# Računalna forenzika: metodologije, alati i primjena u analizi digitalnih dokaza

**Bubalo, Goran**



**VELEUČILIŠTE U ŠIBENIKU**

**ODJEL POSLOVNE INFORMATIKE**

**PREDDIPLOMSKI STRUČNI STUDIJ POSLOVNA INFORMATIKA**

**Goran Bubalo**

# RAČUNALNA FORENZIKA: METODOLOGIJE, ALATI I PRIMJENA U ANALIZI DIGITALNIH DOKAZA

**Završni rad**

Šibenik, 2024.

**VELEUČILIŠTE U ŠIBENIKU**

**ODJEL POSLOVNE INFORMATIKE**

**PREDDIPLOMSKI STRUČNI STUDIJ POSLOVNA INFORMATIKA**

# RAČUNALNA FORENZIKA: METODOLOGIJE, ALATI I PRIMJENA U ANALIZI DIGITALNIH DOKAZA

**Završni rad**

**Kolegij:** Zaštita i sigurnost informacijskih sustava

**Mentor:** Zvonimir Klarin, mag. ing. comp., predavač

**Student:** Goran Bubalo

**Matični broj studenta:** 1219065088

Šibenik, rujan 2024.

**IZJAVA O AKADEMSKOJ ČESTITOSTI**

Ja, Goran Bubalo, student/ica Veleučilišta u Šibeniku, JMBAG 1219065028 izjavljujem pod materijalnom i kaznenom odgovornošću i svojim potpisom potvrđujem da je moj završni/diplomski rad na stručnom prijediplomskom / stručnom diplomskom studiju Poslovna Informatika pod naslovom: Računalna Forenzika: Metodologije, Alati i Primjeri u Analizi Digitalnih Dokaza isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.

Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

U Šibeniku, 19. 09. 2024

Student/ica:

G

TEMELJNA DOKUMENTACIJSKA KARTICA

Veleučilište u Šibeniku Završni rad

Odjel Poslovne Informatike

Stručni prijediplomski studij Poslovna Informatika

# RAČUNALNA FORENZIKA: METODOLOGIJE, ALATI I PRIMJENA U ANALIZI DIGITALNIH DOKAZA

GORAN BUBALO

goranbubalo2422003@gmail.com

Računalna forenzika ključna je disciplina u suvremenim istragama, omogućujući prikupljanje, očuvanje i analizu digitalnih dokaza. Ovaj rad istražuje povijest, metodologije, alate i buduće trendove računