnika elektroničkih usluga. Ovom strategijom iskazuje se odlučnost sudionika kibernetičke sigurnosti za poduzimanje mjera koje su u njihovoj nadležnosti, za suradnju s drugim korisnicima u vidu razmjene potrebnih i korisnih podataka te spremnost za stalnu edukaciju i prilagođavanje. Republika Hrvatska je članica NATO-a i EU-a te je shodno tome poželjna meta za razne oblike kibernetičkih napada.

SOA (Sigurnosno-obavještajna agencija), kao odgovor na izazove u kibernetičkom smislu, 2019. godine je uspostavila Centar za kibernetičku sigurnost. Također, u svrhu podizanja sposobnosti za pravovremeno otkrivanje i zaštitu od kibernetičkih napada izgrađen je sustav SK@UT. Ovaj sustav omogućuje otkrivanje potencijalnih napada u najranijim fazama.

2. SIGURNOSNE KONTROLE I KONCEPTI

Ovo poglavlje bazirat će se na osnovnim sigurnosnim kontrolama. Naglasak se stavlja na očuvanje podataka i infrastrukture. Da bi se to postiglo, provode se učestale kontrole i analize. Spomenut će se tri nezaobilazna načela informacijske sigurnosti. Sigurnosni mehanizmi podrazumijevaju identifikaciju, autentifikaciju i autorizaciju. Autentifikacija je zaštita ostvarena sučeljem prema korisniku dok je autorizacija unutarnji zaštitni mehanizam. Dotaknut će se i nekih osnovnih koncepata provjere autentičnosti i autorizacije. Na kraju poglavlja opisat će se komunikacijski zaštitni mehanizam, odnosno kriptiranje podataka.

2.1. Osnovne sigurnosne kontrole

Primarni cilj informacijske sigurnosti je zaštita dostupnih informacija i informacijskih izvora od neovlaštenog pristupa, napada, krađe ili oštećenja podataka. Odgovorni pojedinci trebaju osigurati svoje povjerljive informacije. Od velike važnosti su stalne kontrole. U području računalne sigurnosti, kontrolom se smatraju protumjere koje se postavljaju kako bi se izbjeglo, ublažilo ili suprotstavilo sigurnosnim rizicima uzrokovanim prijetnjama i napadima. Drugim riječima, kontrole su rješenja i aktivnosti koje omogućuju organizaciji da ispuni ciljeve strategije informacijske sigurnosti. Kontrole su općenito klasificirane kao kontrole prevencije, detekcije i korekcije. Pod prevencijom se smatra kako osobni podaci i podaci o tvrtki moraju biti zaštićeni. Ukoliko dođe do povrede sigurnosti u bilo kojem od ovih područja, tada će organizacija biti izložena ulaganju mnogo truda u povrat gubitaka. Prioritet broj jedan stručnjaka za informacijsku sigurnost morao bi biti sprječavanje subjekata od dobivanja neovlaštenog pristupa povjerljivim informacijama. Detekcija se događa kada se otkrije da korisnik pokušava pristupiti neovlaštenim podacima ili nakon što su informacije izgubljene. Kontrole korekcije pomažu u ublažavanju posljedica prijetnje ili napada koji negativno utječe na računalni sustav. Proces upravljanja sigurnošću uključuje identificiranje i nadzor sigurnosnih kontrola. Na koji način je najbolje zaštititi sustav te otkrivanje problema pripada identificiranju sigurnosne kontrole.

Poželjno je bilježiti detalje kršenja, prikazujući informacije o neuspjelim pokušajima (upisivanje pogrešnog korisničkog imena i lozinke). Nadziranje se, prije produkcije, provodi na testnom okruženju. Pokreću se testovi na različitim instaliranim konzolama uz praćenje učinkovitosti rada i utjecaja napada.

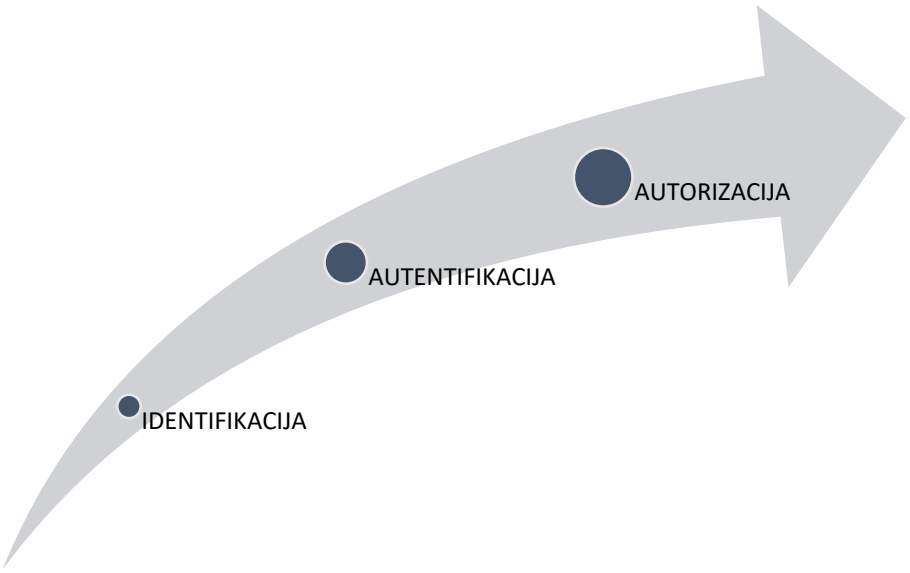
Informacijska sigurnost podrazumijeva tri specifična načela: povjerljivost, cjelovitost (integritet) i dostupnost. Skupni naziv je CIA (eng. *Confidentiality, Integrity, Availability*) trokut. Ako je narušeno jedno od načela, sigurnost organizacije je ugrožena. Povjerljivost je temeljno načelo očuvanja privatnosti informacija i komunikacija te zaštite od neovlaštenog pristupa. Obično se kontrolira enkripcijom, kontrolama pristupa i steganografijom. Pod integritetom se misli na održavanje organizacijskih informacija točnima, bez pogrešaka i bez neovlaštenih izmjena.

Informacije dostupne u računalnim sustavima beskorisne su ako korisnici ne mogu doći do njih. Tu je riječ o dostupnosti kao načelu osiguravanja kontinuiranog rada računalnih sustava i pristupa ovlaštenim osobama podacima koji su im potrebni.

Slika 1 CIA trokut

Povjerljivost je temeljno načelo očuvanja privatnosti informacija i komunikacija te zaštite od neovlaštenog pristupa. Kontrolira se enkripcijom, kontrolama pristupa i steganografijom. Integritet podrazumijeva načelo održavanja organizacijskih informacija točnima, bez pogrešaka i bez neovlaštenih izmjena. Informacije dostupne u računalnim sustavima beskorisne su ako korisnici ne mogu doći do njih. Tu je riječ o dostupnosti kao načelu osiguravanja kontinuiranog rada računalnih sustava i pristupa ovlaštenim osobama podacima koji su im potrebni.

Kao sigurnosni mehanizmi, od velike važnosti su i identifikacija, autentifikacija te auturozacija. Identifikacija je proces kojim se daje tvrdnja o prirodi određenog entiteta. Obično uključuje pridruživanje resursa kao što su adrese e-pošte ili korisničko ime pojedincu. Identitet pojedinca osiguran je autentifikacijom. Autentifikacija se usredotočuje na prepoznavanje ima li određena osoba ispravne vjerodajnice za ulazak u sustav. Provjera autentičnosti temelji se na upotrebi jednog ili više čimbenika. Ti čimbenici uključuju: nešto što jest (fizičke karakteristike poput otiska prsta ili uzorka mrežnice), nešto što pojedinac ima (token ili pristupna kartica), nešto što se zna (lozinka). Nakon pristupanja sustavu, autorizacijom se određuje koja prava i privilegije ima određeni entitet. Kontrola pristupa je način na koji se upravlja autorizacijom. Načelo najmanje privilegije nalaže da korisnici i softver trebaju imati minimalnu razinu pristupa koja im je potrebna za obavljanje dužnosti koje se od njih traže



Slika 2 Identifikacija, autentifikacija i autorizacija

2.2. Osnovni koncepti provjere autentičnosti i autorizacije

Autentifikacija je jedna od primarnih kontrola u upotrebi te postoji mnogo pristupa za postizanje tog cilja. Snažna autentifikacija prva je linija obrane u borbi za sigurnost mrežnih resursa. Provjera autentičnosti nije jedan proces već postoji mnoštvo različitih metoda i mehanizama. Kombinacija korisničkog imena i lozinke jedna je od najosnovnijih i najčešće korištenih shema provjere autentičnosti. Ovdje se vjerodajnice korisnika uspoređuju s vjerodajnicama pohranjenima u bazi podataka. Ako korisničko ime i lozinka odgovaraju bazi podataka, korisnik je autentificiran. U protivnom, korisniku se pristup uskraćuje. Ova metoda nije baš sigurna jer ne identificira nužno pravog vlasnika. Tokeni su virtualni ili fizički objekti, kao npr. pametne kartice, koji pohranjuju podatke za provjeru autentičnosti. Jedinstvene vrijednosti tokena mogu se generirati posebnim hardverom, softverom ili korištenjem neovisnih algoritama.

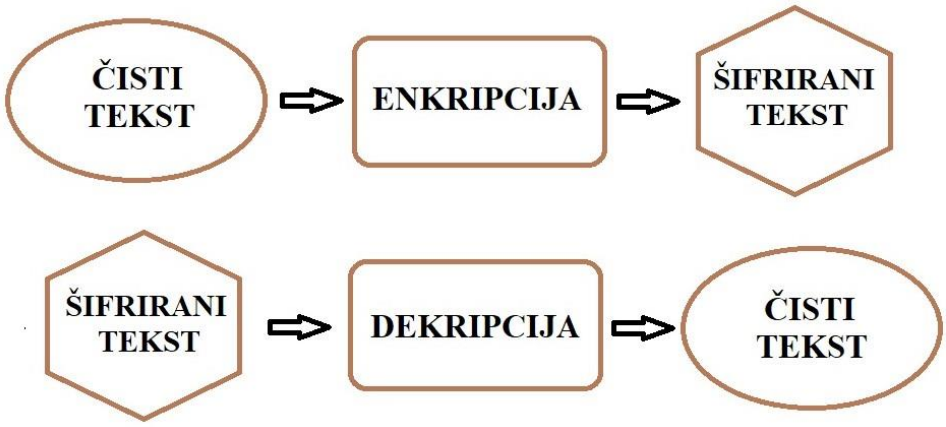
Slika 3 Provjera autentičnosti

Pametne kartice čest su primjer provjere autentičnosti na temelju tokena. Pametna kartica je plastična kartica koja sadrži ugrađeni čip koji može pohraniti različite vrste elektroničkih informacija. Autentifikacija pojedinaca temeljena prema njihovim fizičkim karakteristikama govorio o biometriji. To može uključivati prepoznavanje otiska prsta, prepoznavanje mrežnice ili softver za prepoznavanje glasa i lica. Kako biometrijska funkcija postaje jeftinija za implementaciju, postaje sve šire prihvaćena. U sve više i više mobilnih uređaja koji se povezuju na mreže, geolokacija pruža dodatnu razinu za autentifikaciju.

Korisnicima koji se pokušavaju autentificirati s odobrene lokacije može se dopustiti pristup mreži, dok se korisnicima koji se pokušavaju autentificirati s lokacije koja nije odobrena, može uskratiti pristup mreži. Geolokacija obično funkcionira traženjem IP adrese domaćina u geolokacijskoj bazi podataka. Organizacije koje posluju u određenim dijelovima svijeta mogle bi konfigurirati svoje sustave tako da uvijek odbijaju zahtjeve za autentifikaciju koji dolaze iz područja izvan njihovih zona interesa, čime se ograničava njihov potencijalni rizik. Više-faktorska provjera autentičnosti je svaka shema provjere autentičnosti koja zahtjeva provjeru valjanosti dva ili više faktora. To može biti bilo koja kombinacija onoga tko ste, što imate, što znate, gdje ste i što radite. Zahtijevanje fizičke osobne iskaznice zajedno s tajnom lozinkom primjer je provjere autentičnosti s više faktora. Treba imati na umu da provjera autentičnosti s više faktora zahtijeva da faktori budu različiti, a ne samo specifični objekti ili metode. Npr. korištenje pametne kartice s VPN tokenom nije autentifikacija s više faktora, jer obje metode su dio istog faktora, onoga što imate. Uzajamna provjera autentičnosti je sigurnosni mehanizam koji zahtijeva da svaka strana u komunikaciji međusobno potvrdi identitet. Usluga ili resurs provjerava vjerodajnice klijenta, a klijent provjerava vjerodajnice resursa. Međusobna provjera autentičnosti sprječava klijenta da nenamjerno pošalje povjerljive informacije nesigurnom pošiljatelju.

2.3. Osnovni koncept kriptografije

Kriptografija je jedan od najsvestranijih sigurnosnih alata koji se mogu koristiti kako bi se opravdali povjerljivost, integritet i dostupnost. Smatra se složenom i snažnom metodom u borbi za održavanje računalne sigurnosti. To je znanost o skrivanju informacija, najčešće kodiranjem i dekodiranjem tajnog koda koji se koristi za slanje poruka. Moderne komunikacije i računarstvo u velikoj mjeri koriste kriptografiju kao zaštitu osjetljivih informacija i komunikacija od neovlaštenog pristupa. Razlikuju se dva pojma: šifriranje (enkripcija) i dešifriranje (dekripcija). Enkripcija je kriptografska tehnika koja pretvara podatke iz čistog teksta u kodirani ili šifrirani oblik. Dekripcija je obrnuta tehnika, tj. šifrirani tekst pretvara natrag u otvoreni tekst.



Slika 4 Enkripcija i dekripcija

Šifriranu poruku, samo ovlaštene strane s posebnim informacijama za dešifriranje mogu dekodirati i čitati podatke. Postoje simetrična i asimetrična enkripcija. Simetrična enkripcija je dvosmjerna shema šifriranja u kojoj se šifriranje i dešifriranje izvode istim ključem. Ključ se mora prenijeti na siguran način između dviju strana prije šifrirane komunikacije. Simetrična enkripcija je relativno brza, ali i ranjiva ako se ključ izgubi ili je ugrožen. Za razliku od simetrične enkripcije, glavna karakteristika asimetrične enkripcije je korištenje javnih i privatnih ključeva. Privatni ključ čuva u tajnosti jedna strana tijekom dvosmjerne enkripcije. S druge strane, javni ključ se može dati svakome. Ovisno i primjeni enkripcije, bilo koja strana može koristiti ključ za šifriranje. Drugi ključ u paru koristi se za dešifriranje. Privatni ključ u paru može dekriptirati podatke kodirane odgovarajućim javnim ključem. Asimetrični algoritmi obično su sporiji od simetričnih zbog veće količine ključeva.

Steganografija je alternativna tehnika šifriranja gdje se skriva tajna poruka stavljajući je u običnu datoteku kao što je zvučna, grafička ili filmska datoteka. Skriva se sadržaj informacije, ali ne pokušava se sakriti činjenica da informacija postoji.

3. VRSTE DIGITALNE FORENZIKE

3.1. Mrežna forenzika

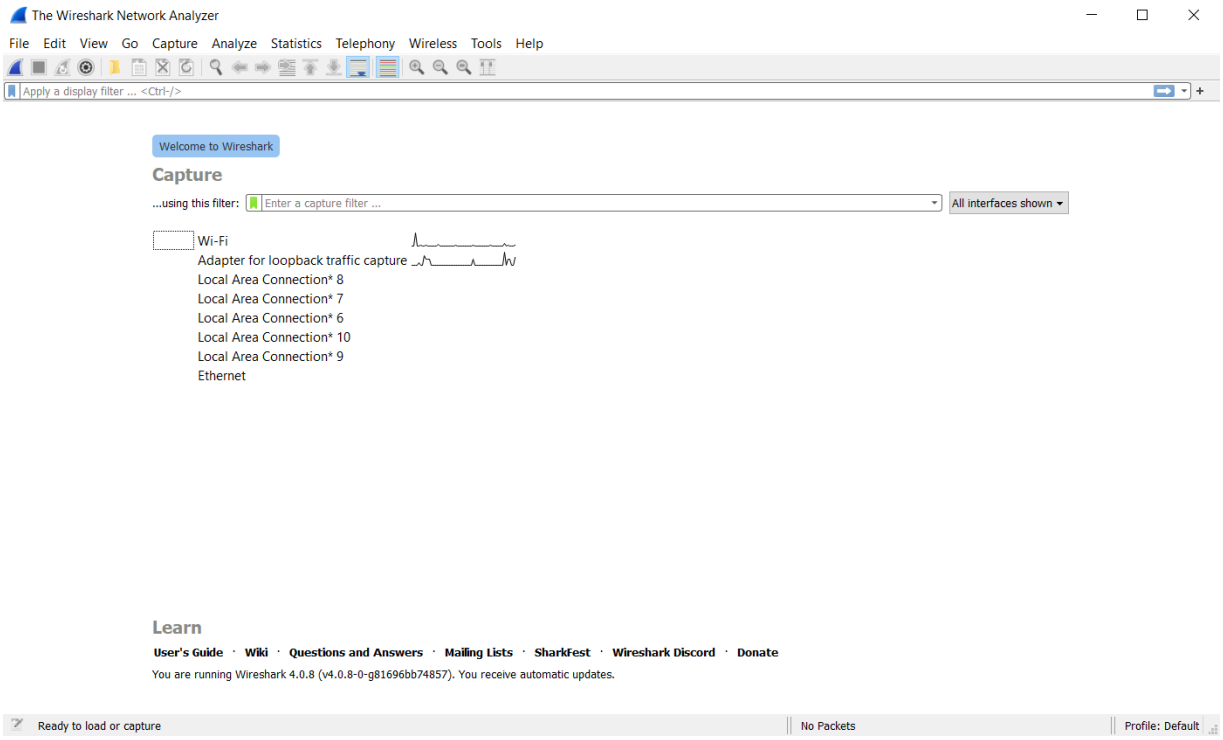
Tok podataka je prisutan na mreži te ako je ona ugrožena, ugroženi su i podaci. Mrežna forenzika je prikupljanje i analiziranje događaja na mreži u svrhu otkrivanja napada. Razni su načini upada u mrežu i sustave, a oni će detaljnije biti opisani u idućem poglavlju. Napadači koriste ranjivosti sustava, otkrivanje zaporki, a česta su i slanja neželjenih e mail poruka. U praksi, snimanje mrežnog prometa je vrlo složeno radi velike količine podataka koji se nalaze na mreži te složenosti protokola. Ne koriste se vri istim metodama analize mrežnog prometa. Pojedinci prate sav promet na mreži dok drugi koriste posebna i ciljana promatranja prometa. Mrežna istraga bavi se dinamičnim i nestabilnim informacijama.

Mrežna forenzika uključuje i analizu mrežne opreme u koju se ubrajaju usmjeritelj (eng. switch), koncentrator (eng. hub), vatrozid (eng. firewall) te samo računalo. Važno je poznavati topologiju same mreže. Linija između mrežnih uređaja je postala jako nedefinirana, tj. postoji samo teoretska linija. Tragovi za koje se očekuje da će se naći na jednom uređaju, zapravo postoje na drugom. Preklopnik sadržava MAC adrese mrežnih kartica koje komuniciraju na lokalnoj podmreži. Glavni uređaj za ulaz u mrežu je usmjerivač, jer preko njega ide sav promet. Usmjerivač je jedan od najosnovnijih uređaja za vođenje dnevnika na bilo kojoj mreži. Mrežni dnevnici pružaju informacije o stanju sustava i okolini u određenom trenutku. U dnevnicima događaja mogu biti pohranjene informacije o pristupu sustavu, o trenutku paljenja odnosno gašenja, greškama, problemima itd. Aplikacijski poslužitelji, usmjerivači, kamere, svi oni generiraju mrežne dnevnike. Istražiteljima su uvijek zanimljivi dnevnici vatrozida. Vatrozid je zapravo usmjeritelj koji može pregledavati i filtrirati promet na napredniji način. Dnevnici vatrozida obično sadržavaju brojne informacije – pokušaji spajanja, koliko podataka je prenešeno od izvorišta do odredišta, korišteni protokoli pa čak i sadržaj paketa. Postoje i izazovi povezani s mrežnim tragovima. U prvom redu riječ je o ograničenom kapacitetu pohrane podataka u dnevnike, kao i to da podaci koje sadržavaju mrežni uređaji mogu biti netrajni odnosno ne prežive ponovno pokretanje uređaja.

Rekonstrukcija mrežnog prometa (npr. privitci e mail poruke, web stranice), moguća je jedino ako se prenose ili primaju nekriptirani. Međutim, ako je napadač iskusniji i svjestan da bi se njegova mreža mogla prisluškivati, mogao bi upotrijebiti enkripciju. Za praćenje i snimanje mrežnog prometa uobičajeno se koristi alat Wireshark.

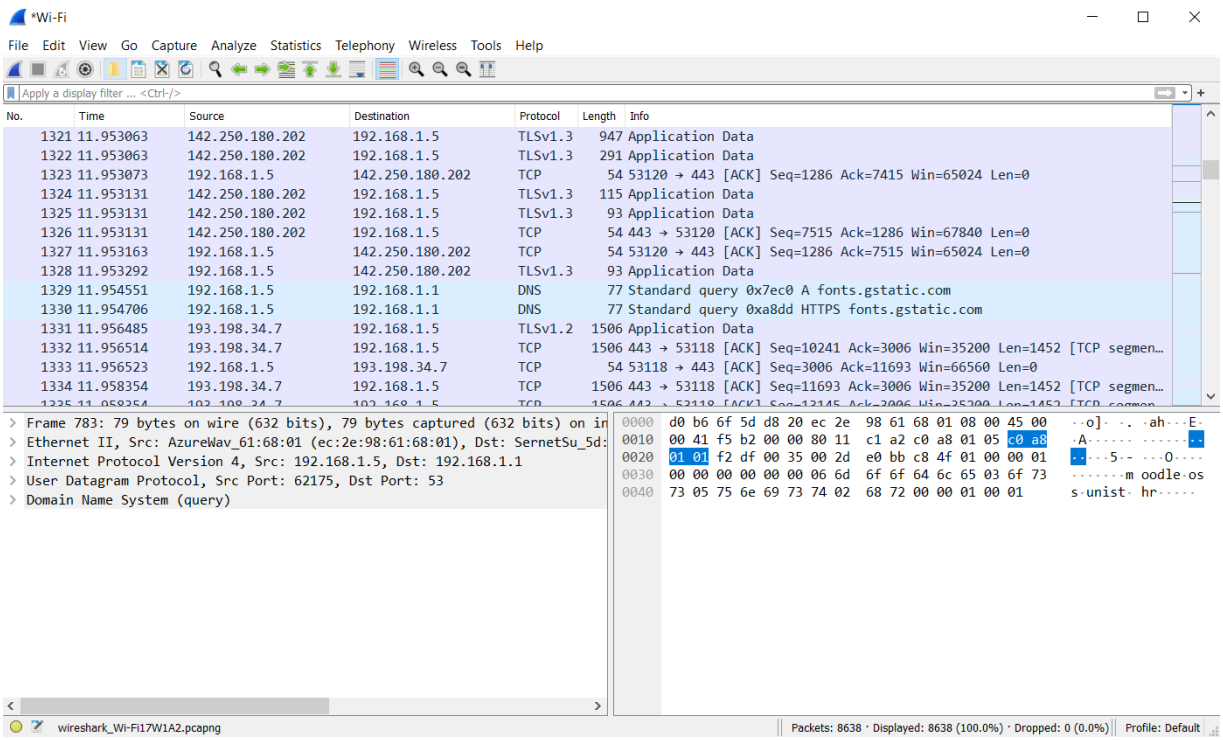
3.1.1. Wireshark

Wireshark je potpuno besplatni alat za analizu i praćenje mrežnog prometa. Pogodan je za edukaciju te upoznavanje s osnovama računalnih mreža i protokola. S druge strane, moguća je primjena ovog programa i u zlonamjerne svrhe. U ovom primjeru, laptop je spojen na bežičnu vezu te se dvoklikom na WiFi pokreće snimanje mrežnog prometa.



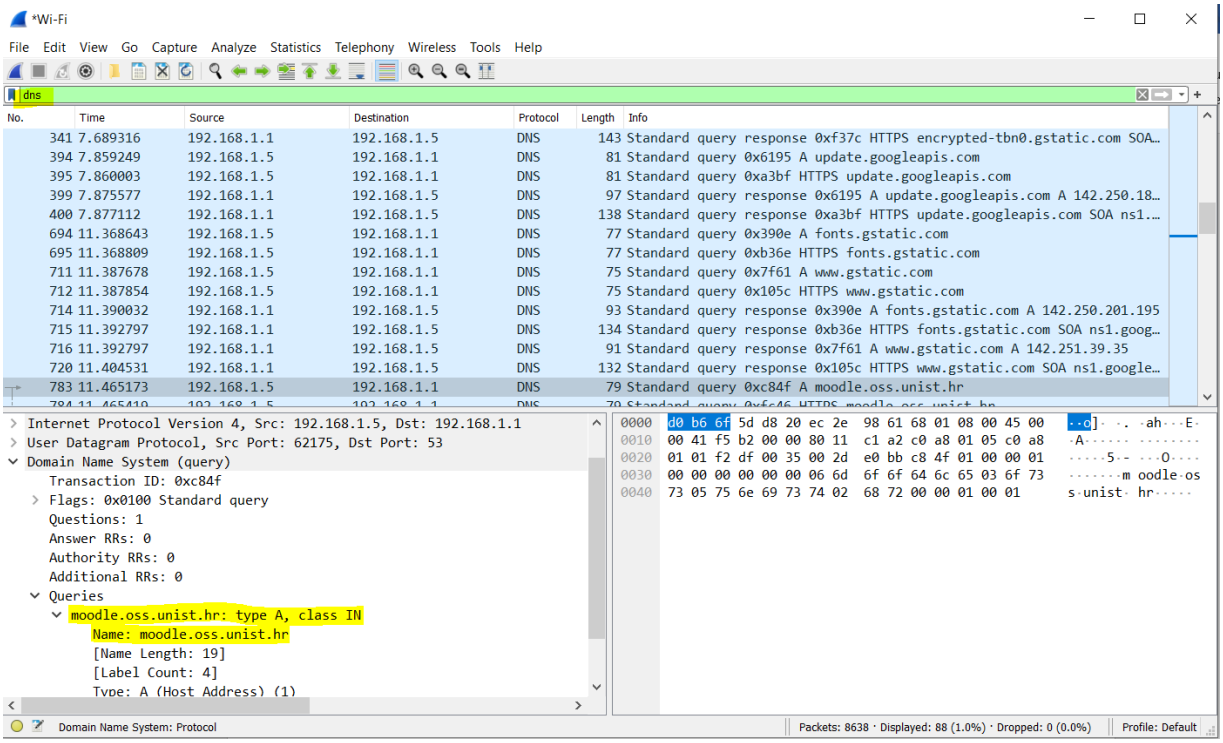
Slika 5 Početno sučelje wiresharka

Na popis paketa dodaju se paketi kako dolaze odnosno odlaze s mrežnog sučelja.



Slika 6 Dio snimljenih paketa

Broj snimljenih paketa na mreži može biti jako velik. Velika prednost ovog programa su filteri za pronalazak traženih paketa. Moguće ih je filtrirati po IP adresama, protokolima, portovima, sadržaju paketa itd. Za svrhu ovog rada, odrađeno je filtriranje po DNS prometu. DNS (eng. *Domain Name System*) povezuje IP adrese sa simboličkim imenima koja su puno lakša za pamtiti. Komunikacija među računalima se odvija korištenjem IP adresa, a prije korištenja, računalo mora simbolička imena prevesti u IP adresu. Taj proces se događa na mreži te ga je moguće analizirati u Wireshark-u.



Slika 7 DNS filtriranje

Na slici 15 prikazan je dio paketa snimljenih primjenjujući DNS filter. Ispod popisa snimljenih paketa nalazi se prozorčić u kojem je vidljivo polje upita tipa A kojim se traži IP adresa za simboličko ime *moodle.oss.unist.hr*

Wireshark omogućuje detaljnu analizu velikog broja protokola te se razni stručnjaci služe njime svakodnevno. Uz činjenicu da je besplatan, pogodan je i za razne edukacije te upoznavanje osnova rada računalnih mreža.

3.2. Forenzika mobilnih uređaja

Pod mobilnim uređajima se podrazumijevaju: pametni telefoni, GPS uređaji, tableti, razni uređaji za reprodukciju glazbe (iPod, mp4), digitalne kamere i aparati, dronovi. Forenziku mobilnih uređaja mnogi smatraju najtežom zbog nekoliko različitih operacijskih sustava (Android, iOS, Windows). Svako ažuriranje softvera donosi promjenu prilikom spremanja datoteka, tj. mijenja se putanja na kojoj se mogu nalaziti neki podaci. Mobilni uređaji mogu se koristiti za spremanje nekoliko vrsta osobnih podataka kao što su fotografije, bilješke, kontakti, SMS i MMS poruke. Napretkom tehnologija mobilnih uređaja, količina i vrste podataka koji se mogu pronaći neprestano se povećavaju. Potencijalni dokazi mogu potjecati iz nekoliko različitih izvora, uključujući SIM karticu i vanjsku memoriju (SD kartice). Tradicionalno se forenzika mobilnih telefona povezuje s vraćanjem SMS i MMS poruka, kao i povijesti poziva. Novije generacije pametnih telefona uključuju veću bazu informacija. Ta baza podrazumijeva pregledavanje weba, postavke bežične mreže, informacije o lokaciji, e-pošta. Veliku ulogu prilikom istrage mogu odigrati i objave i kontakti na društvenim mrežama. Mobilni telefoni se upotrebljavaju za pohranu i prijenos osobnih i korporativnih informacija, Također, povećana je njihova upotreba prilikom online transakcija. Sve su to razlozi zbog kojih se javlja sve veća potreba za mobilnom forenzikom. Prve tehnike za analizu mobilnih uređaja nisu mogle vratiti izbrisane podatke. Međutim, kako se broj mobilnih uređaja počeo povećavati, javile su se i nove, konkretnije tehnike za izvlačenje podataka. Iako tehnički nisu dio forenzike mobilnih uređaja, zapisi s detaljima poziva telefonskih operatera često služe kao pomoćni dokazi. Ovo je korisno kada su povijest poziva ili tekstualne poruke obrisane s uređaja. Zapis detalja o pozivima može pokazati baznu stanicu na koju je korisnik bio spojen tijekom poziva (ili više njih ako je bio u pokretu).

U mobilne uređaje pripadaju i dronovi. U dronovima je moguće pronaći podatke od kuda je poletio pa čak i video snimke u pojedinim slučajevima. Lako su dostupne i informacije o samom vlasniku budući da prilikom registracije na službenu aplikaciju za upravljanje dronom moraju unijeti vlastite podatke. Otkriveno je kako se u dronovima nalazi operacijski sustav Android 4.4.4. koji sadrži puno sigurnosnih propusta. Iz tog razloga, tvrtke koje proizvode softvere za analizu, mogle su napraviti alate koji omogućuju pristup podacima s drona.

Proces forenzike mobilnog uređaja može se podijeliti u tri kategorije: zapljena, akvizicija i analiza. Prilikom zapljene, od presudne je važnosti zaštititi uređaj tako da interakcija forenzičara s dokazima ne mijenja dokaze. Nastoji se izbjeći gašenje ili zaključavanje uređaja. Međutim, ostavljanje mobilnog telefona uključenog nosi novi rizik – uređaj i dalje može uspostaviti mrežnu vezu. Napadači često pokušavaju udaljeno obrisati sve podatke s uređaja. To se postiže npr. preko Google računa koji je konfiguriran na samom uređaju, a preko kojega može saznati i lokaciju uređaja, što predstavlja dodatni rizik. Iz tog razloga, transport se odvija u Faradeyevim vrećicama ili kavezu. Ukratko rečeno, Faradeyev kavez i vrećica potpuno blokiraju funkciju radio komunikacije. Ako ova opcija nije dostupna, preporuča se stavljanje uređaja u zrakoplovni način rada. Zrakoplovni način rada onemogućuje funkcije bežičnog prijenosa s uređaja (WLAN i Bluetooth).

Slika 8 Faradejeva vrećica [5]

Nakon zapljene uređaja slijedi faza akvizicije koja se obično odnosi na pronalaženje materijala s uređaja. Zbog sigurnosnih značajki često nije moguće lako dohvatiti podatke. Razlikuju se sljedeće metode akvizicije podataka: ručna, logička i fizička.

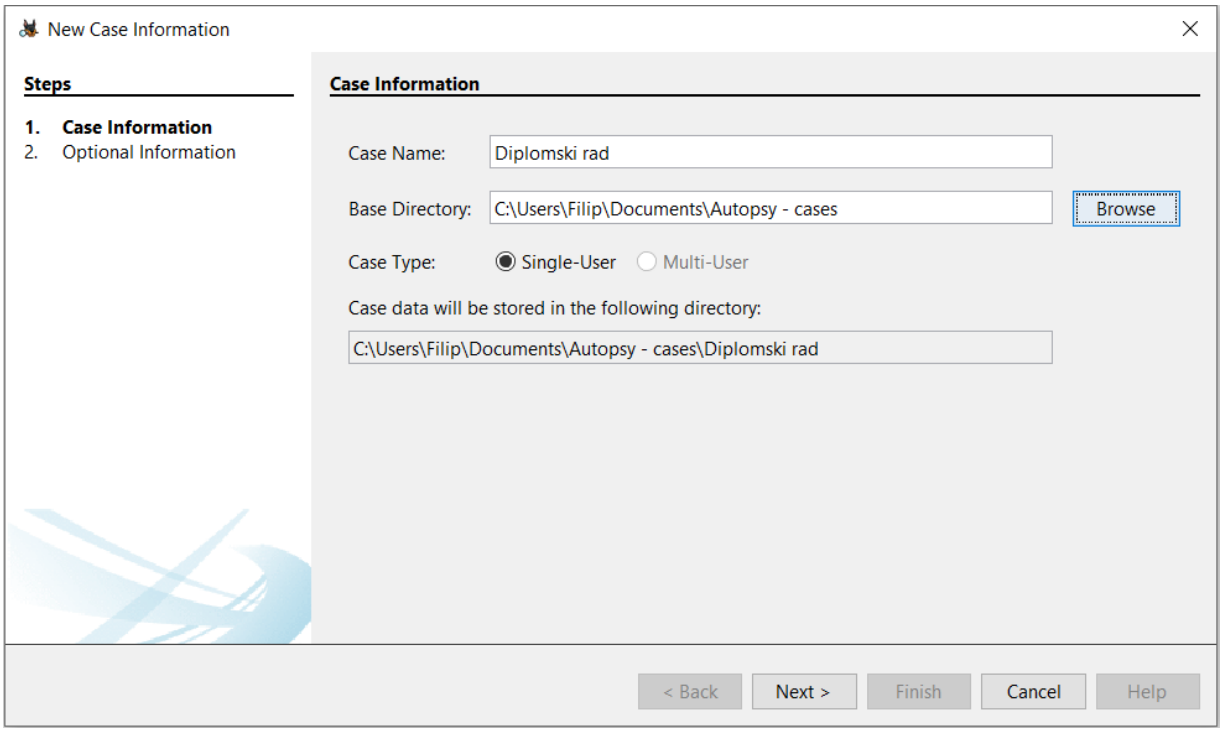
Ručna akvizicija je ujedno i najjednostavnija. Koristi se korisničko sučelje uređaja za analizu te nisu potrebni nikakvi posebni alati i tehnike. Ograničenje ove metode je što se mogu izdvojiti samo podaci dostupni kroz korisničko sučelje. Logička ekstrakcija se odnosi na vađenje podataka koji se nalaze pohranjeni u logičkoj strukturi, Uključuje dobivanje podataka poput povijesti poziva, lokacijske podatke, tekstualne poruke, povijest pretraživanja interneta.

Fizička akvizicija podrazumijeva bit po bit kopiju cijele fizičke memorije uređaja. Ova metoda daje uvid u izbrisane datoteke kao i ostatke podataka.

3.2.1. AUTOPSY

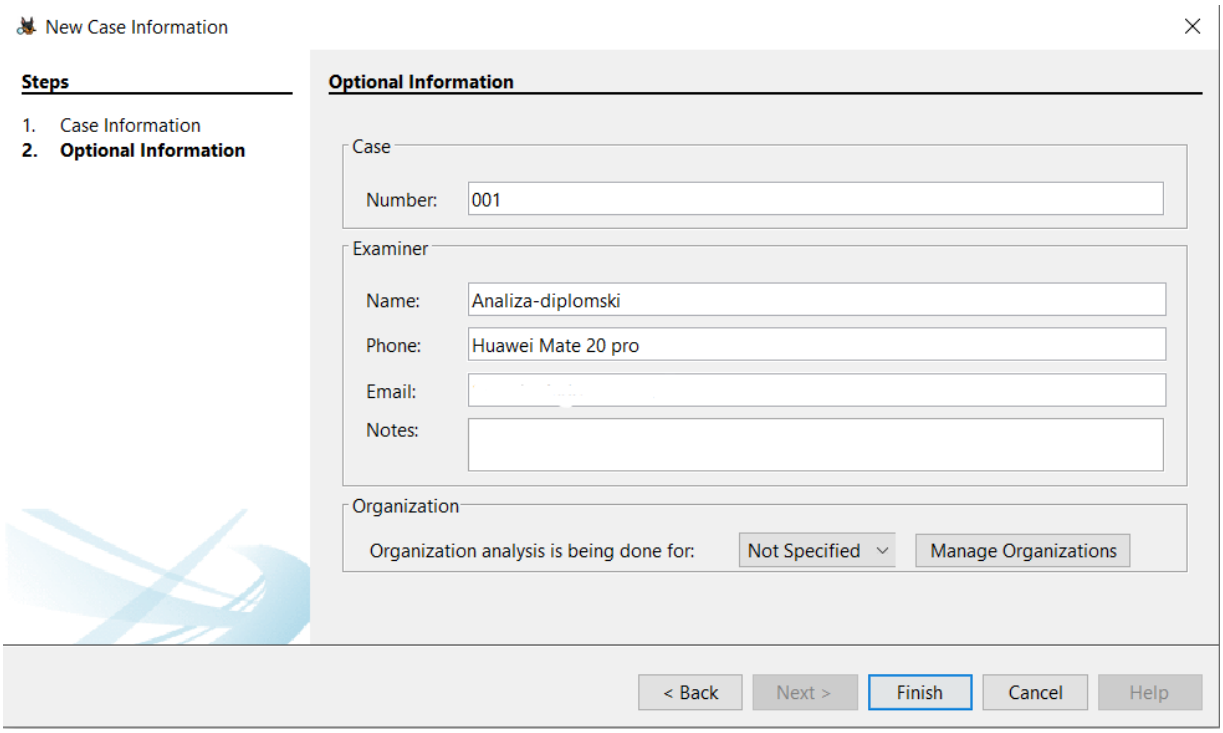
Autopsy je digitalna forenzička platforma. Koriste ga službe za provedbu zakona, vojska i ostali kako bi istražili što se dogodilo na uređaju. Pomoću ovog programa najčešće se analiziraju diskovi računala, a u ovom radu je korišten za analizu pametnog mobitela Huawei Mate 20 Pro. Sama instalacija je vrlo jednostavna, a grafičko sučelje jasno raspoređeno i intuitivno. Rezultati se prikazuju u vrlo kratkom roku. Vjerojatno i najveća prednost programa je što je besplatan za razliku od mnogih drugih komercijalnih alata za digitalnu forenziku.

Nakon instalacije potrebno je pokrenuti program te odabrati izbornik Case, a zatim New Case gdje se otvara prozor za kreiranje novog slučaja.



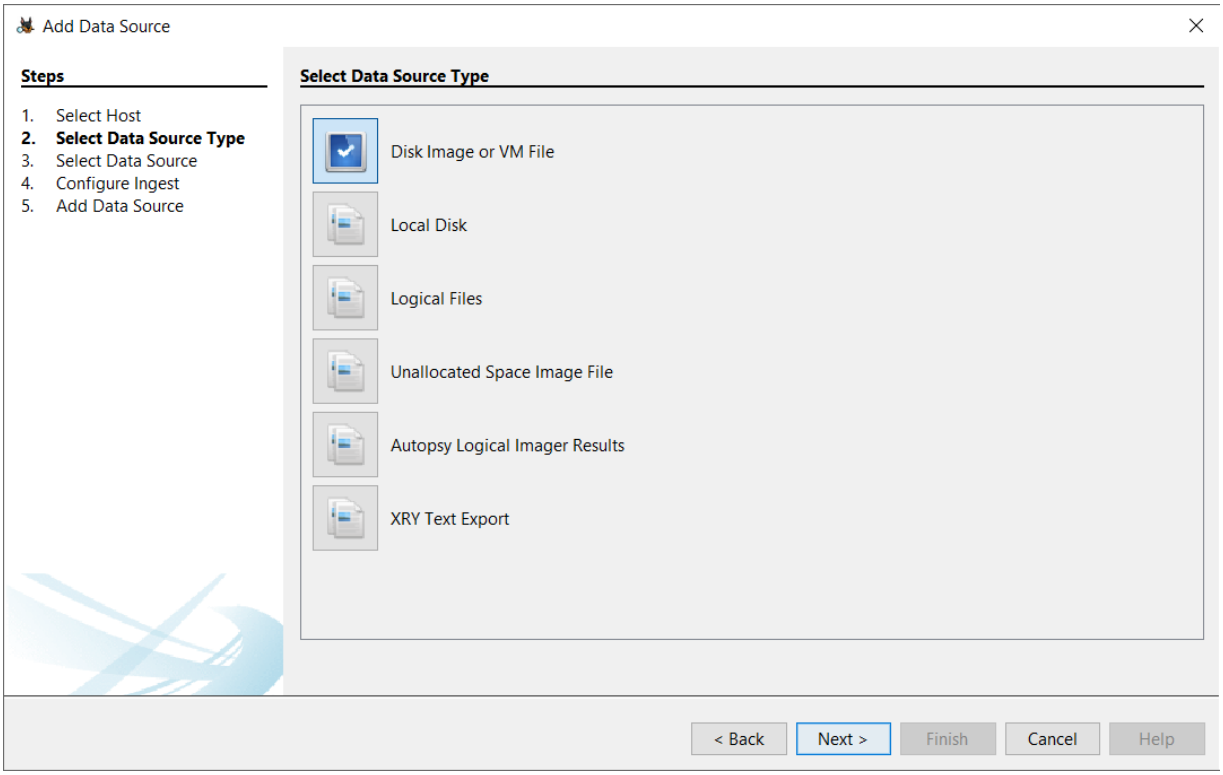
Slika 9 Autopsy - početni zaslon

Pritiskom na tipku Next otvara se sljedeći prozor pod nazivom Opcionalne informacije u kojem je potrebno unijeti određene informacije vezane za ispitivača



Slika 10 Opcionalne informacije

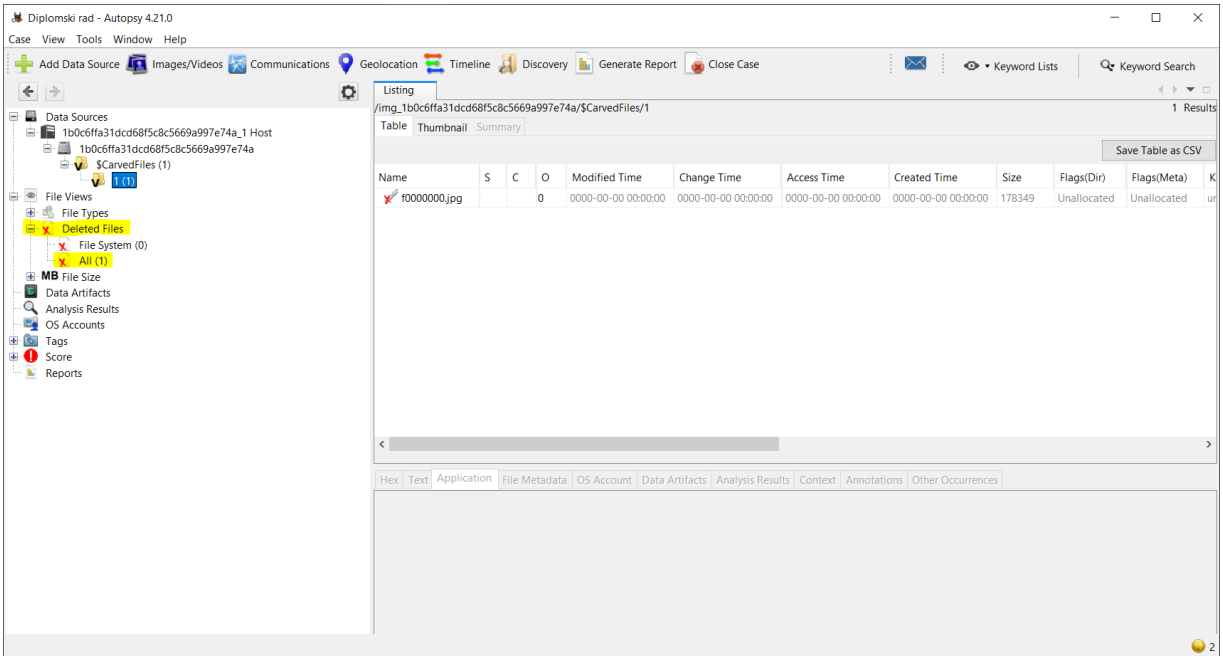
Sljedećim korakom potrebno je izvršiti Odabir vrste izvora podataka. Nakon toga pojavljuje se program Odabir izvora podataka gdje se odabire putanja do izvorišne datoteke. Za ovu analizu koristila se datoteka „smeće“ na pametnom mobitelu. Istražiteljima su uvijek od velike zanimljivosti obrisane datoteke i podaci.



Slika 11 Odabir vrste izvora podataka

Potvrdom odabira vrste izvora podataka pojavljuje se prozor s odabirom modula. Radi pronalaženja što više informacija, preporuka je ostaviti uključene sve module.

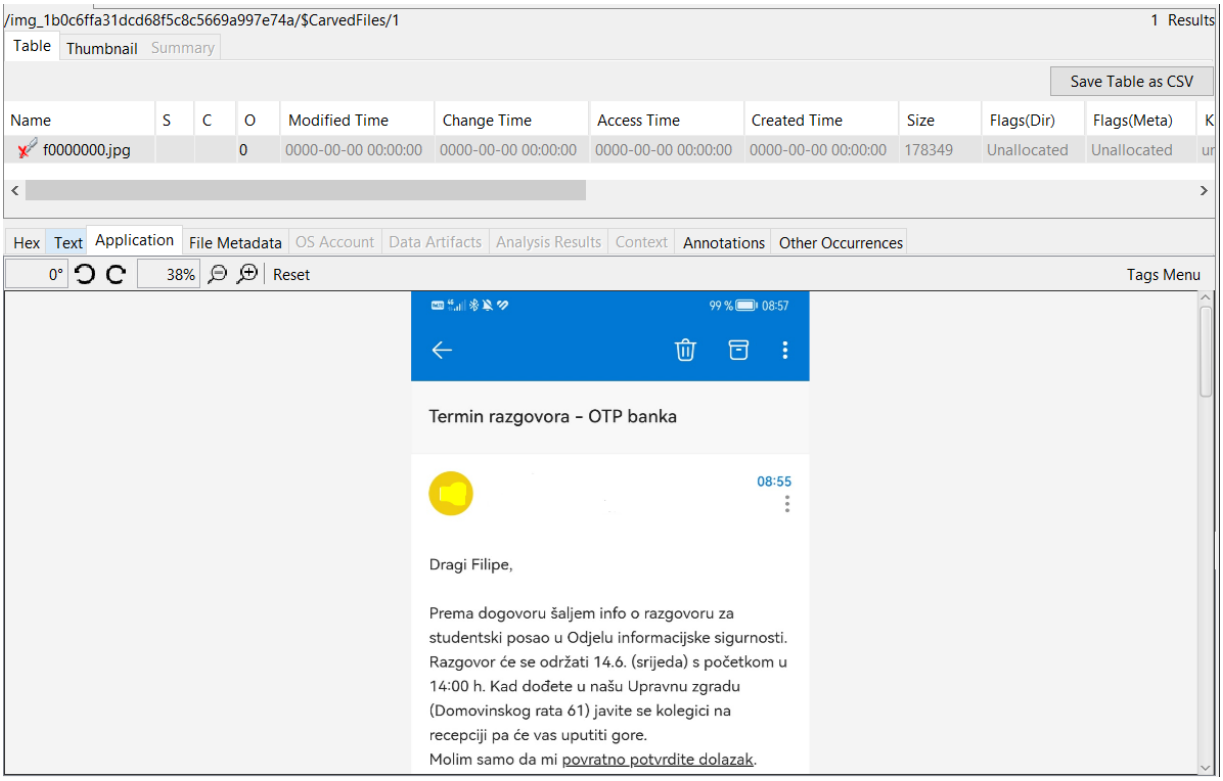
Započinje učitavanje predmeta te se pokreću moduli. U konkretno ovom primjeru pronađena je jedna obrisana datoteka, a riječ je o snimci zaslona.



Slika 12 Sučelje programa Autopsy

Odabirom na samu pronađenu datoteku, dobije se prikaz te uvid u podatke o nastanku same datoteke. Iako je korisnik obrisao datoteku, podaci su ostali u uređaju i program Autopsy ih prikazuje. Tu su još i razne opcije koje bi mogle biti od koristi u detaljnijoj analizi.

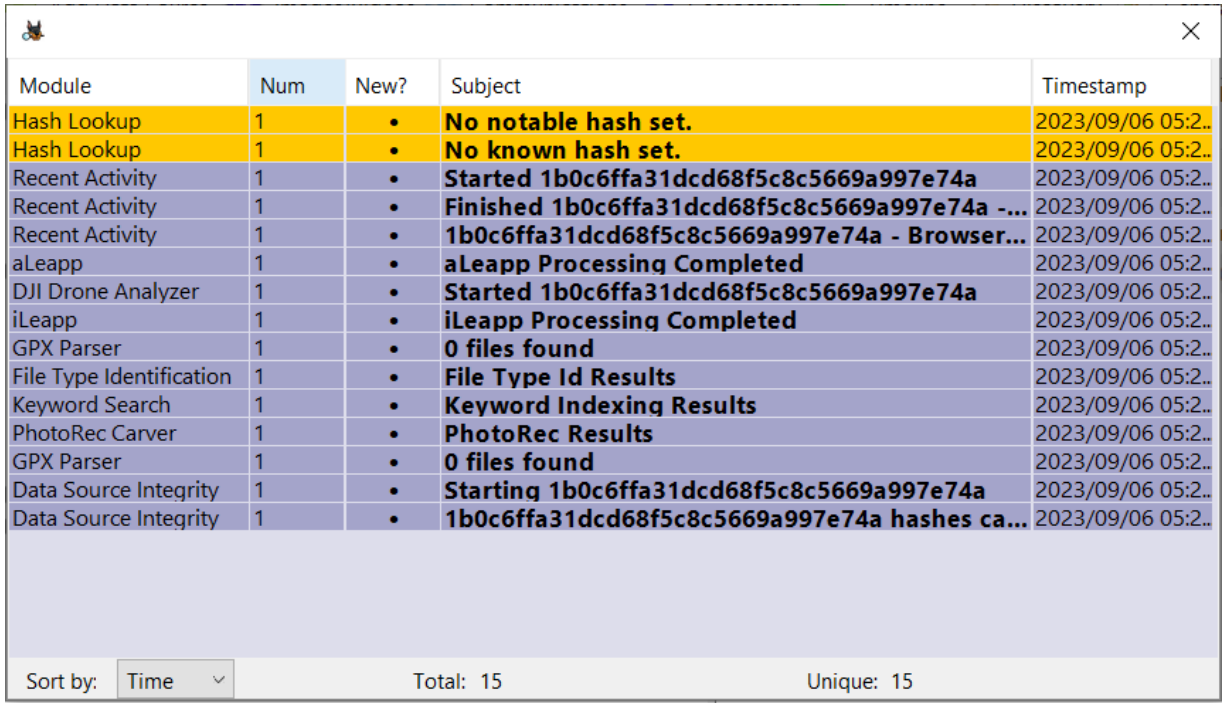
Unutar same aplikacije dostupne su informacije o komunikaciji. Tako se može doći do uvida u ispis poziva i SMS poruke. Također postoji i opcija uvida u lokacije koje su ostale zabilježene na samom uređaju.



Slika 13 Prikaz nađene datoteke

Završetkom analize, postoji mogućnost kreiranja izvješća slučaja. Nudi se opcija izbora koji će se sve rezultati nalaziti u izvještaju. Postoje i zapisi unutar aplikacije koji u svakom trenutku pokazuju što je forenzičar radio unutar analize (logovi). Oni su od koristi ako se želi vratiti na neki prethodni korak ili nije siguran u neku od prethodnih radnji.

Rad u Autopsy okruženju je jednostavan i ne zahtjeva neka prevelika znanja za analizu obrisanih datoteka ili nekih drugih informacija potrebnih istražitelju. Ako se uz jednostavnost korištenja pridoda i činjenica kako je potpuno besplatan i lako dostupan alat, to ga zasigurno svrstava pri samom vrhu odabira programa za ovakvu vrstu analize.



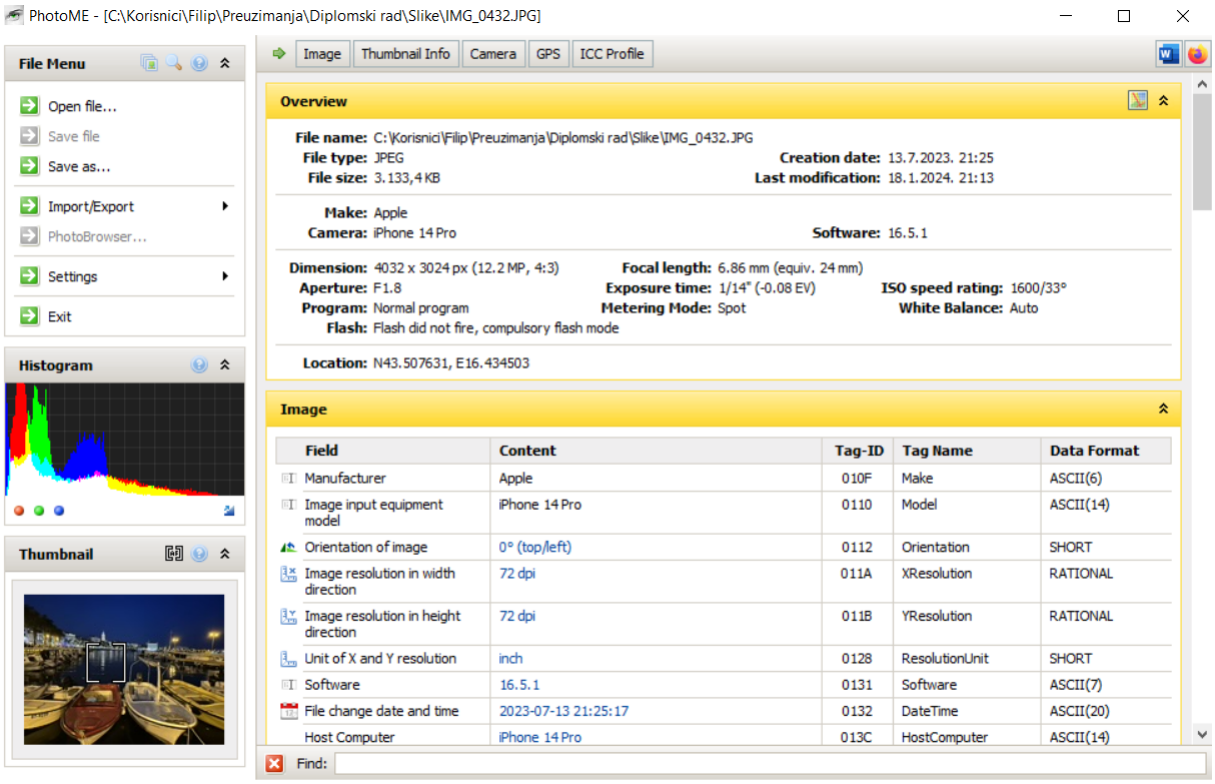
Module	Num	New?	Subject	Timestamp
Hash Lookup	1	•	**No notable hash set.**	2023/09/06 05:2..
Hash Lookup	1	•	**No known hash set.**	2023/09/06 05:2..
Recent Activity	1	•	**Started 1b0c6ffa31dcd68f5c8c5669a997e74a**	2023/09/06 05:2..
Recent Activity	1	•	**Finished 1b0c6ffa31dcd68f5c8c5669a997e74a -...**	2023/09/06 05:2..
Recent Activity	1	•	**1b0c6ffa31dcd68f5c8c5669a997e74a - Browser...**	2023/09/06 05:2..
aLeapp	1	•	**aLeapp Processing Completed**	2023/09/06 05:2..
DJI Drone Analyzer	1	•	**Started 1b0c6ffa31dcd68f5c8c5669a997e74a**	2023/09/06 05:2..
iLeapp	1	•	**iLeapp Processing Completed**	2023/09/06 05:2..
GPX Parser	1	•	**0 files found**	2023/09/06 05:2..
File Type Identification	1	•	**File Type Id Results**	2023/09/06 05:2..
Keyword Search	1	•	**Keyword Indexing Results**	2023/09/06 05:2..
PhotoRec Carver	1	•	**PhotoRec Results**	2023/09/06 05:2..
GPX Parser	1	•	**0 files found**	2023/09/06 05:2..
Data Source Integrity	1	•	**Starting 1b0c6ffa31dcd68f5c8c5669a997e74a**	2023/09/06 05:2..
Data Source Integrity	1	•	**1b0c6ffa31dcd68f5c8c5669a997e74a hashes ca...**	2023/09/06 05:2..

Sort by: Time Total: 15 Unique: 15

Slika 14 Logovi

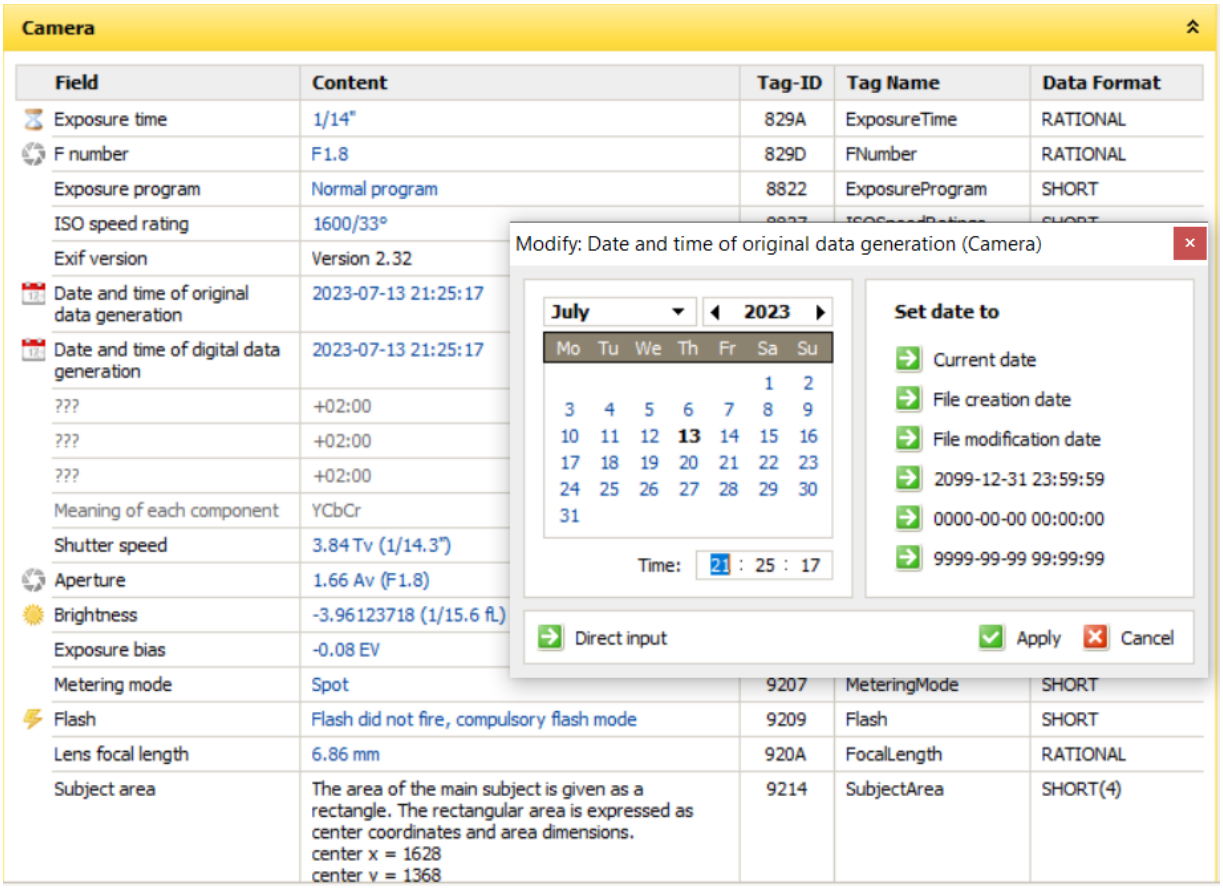
3.3. Analiza digitalne datoteke

U ovom poglavlju rada će se ukratko objasniti analiza te dio mogućih manipulacija digitalne datoteke (u ovom primjeru vlastite fotografije). Metapodatak je pojam koji se odnosi na podatke o podacima. Iz perspektive digitalne forenzike, metapodaci mogu biti od koristi kao dokaz za analizu krivotvorenih ili mijenjanih datoteka. Također, ovim putem mogu se dobiti korisne informacije o nastanku samog digitalnog sadržaja kao i za zaštitu autorskih prava. Korišten je besplatni program PhotoME.



Slika 15 Sučelje programa PhotoME

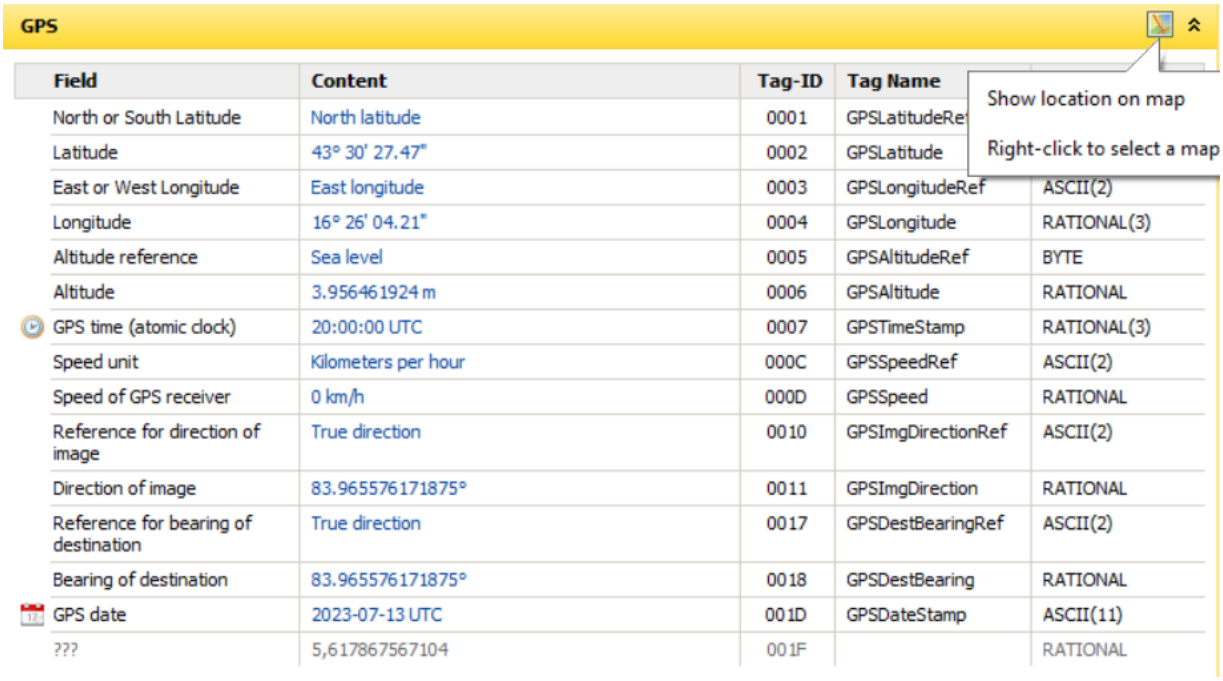
Slika 15 prikazuje početno sučelje programa PhotoME. U donjem lijevom kutu slike prikazana je digitalna fotografija na kojoj će se vršiti analiza. Na samom početku vidljivo je da je fotografija nastala 13.7.2023. godine, posljednja modifikacija je određena 18.1.2024. te je uslikano mobilnim uređajem Iphone 14 Pro. Program nam između ostaloga daje detaljnije informacije o samoj kameri uređaja (ponuđeni izbornik *Camera*) kao i o lokaciji na kojoj je fotografija nastala (izbornik GPS). Spuštanjem do izbornika vezanog za kameru, pojavljuje se mogućnost za promjenu, odnosno manipulaciju vremena nastanka fotografije što je i prikazano na sljedećoj slici.



Slika 16 Moguća manipulacija vremenom nastanka fotografije

Zanimljiv je i pregled izbornika GPS. U navedenom izborniku kriju se informacije o lokaciji nastanka fotografije. Unutar samog izbornika navedene su koordinate lokacije.

Za detaljniju analizu od velike koristi je i histogram fotografije koji se nalazi na početnom sučelju programa. Histogramom su prikazani određeni slojevi fotografije. Svaki sloj je po potrebi moguće uključiti ili isključiti pa se tako fotografija može prikazati u samo jednoj boji zbog lakšeg utvrđivanja mogućeg plagiranja.



Field	Content	Tag-ID	Tag Name	
North or South Latitude	North latitude	0001	GPSLatitudeRe	
Latitude	43° 30' 27.47"	0002	GPSLatitude	
East or West Longitude	East longitude	0003	GPSLongitudeRef	ASCII(2)
Longitude	16° 26' 04.21"	0004	GPSLongitude	RATIONAL(3)
Altitude reference	Sea level	0005	GPSAltitudeRef	BYTE
Altitude	3.956461924 m	0006	GPSAltitude	RATIONAL
GPS time (atomic clock)	20:00:00 UTC	0007	GPSTimeStamp	RATIONAL(3)
Speed unit	Kilometers per hour	000C	GPSSpeedRef	ASCII(2)
Speed of GPS receiver	0 km/h	000D	GPSSpeed	RATIONAL
Reference for direction of image	True direction	0010	GPSImgDirectionRef	ASCII(2)
Direction of image	83.965576171875°	0011	GPSImgDirection	RATIONAL
Reference for bearing of destination	True direction	0017	GPSDestBearingRef	ASCII(2)
Bearing of destination	83.965576171875°	0018	GPSDestBearing	RATIONAL
GPS date	2023-07-13 UTC	001D	GPSDateStamp	ASCII(11)
???	5,617867567104	001F		RATIONAL

Slika 17 GPS izbornik

Klikom na jednu od koordinata ili odabirom ikone u gornjem desnom kutu izbornika (*Show location on map*), program nas vodi na mapu s prikazom lokacije na kojoj je nastala fotografija.

Program PhotoME je besplatan te vrlo jednostavan za korištenje s uredno prikazanim dostupnim parametrima. Ovaj program je od koristi digitalnom forenzičaru, ali i napadaču, jer je moguća i manipulacija određenim podacima. Na istražiteljima je da otkriju moguće manipulacije i usmjere istragu u pravom smjeru.

4. RIZICI

4.1. Analiza rizika

Sigurnosne kontrole se provode od strane organizacije kako bi smanjile mogućnosti izmjene, gubitka ili krađe informacija. Identifikacija onoga što predstavlja prijetnju i kolika je vjerojatnost da se ta prijetnja dogodi je ono što analiza rizika predstavlja. Analiza rizika igra glavnu ulogu u osiguravanju sigurnog okruženja za organizaciju. Ublažavanje mogućih prijetnji može se postići procjenom i identificiranjem specifičnih rizika koji mogu uzrokovati štetu mrežnim komponentama, hardveru i osoblju. Dobro planirana sigurnosna infrastruktura uključuje poznavanje koju imovinu treba zaštiti i na kojoj razini. Rizici se pojavljuju u mnogo različitih oblika kada je riječ o upravljanju informacijama. Potrebno je ispravno upravljati rizikom kako ne bi došlo do otkrivanja, uništenja ili prekida imovine. Upravljanje rizicima uključuje četiri faze:

- identifikacija i procjena rizika koji postoje u sustavu

- analiza utjecaja potencijalnih rizika na sustav

- formuliranje strategije kako odgovoriti na rizike

- smanjenje utjecaja rizika na buduću sigurnost

Slika 18 Upravljanje rizicima

Vjerojatnost da prijetnja može iskoristiti ranjivost kako bi nastala neka vrste štete je rizik. Iz tog razloga, kada se provodi analiza postoji li rizik, nije dovoljno samo identificirati potencijalne prijetnje, nego i utvrditi postoje li ranjivosti koje bi mogle biti iskorištene. Nakon utvrđivanja postojanja, ozbiljnost rizika se određuje na temelju koliko štete bi mogao prouzročiti i kolika je vjerojatnost da će se dogoditi. Analiza rizika je sigurnosni proces koji se koristi za procjenu štete od rizika koja može utjecati na organizaciju. Postoji šest faza u procesu analize rizika:

1. Identifikacija imovine – identificiranje imovine kojoj je potrebna zaštita i određivanje vrijednosti imovine

2. Identifikacija ranjivosti – lociranje slabosti kako bi se ustvrdilo gdje postoje problemi zaštite imovine; otkrivaju se kritična područja najosjetljivija na ranjivost

3. Procjena prijetnji – nakon utvrđivanja ranjivosti, utvrđuju se prijetnje koje bi ih mogle iskoristiti

4. Kvantifikacija vjerojatnosti – vjerojatnost da će prijetnje iskoristiti ranjivost

5. Analiza utjecaja – procjena učinka potencijalnih prijetnji; može uključivati učinak oporavka od štete ili učinak provedbe mogućih preventivnih mjera

6. Određivanje protumjera – određivanje i razvoj protumjera za uklanjanje ili smanjenje rizika; moraju biti ekonomski opravdane i osigurati očekivanu razinu zaštite, tj. protumjere ne smiju koštati više od očekivanog gubitka

Poznavanje izvora prijetnji može biti od pomoći prilikom analize rizika. Sigurnosne prijetnje često se kategoriziraju kao prirodne, umjetno stvorene ili sustavne, ovisno o njihovom izvoru, a objašnjene su u tablici ispod.

Tablica 1 Mogući izvori prijetnji

Prirodne	Poplave, tsunami, tornado, klizišta
Čovjek - namjerne	Paljevina, teroristički napadi, krađa opreme, oštećenje opreme
Čovjek – nenamjerne	Računalne pogreške zaposlenika, česte bolesti
Sustav	Neosigurana oprema, ranjivost e-pošte, nedodijeljene privilegije

Nakon što se identificira rizik, definiraju se strategije kako bi se odredile odgovarajuće radnje koje je potrebno poduzeti. Četiri su uobičajene tehnike:

Prihvaćanje – priznavanje i prihvaćanje rizika i posljedica koje dolaze s njim; prihvaćanje ne znači ostaviti sustav potpuno ranjivim, već prepoznavanje da se određeni rizik ne može u potpunosti izbjeći

Prijenos – dodjela odgovornosti za rizik drugoj agenciji ili trećoj strani kao npr. osiguravajućem društvu

Izbjegavanje – potpuno uklanjanje rizika uklanjanjem uzroka; proces može biti vrlo jednostavan poput prekida operacije ili entiteta koji je u opasnosti

Ublažavanje – primjenjuje se kada je utjecaj potencijalnog rizika značajan; može doći u obliku sigurnosnog kopiranja podataka

Rizik se može umanjiti primjenom odgovarajućih sigurnosnih kontrola. Instalacija hardvera ili softvera je tehnička kontrola. Promjene su sastavi dio svakog procesa. Kada organizacija promijeni svoj hardver, softver ili infrastrukturu, riskira uvođenje neočekivanih posljedica. Važno je da organizacija može ispravno procijeniti rizik

4.2. Kritični sustavi i funkcije

Kritični sustavi i funkcije organizacije sprječavaju istu da djeluje na utvrđenoj minimalnoj razini očekivanja. Jedan od načina za određivanje važnosti sustava ili funkcije je izrada nekih kvantitativnih podataka za usporedbu. Dalje u tekstu će biti nabrojane ukratko objašnjene uobičajene metrike koje su uključene u analizu poslovanja.

Prva u nizu metrika je maksimalno podnošljivo vrijeme zastoja (*eng. Maximum tolerable downtime – MTD)*. To je najduže vremensko razdoblje u kojem se može dogoditi prekid poslovanja bez uzroka nepopravljivog poslovnog kvara. Svaki poslovni proces može imati vlastiti MTD. Rasponi idu od minuta do sati za kritične funkcije, 24 sata za hitne funkcije, 7 dana za normalne funkcije itd. Sljedeća u nizu je ciljna točka oporavka (*eng. Recovery point objective - RPO)*. Predstavlja najdulje vremensko razdoblje u kojem organizacija može tolerirati nepopravljivost izgubljenih podataka.

RPO se obično izražava u satima i u većini IT sustava određuje učestalost izrade sigurnosnih kopija. Srodno RPO-u postoji i RTO (eng. *Recovery time objective)*, a što predstavlja duljinu vremena unutar kojeg se normalne poslovne operacije i aktivnosti mogu obnoviti nakon događaja. Normalno je i očekivano da dođe do kvara. Prosječno vrijeme za koje se očekuje da uređaj ili komponenta budu u radu definira srednje vrijeme do kvara *(eng. Mean time to failure - MTTF)*. MTTF se izračunava kao ukupni broj sati rada podijeljen s brojem kvarova. Za poslovanje je od koristi i srednje vrijeme za oporavak MTTR (*eng. Mean time to repair*) što označava prosječno vrijeme potrebno da se uređaj ili komponenta oporavi od incidenta ili kvara. Kao mjera pouzdanosti uređaja ili komponente uzima se metrika MTBF – srednje vrijeme između kvarova (*eng. Mean time between failure*).

5. NAPADI I PRIJETNJE

Brojne su vrste prijetnji i napada s kojima se može određena organizacija suočiti. Postoje različiti ciljevi, resursi i sposobnosti koje napadači posjeduju. U prošlosti, hakerom se nazivalo korisnika koji je briljirao u programiranju i administraciji računalnog sustava. Hakiranje je bilo znak tehničke vještine i kreativnosti povezane s ilegalnim i zlonamjernim upadima u sustav. Napadač je pojam koji oduvijek predstavlja zlonamjernog uljeza unutar sustava ili netko tko na bilo koji način nanosi štetu. Iz današnje perspektive, haker i napadač su srodni pojmovi za pojedince koji posjeduju vještine pristupa računalnim sustavima neovlaštenim i ilegalnim sredstvima. U ovom kontekstu, postoje dva suprotna pojma, a to su bijeli i crni šeširi. Bijeli šešir je haker koji radi u korist organizacije. On otkriva sigurnosne propuste u aplikacijama i sustavima kako bi ih proizvođači mogli popraviti prije nastanka problema. Ova aktivnost se obavlja uz suglasnost proizvođača. Crni šešir je haker koji razotkriva sigurnosne propuste radi zlonamjerne svrhe i financijske dobiti. Ova aktivnost se provodi bez suglasnosti organizacije.

Slika 19 Članci s portala povezani za računalni kriminal

5.1. Društveni inženjering

Kada se razmišlja o napadima na informacijske sustave, najviše se pitanja postavlja o zaštiti tehnoloških komponenata tih sustava. Međutim ljudi, korisnici sustava, jednakim dijelom su dio informacijskog sustava kao i tehnološke komponente. Ljudi također imaju vlastite ranjivosti i mogu podleći određenim vrstama napada. Korist računala i tehnologije dolazi od načina na koji ih ljudi koriste i komuniciraju s njima, a s druge strane i napadači su upoznati s tom činjenicom.

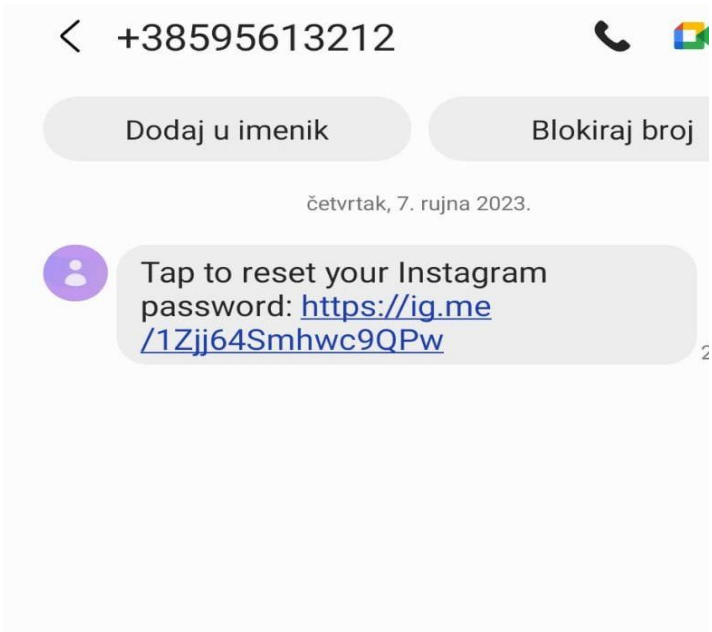
Napad društvenim inženjeringom koristi obmanu i prijevaru kako bi uvjerio korisnika da prekrše sigurnosne smjernice i daju osjetljive podatke. Izvedivi su na razne načine: osobno, putem e-pošte ili preko telefona. Žrtve su obično korisnici koji nemaju tehničko znanje. Društveni inženjering se smatra jednom od najčešćih i najuspješnijih zlonamjernih tehnika u informacijskoj sigurnosti. Učinkovitost postiže postavljanjem lažnog autoriteta ili uvjeravanjem u hitnost situacije. Jednostavnije je implementirati sigurnost u softver ili hardver nego u potpunosti obučiti ljudske resurse. Budući da je društveni inženjering neizravan i varljiv, jedan nemaran i tehnološki neiskusan korisnik je dovoljan da bi ugrozio cijeli rad.

5.1.1. Lažno predstavljanje i podvale

Lažno predstavljanje je napad u kojem se napadač pretvara da je netko tko nije. Oponašanje je često uspješno u situacijama u kojima se ne može lako utvrditi identitet. Cilj prijevare je navesti korisnika da izvrši nepotrebnu ili neželjenu radnju. Poput ostalih tehnika, također ovisi o količini iskustva kojeg meta ima s računalnom tehnologijom. Od koristi je naglasiti i nekoliko vrsta iskorištavanja društvenog inženjeringa koji omogućuju napadačima da dobiju fizički pristup ograničenim informacijama i resursima. Gledanje preko ramena pojedinca dok ona/on unosi podatke o lozinki ili PIN-u poznato je kao *eng. shoulder surfing*. Danas je ovo vrlo jednostavno učiniti s mobilnim telefonima i njihovom kamerom. Zanimljiva je metoda povratka važnih informacija pregledom sadržaja kontejnera za smeće. Posebna učinkovitost metode se javlja u prvih nekoliko tjedana u godini jer korisnici odbacuju stare kalendare s upisanim lozinkama i ostalim povjerljivim informacijama.

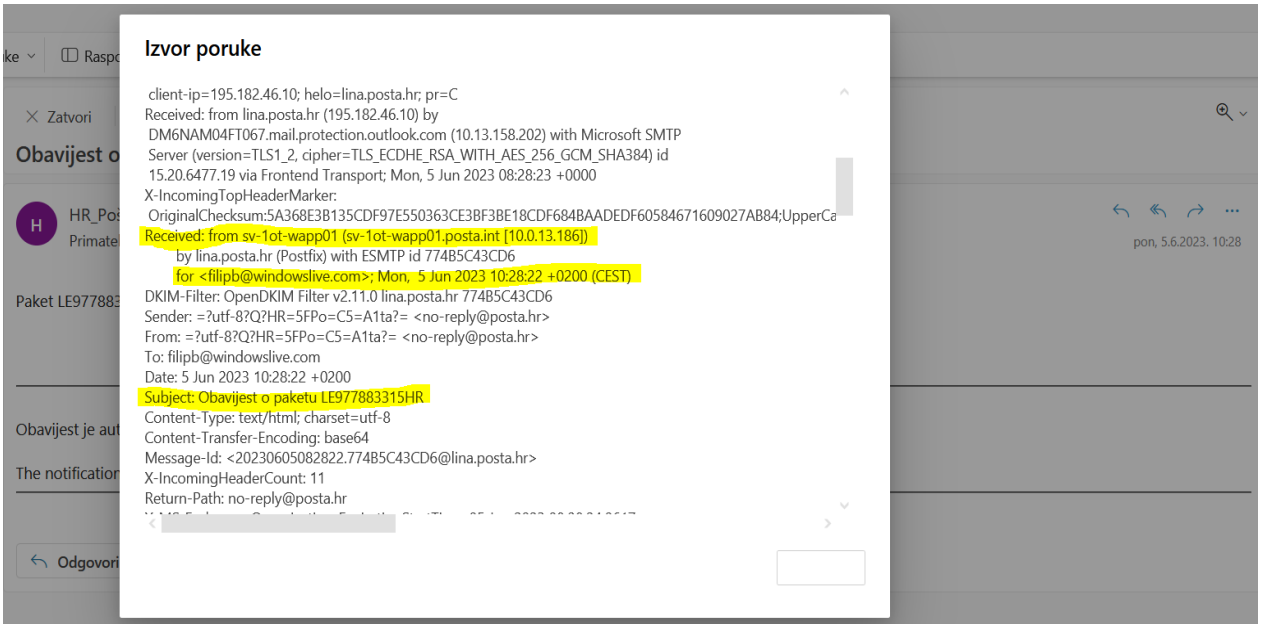
5.1.2. Phishing i srodni napadi

Elektronička pošta je službeni kanal komunikacije u mnogim poduzećima , no može predstavljati i određene rizike posebno zbog slanja neželjene pošte. Phishing (od eng. izraza fishing, u prijevodu ribarenje/pecanje) je vrsta socijalnog inženjeringa koja se odnosi na prijevare kojima se služe napadači šaljući najviše lažne e-mail poruke ili poruke drugim kanalom komunikacije (SMS, društvene mreže) kako bi „upecali“ povjerljive podatke. Napadač zahtjeva odgovor na poruku, klik na poveznicu ili otvaranje priloga (najčešće virus). Po primitku ovakve vrste poruke, prva reakcija bi trebala biti da se zapitamo očekujemo li primljenu e-mail poruku i očekujemo li poruku baš od tog pošiljatelja, a zatim i je li zahtjev u poruci opravdan. Važan je i sadržaj same poruke. Ako je ponuđena neka predobra ponuda, postoji velika mogućnost da se radi o prijevari. Razvilo se nekoliko varijacija krađe identiteta. Kada napadač kao metu izabire uži krug ljudi, poput pojedine organizacije ili pojedinca te priprema napad posebno za njih, takav napad se naziva spear phishing. Prevedeno na hrvatski jezik, kitolov (eng. whaling), kao žrtvu izabire osobu visokog profila ili osobu koja posjeduje vrijednosne informacije. Napad nazvan pharming se izvodi preusmjeravanjem na određeno web mjesto, ali lažno.



Slika 20 Primjer phishing poruke [11]

E-mail je danas najpopularniji način komunikacije bilo za službenu ili neslužbenu komunikaciju. Iz tog razloga često je ključni dokaz prilikom analize. Za forenzičku istragu važno je proučiti zaglavlje same poruke u kojoj se nalaze informacije koje bi mogle biti od koristi. Ti podaci u zaglavlju se postavljaju automatski i mogu se vidjeti bez posebnih alata. Slika 18 prikazuje primjer lažne e-mail adrese gdje se pošiljatelj predstavlja kao Hrvatska pošta te šalje obavijest i link za praćenje navodne pošiljke.



Slika 21 Analiza zaglavlja e-mail poruke

5.2. Zlonamjerni softver (malware)

Zlonamjerni kod jedna je najčešćih prijetnji današnjim računalima. Čak i redoviti prosječni korisnik računala, doći će do susreta s neželjenim softverom. To je neovlašteni ili neželjeni softver koji se postavlja u ciljni sustav da ometa operacije i preusmjerava resurse u korist napadača. Ovakva vrsta koda često se kombinira s društvenim inženjeringom kako bi se korisnika uvjerilo da je zlonamjerni softver iz pouzdanog izvora.

5.2.1. Virusi i crvi

Virus je komadić zlonamjernog koda koji se širi s jednog računala na drugo spajajući se na druge datoteke. Proces ne počinje sve dok ne dođe do neke ljudske radnje, kao npr. otvaranje zaraženog privitka e-pošte. Svrha virusa je omogućiti daljnje napade, poslati podatke natrag napadaču ili čak uništiti podatke. Zbog svoje prirode, stalnog umnožavanja, viruse je teško u potpunosti ukloniti iz sustava. Postoje razne vrste zlonamjernog softvera koji se naziva virusom, a u nastavku će biti ukratko opisani neki od najpoznatijih.

Adware je softver koji automatski prikazuje ili preuzima neželjene reklame kada je u upotrebi. Često se pojavljuje na računalu korisnika kao skočni prozor preglednika. Može smanjiti produktivnost samog računala usporavajući ga ili jednostavno smetajući.

Spyware je špijunski softver namijenjen praćenju i izvješćivanju te preuzimanju kontrole nad računalom korisnika bez njegovog znanja. Razvijen je za komercijalnu dobit. Prikupljeni podaci mogu biti povijest pregledavanja interneta, osobni podaci, korisnička imena i lozinke. Posljedice se očituju u degradiranim performansama sustava kao npr. opterećenje procesora te povećana mrežna aktivnost.

Trojanski konj ili često nazivani trojanac uzrokuje štetu sustavu dajući napadaču platformu za nadzor i/ili kontrolu sustava. Puno lakše ostaje neotkriven jer se predstavlja kao neki koristan softver. Najčešće se skriva u inače benignom paketu pa tako npr. preuzimanjem računalne igrice piratskim putem, često se u paketu dobije i trojanac.

Ransomware je sve popularnija vrsta malwarea. Napadač inficira žrtvino računalo kodom koji žrtvi ograničava pristup njezinu računalu ili podacima na njemu. Nakon toga, napadač zahtijeva plaćanje otkupnine pod prijetnjom da će zadržati ograničenje ili uništiti zaključane podatke.

Izuzetno je štetan kada iskorištava snagu enkripcije te tako učini bezvrijednima podatke koji nisu sigurnosno kopirani.

Samim tim dolazi i do sve veće vjerojatnosti da će žrtve platiti otkupninu za dekriptiranje svojih datoteka. Ne tako davno, 2017. godine dogodio se možda i najpoznatiji ransmoware napad pod nazivom „WannaCry“.

Pogođeni su između ostalog sustav javnog zdravstva Ujedinjenog kraljevstva, tvrtka koja upravlja željezničkom infrastrukturom u Njemačkoj, Ministarstvo unutarnjih poslova Ruske Federacije te mnogi drugi. Navodi se da je ugroženo bilo preko 200 000 korisnika. Za sprječavanje zaraze dovoljno je bilo samo redovito ažurirati računalo, no mnoga računala nisu bila ažurirana.

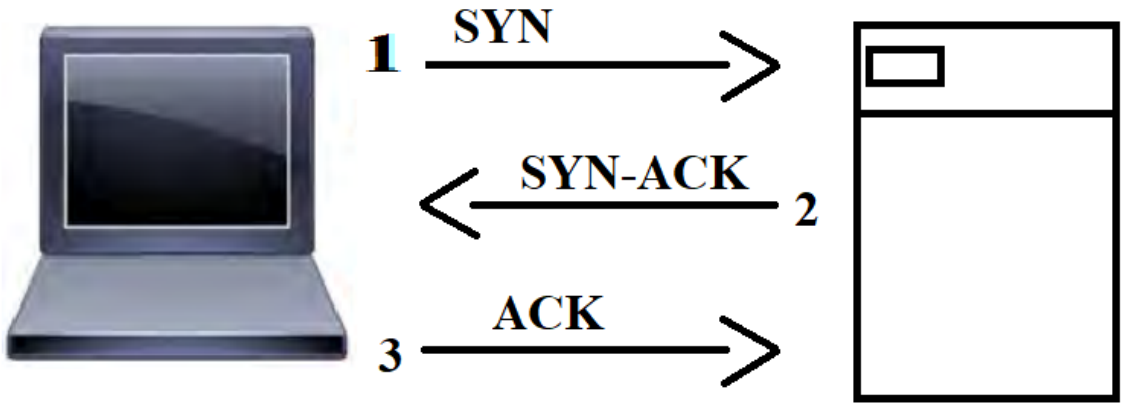
5.3. Prijetnje na mreži

Mreža je žila kucavica današnjeg poslovanja, bilo da je riječ o lokalnoj ili bežičnoj mreži. Mreža omogućuje ljudima da ostanu povezani jedni s drugima na organiziran način, a tvrtkama omogućuje pristup i dijeljenje informacija što je brže i sigurnije moguće. Većina današnjih tvrtki oslanja se na svoje mreže kao temelj svih operacija. Uz pomoć mreže, ljudi ostaju povezani jedni s drugima na organiziran način, a tvrtkama omogućuje pristup i dijeljene informacija što je sigurnije i brže moguće.

5.3.1. TCP/IP

Poznavanje TCP/IP-a dobar je početak za razumijevanje načina na koji može doći do pokretanja mrežnih napada. TCP/IP (eng. *Transmission Control Protocol/Internet Protocol*) je standardni mrežni protokol koji se danas koristi. To je slojeviti skup kojeg čini više protokola. Svaki uređaj domaćin (host) na TCP/IP mreži prima brojčanu adresu kao i opisno ime. Ova veza između klijenta i poslužitelja uspostavlja se metodom trosmjernog rukovanja. Prvo klijent šalje SYN (sinkronizacijski) paket poslužitelju. Zatim poslužitelj prima SYN paket i odgovara sa SYN-ACK (sinkronizacija-potvrda) paketom. Na kraju, klijent prima SYN-ACK paket i odgovara ACK (potvrda) paketom.

Mrežni sloj razlikuje dva protokola: TCP i UDP. TCP je pouzdan protokol koji osigurava provjeru prijema podataka, dok to nije slučaj kod UDP. Za prijenos većih poruka, kada komunikacija traje dulje vremena, koristi se TCP, a UDP za kratke poruke tipa upit-odgovor.



Slika 22 Trosmjerno rukovanje

Slojevitu strukturu ovog mrežnog protokola čine četiri sloja, a to su: sloja podatkovne veze, mrežni, transportni i aplikacijski sloj. Često se postavlja paralela s OSI modelom koji sadrži sedam slojeva.

5.3.2. Napadi na mreži

Nije neuobičajeno lažno predstavljanje na mreži. Tako imamo lažiranje IP adrese kao i lažiranje adrese kontrole pristupa medijima (MAC). U napadu lažiranja IP adrese, napadač šalje IP pakete s lažne adrese kako bi uspostavio komunikaciju s metama. Krivotvorenje MAC adrese mijenja početnu dodijeljenu MAC adresu mrežnog sučelja na uređaju u mreži. Iako je MAC adresa tvrdo kodirana na mrežnom sučelju, postoje alati koji će natjerati operativni sustav da vjeruje da sučelje ima drugu MAC adresu.

Portovi su logičke krajnje točke između računala. Otvoreni port je ono što napadač traži kada skenira portove. Skeniranje portova je vrsta napada gdje potencijalni napadač skenira računala i uređaje kako bi vidio koje su usluge u sustavu aktivne. Smatra se da je ovo često prvi u nizu napada na cilj. Kada su u pitanju prisluškivanja, ona mogu biti na žičanoj i bežičnoj mreži. Na žičanoj mreži napadač mora imati fizički pristup ili pristupiti mrežnom kabelu, dok je kod bežične mreže potrebno imati uređaj koji može primati signale.

Jedan od načina prisluškivanja je „Čovjek u sredini napada“ (eng. *Man in the middle attacks*). U tom slučaju napadač uspostavlja vezu između dvije žrtve i prenosi informacije između njih kao da izravno razgovaraju jedna s drugom. U stvarnosti, napadač kontrolira informacije koje putuju između dviju žrtava.

Napad uskraćivanjem usluge (eng. *DoS – Denial of service*) je vrsta mrežnog napada u kojem napadač pokušava poremetiti ili onemogućiti sustave koji pružaju mrežne usluge na različite načine. Ovakvi napadi često koriste krivotvorenje IP adresa kako bi preopteretili mrežu i uređaje paketima koji izgledaju kao da dolaze s legitimnih IP adresa. Napad može imati za cilj bilo koju uslugu ili mrežni uređaj, ali obično se postavlja protiv poslužitelja ili usmjerivača.

5.3.3. Bežične prijetnje

Bežične mreže su posvuda, a zaštita uređaja od ranjivosti bežičnim putem ključna je za zaštitu osjetljivih podataka od neovlaštenog pristupa. Bežične mreže brzo su postale norma u današnjem poslovanju. Većina organizacija ima bežičnu mrežu za pristup zaposlenicima dok su u pokretu unutar svojih objekata. Lažne pristupne točke mogu uzrokovati značajnu štetu podacima organizacije. U kontekstu bežičnog umrežavanja, ometanje odnosno interferencija je napad u kojem radiovalovi ometaju bežične signale. Obično se događa kod kuće zbog različitih elektroničkih uređaja koji rade u propusnosti bliskoj bežičnoj mreži. Dolazi do čekanja prije slanja, a čekanje ponekad može biti neodređeno. Napadači mogu presresti prijenos i ometati normalan tijek prometa kroz mrežu. Slanje neželjenog sadržaja može se odviti i preko Bluetooth signala s pametnih telefona. Bluetooth ima relativno niske granice prijenosa te je obično ovaj napad iz neposredne blizine. Može dovesti do kvara uređaja ili čak širiti viruse.

Komunikacija kratkog polja (eng. *Near Field Communication* – NFC) je komunikacija između mobilnih uređaja koji su vrlo blizu. Npr. učestala je upotreba NFC-a za komunikaciju s terminalima za beskontaktno plaćanje (Android Pay, Apple Pay). Za razliku od Bluetootha, NFC je više ograničen od Bluetootha u pogledu količine podataka koji se mogu prenijeti.

Velika primjena je i radiofrekvencijske identifikacije (RFID) gdje se koriste elektromagnetska polja za identifikaciju i praćenje čipova koji su integrirani u odabrane objekte i koji pohranjuju informacije o njima. Najšira primjena je kod kartica za beskontaktno plaćanje.

6. PRIMJENA DIGITALNE FORENZIKE

6.1. Proces istrage

DFRWS (eng. Digital Forensics Research Workshop) je model koji je razvijen pri digitalnoj istraživačkoj radionici. Ovaj model obuhvaća digitalno istražne radnje koje su definirane klasama. Klase služe za kategorizaciju istražnih radnji. Promatrajući ovaj model, postoji ukupno šest faza u procesu digitalne forenzike, a to su: identifikacija, prikupljanje i pohrana, pretraživanje, analiza, prezentacija i odluka.

Identifikacija podrazumijeva osiguranje značajnih elektronskih zapisa koji su dostupni i upotrebljivi. Od velike važnosti je jasno definiranje procedure, kao i razumijevanje pravnih normi. Ovdje se utvrđuje raspolaganje sa svom potrebnom infrastrukturom i tehnologijom za provođenje istrage. Dolazi do razvoja plana, daju se zadaci službenicima kao i tehnički zahtjevi. Cilj je što detaljnija dokumentacija radi krhkosti digitalnih dokaza. Prema forenzici, zločinac ne može otići s mjesta zločina bez da ostavi trag ili ponese nešto sa sobom. Postoje različite forme digitalnog dokaza kao npr. logovi aplikacija, metapodaci, logovi mrežnog prometa, sadržaj iz baze podataka itd. Također, elektronski uređaji mogu biti nestabilni (slaba baterija, prekid struje) te sama identifikacija može biti poprilično složena i zahtjevna.

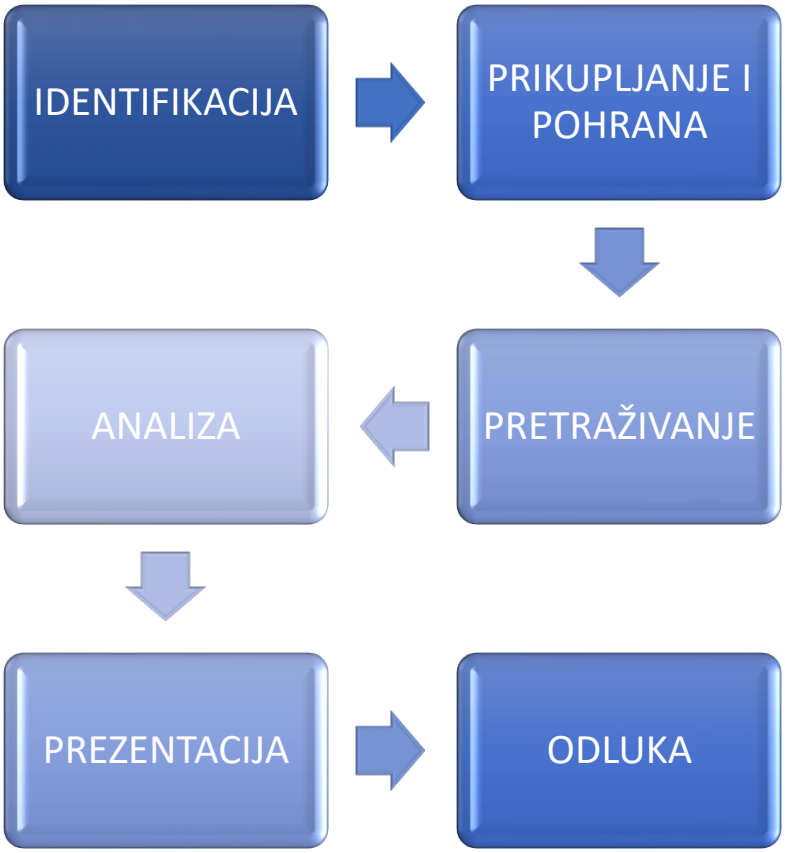
Forenzička pohrana predstavlja bit po bit kopiju originalnog dokumenta, datoteke, slike ili diska. Prikupljanje podrazumijeva pohranu i osiguranje osjetljivih digitalnih dokaza tj. dokaza koji se mogu lako izmijeniti ili ukloniti. Bitna je izolacija sustava iz mreže kao i prepoznavanje mogućih sumnjivih procesa. U ovoj fazi se radi kompletna kopija na forenzičkom računalu. Odgovornost ove faze je u poduzimanju potrebnih mjera s ciljem očuvanja integriteta fizičkih i digitalnih dokaza. Kako bi istraga bila što uspješnija, bitnu ulogu imaju korišteni forenzički alati i metode kao i sama stručnost istražitelja. Veliki broj stručnjaka se slaže da baš od ove faze počinje prava digitalna istraga. Istražitelji naprave veći broj kopija digitalnih dokaza iz svih izvora dok se originalni materijal pohranjuje unutar sigurnog okruženja u nepromijenjenom stanju.

Ukoliko je poznato što se otprilike traži, moguće je olakšati istragu i pretraživati prema ključnim riječima, mailu, kolačićima, datumu nastanka ili zadnje promjene datoteke itd. Faza pronalaženja daje uvid i očigledne dijelove digitalnih dokaza koji odgovaraju pojedinoj vrsti nezakonite aktivnosti. Pretraživanje je moguće izvesti direktno na terenu, ali je preporuka da se odradi u forenzičkom laboratoriju.

Analizom digitalnih dokaza pronalaze se i povezuju činjenice. Podrazumijeva se vrlo detaljan pregled podataka. Tijekom istrage, informacije se prikupljaju iz raznih izvora. Podaci sami za sebe ne mogu složiti priču i događaj već se moraju povezati kako bi se izgradila cjelina. Kreira se vremenska crta razvoja događaja. Ovim se dolazi do odgovora gdje, kada, a ponekad i kako se dogodio istraživani događaj.

Istražitelj mora na jednostavan način obrazložiti rezultate istrage iz prethodnih faza. Vodi see računa o tome da se isti mogu ponoviti ili da netko drugi može doći do jednakih zaključaka. Izvještaj je ključna faza digitalne forenzike jer sadržava detaljnu dokumentaciju alata, procesa i metodologije. Kada je istraga zaključena i slučaj predan na sud, rezultati istrage se prezentiraju odvjetnicima i tužilaštvu. U nekim slučajevima od načina prezentacije ovisi i tok cijelog slučaja.

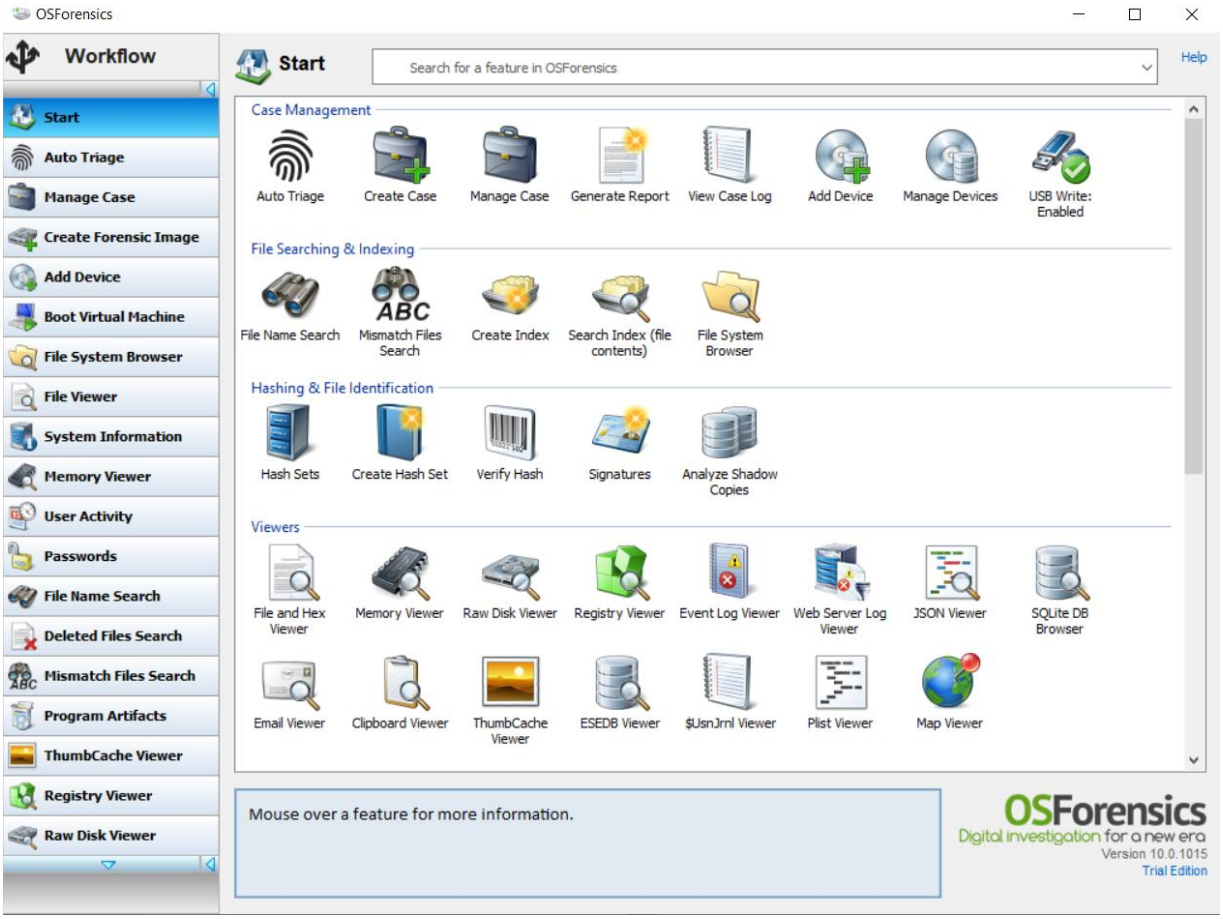
Interes svih istražitelja je sastaviti istinitu verziju događaja potkrijepljenu dokazima. Krajnji korak prikupljanja informacija i obavljene analize se svodi na dokument i odluku vještaka. Sud na temelju svih rezultata vještačenja i cjelovite priče donosi odluku.



Slika 23 Blok dijagram procesa istrage

6.2. Primjena OSFORENSICS

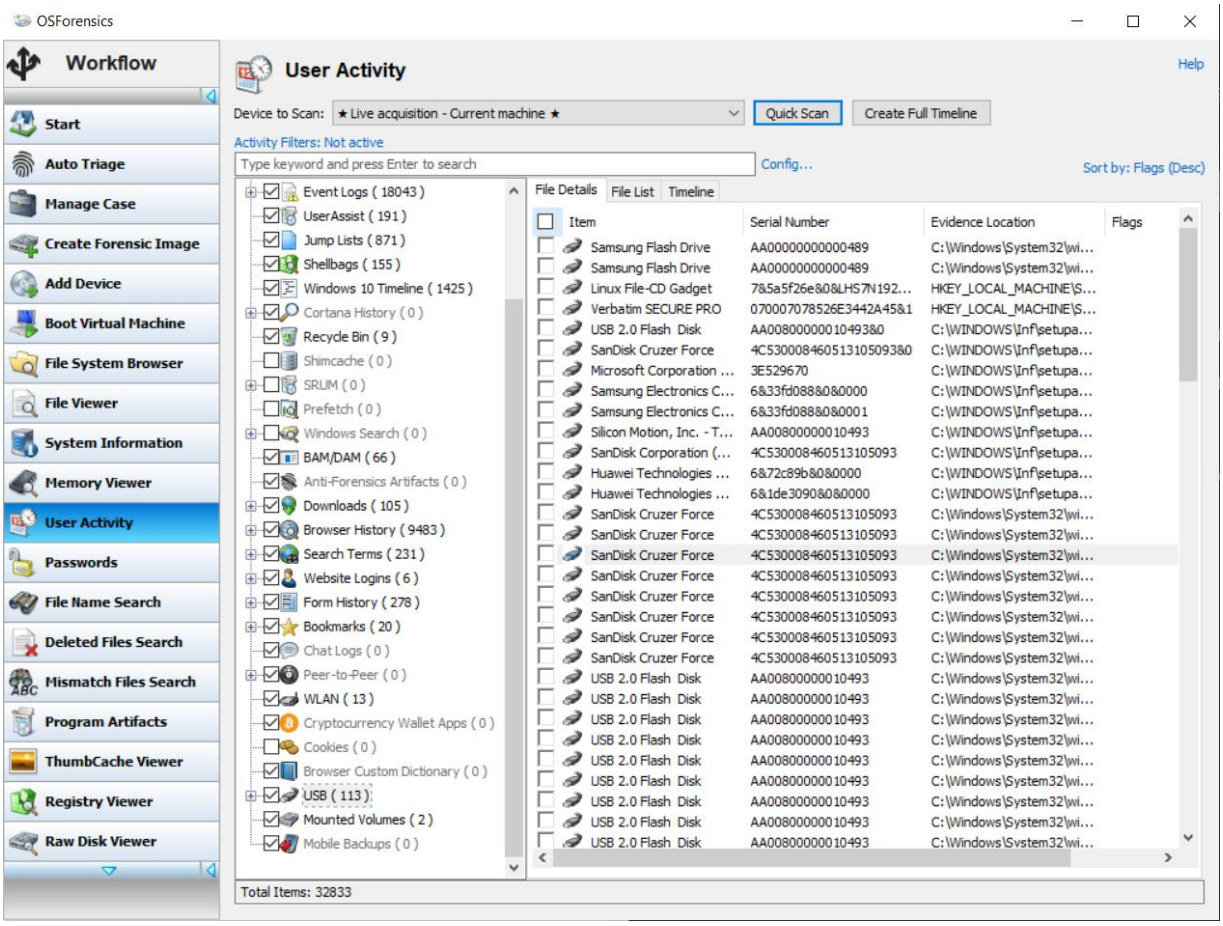
Ovo poglavlje će dati uvid u neke funkcije jednog od moćnih alata za digitalnu forenziku. Riječ je o programu OSForensics. Program je lako dostupan i vrlo lagan za instalaciju. Može se preuzeti kao besplatna, probna verzija na rok od 30 dana, kako je i napravljeno u svrhu analize i potreba ovog rada. Redovna godišnja licenca ovog programa iznosi 799$ godišnje za jednog korisnika.



Slika 24 Sučelje programa OSForensics

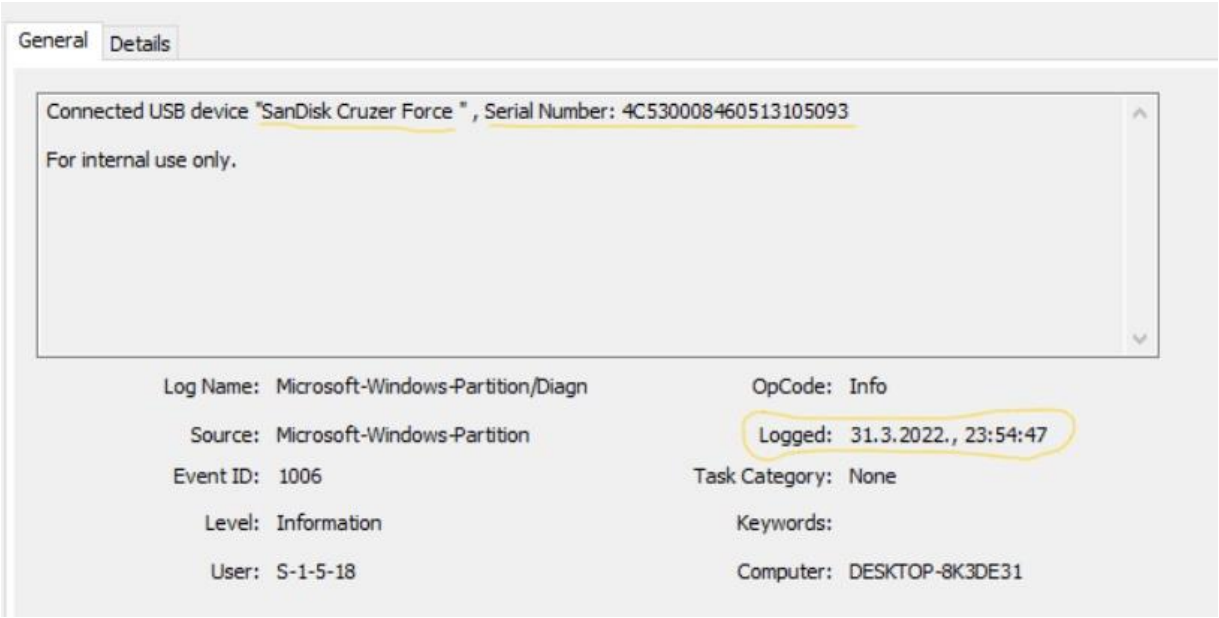
OSForensics skenira sustav korisnika tražeći dokaze o nedavnim aktivnostima kao što su web stranice kojima se pristupilo, USB priključci, bežične mreže, prijave na web stranice kao i spremljene lozinke. Jako je korisno za uvid u račune ili bilo kakve materijale kojima se pristupalo na uređaju.

S lijeve strane početnog zaslona, unutar samog programa nalazi se popis mogućih izbornika koji nude daljnje opcije. Na samom startu analize, izabran je izbornik koji daje uvid u aktivnost korisnika.



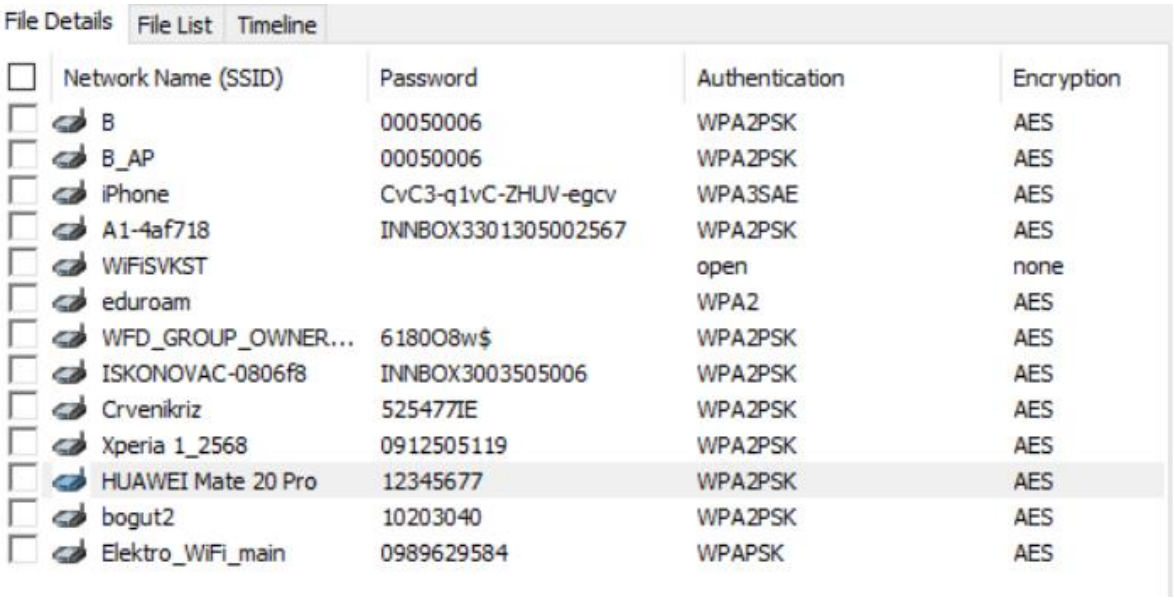
Slika 25 Popis pronađenih USB priključaka

Klikom na podizbornik USB, s desne strane se prikaže popis USB priključaka koji su bili spojeni na promatranom uređaju. Prikazane su informacije o datumu zadnje veze, ali i podaci o uređaju kao što su naziv proizvođača, ID proizvoda i serijski broj. Moguće je očitati USB vanjske memorije, prijenosni hard disk te bilo kakve vanjske uređaje povezane putem USB priključka.



Slika 26 Detaljniji prikaz informacija o spajanju USB priključka

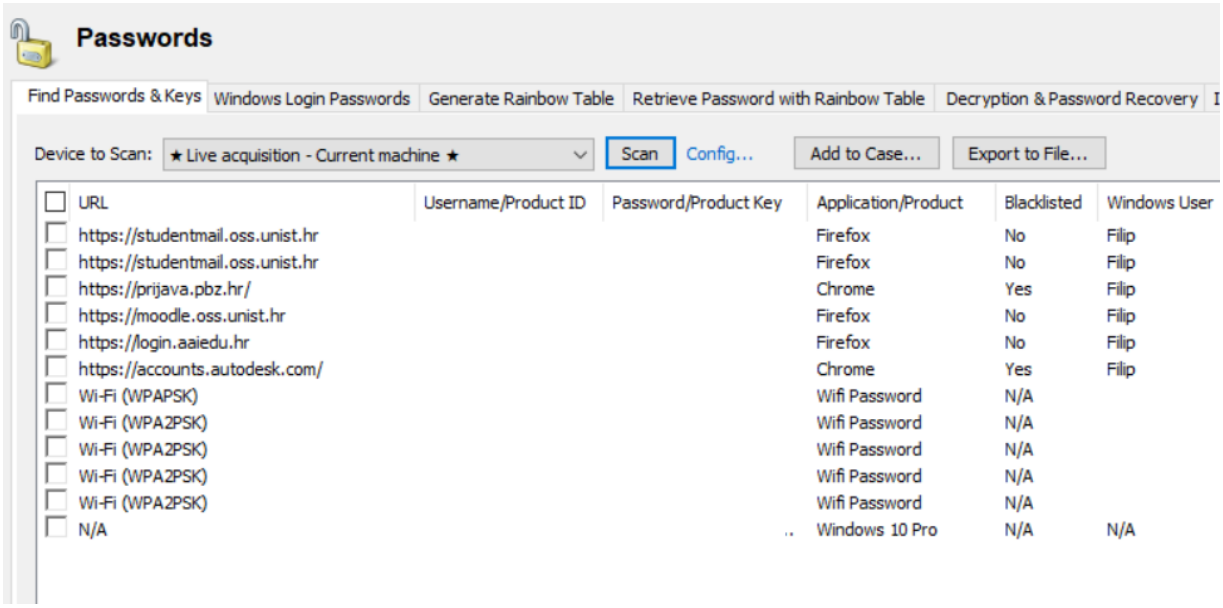
OSF može ispisati bežične WiFi pristupne točke na koje se uređaj povezivao u prošlosti, uključujući datum i vrijeme kada je došlo do spajanja.



Network Name (SSID)	Password	Authentication	Encryption
B	00050006	WPA2PSK	AES
B_AP	00050006	WPA2PSK	AES
iPhone	CvC3-q1vC-ZHUV-egcv	WPA3SAE	AES
A1-4af718	INNBOX3301305002567	WPA2PSK	AES
WiFiSVKST		open	none
eduroam		WPA2	AES
WFD_GROUP_OWNER...	6180O8w$	WPA2PSK	AES
ISKONOVAC-0806f8	INNBOX3003505006	WPA2PSK	AES
Crvenikriz	525477IE	WPA2PSK	AES
Xperia 1_2568	0912505119	WPA2PSK	AES
HUAWEI Mate 20 Pro	12345677	WPA2PSK	AES
bogut2	10203040	WPA2PSK	AES
Elektro_WiFi_main	0989629584	WPAPSK	AES

Slika 27 Popis WiFi spajanja

Odabirom izbornika lozinke, dolazi se do uvida u lozinke spremljene na određenim web preglednicima kao i lozinke za pristupne točke na kojima se spajalo. Prikaže se link stranice, korisničko ime za prijavu te sama lozinka za pristup (za potrebe rada korisnička imena i lozinke su izrezane iz snimke vlastitog zaslona).



Slika 28 Prikaz spremljenih lozinki

Prethodno je prikazan samo mali dio potencijala ovog alata za digitalnu forenziku. Mogućnosti su brojne, a uvid u rezultate jasno prikazan. Na izbor su dostupni mnogi podizbornici te se lako adaptirati na snalaženje u programu.

7. ZAKLJUČAK

Uređaji, a i općenito tehnika u stalnom su razvitku iz dana u dan. U jednu ruku to olakšava ljudima život, pomaže u mnogim situacijama, dok s druge strane na isti način se razvijaju i metode zlouporabe. Računalni kriminal je sve prisutniji u današnjem svijetu. Pojava je sve većeg beskontaktnog plaćanja i prenošenja informacija te bitnih podataka udaljenim putem. Velike tvrtke i organizacije ne mogu zamisliti svoje poslovanje bez e mail komunikacije. Svi ti sustavi imaju svoje ranjivosti i nedostatke. Na samoj organizaciji je da se posveti očuvanju svoje infrastrukture kao i podataka kako ne bi došlo do curenja informacija. Kao posljedica svega ovog razvila se relativno nova grana znanosti, a to je digitalna forenzika. Mnogi smatraju da je računalna isto što i digitalna, međutim računalna forenzika je samo jedan dio digitalne forenzike. Ovim radom, približen je sam pojam digitalne forenzike. Rad daje uvid u određene grane ove znanosti kroz konkretne vlastite primjere te koristeći vlastitu opremu. Od nužne važnosti je obučiti ljude kako bi pravilno pristupili svim mogućim napadima i problemima koji se pojave tijekom obavljanja posla. Jedan krivi korak, odnosno u ovom slučaju klik miša, može dovesti do niza problema. Tu su i razni sustavi kontrole i zaštite koji se postavljaju, ali ljudski faktor je najbitniji. Kroz rad su prikazani neki od najčešćih napada današnjice. Također opisane su ranjivosti na koje ciljaju napadači te razni izazovi s kojima se susreću istražitelji tijekom istrage. Trenutno su dostupni i razni forenzički alati, softverski i hardverski, kako bi proučavanje i analiza digitalne forenzike bili olakšani. Većina od njih je poprilično skupa, komercijalna, ali postoje i besplatni programi koji mogu odraditi dobar dio posla. Cijela komunikacija se odvija putem mreže, a mreža je sastavljena od niza elemenata, protokola i procesa. Zbog toga obučavanje ide u smjeru uskih područja (stručnjak za mrežu, programiranje, baze podataka itd.). Bitno je bilježiti sve propuste koji se dogode kako bi se u budućnosti u početku napada ili štete znalo barem kojom metodom započeti proces. Na samom kraju opisan je proces istrage te primjena jednog jakog alata OSFORENSICS za kojeg je potrebno posjedovati godišnju licencu. Za svrhe ovog rada, iskorištena je mogućnosti probnog besplatnog perioda korištenja programa od 30 dana.

LITERATURA

[1] Taylor Pamela J., Nufryk Jason, *CompTIA Security+ (Exam SY0-501)*

[2] Chapple Myke, Seidl David, *CompTIA Scurity+ Study guide (Exam SY0-601)*

[3] Pale Predrag, Petrović Juraj, *Računalna forenzika – materijali (FER),* https://www.fer.unizg.hr/predmet/racfor_b/materijali (Posljednji pristup: 22.8.2023. god.)

[4] https://mup.gov.hr/istaknute-teme/nacionalni-programi-planovi-i-projekti/nacionalne-strategije/kiberneticka-sigurnost/222335 (Posljednji pristup: 4.1.2024. god.)

[5] Nacionalni CERT, *Računalna forenzika,* https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-05-301.pdf (Posljednji pristup 25.8.2023. god.)

[6] https://security.foi.hr/wiki/index.php/Ra%C4%8Dunalni_kriminal/cyber_kriminal.html (Posljednji pristup (28.8.2023. god.)

[7] https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools (Posljednji pristup 28.8.2023. god.)

[8] https://www.cert.hr/wp-content/uploads/2018/01/wireshark.pdf

(Posljednji pristup 28.8.2023. god.)

[9] https://en.wikipedia.org/wiki/Computer_forensics (Posljednji pristup 29.8.2023. god.)

[10] https://www.sleuthkit.org/autopsy/ (Posljednji pristup 31.8.2023. god.)

[11] https://hrcak.srce.hr/file/315458 (Posljednji pristup 9.1.2024. god.)

[12] https://www.cert.hr/phishing/ (Posljednji pristup 2.9.2023. god.)

[13] https://www.dalmacijadanas.hr/splicanka-nije-nasjela-dobila-je-poruku-s-poveznicom-i-konzultirala-se-sa-strucnjakom/ (Posljednji pristup 7.9.2023. god.)

[14] https://www.cert.hr/19795-2/malver/ (Posljednji pristup 4.9.2023.)

[15] https://www.osforensics.com/ (Posljednji pristup 6.9.2023. god.)

POPIS SLIKA

POPIS TABLICA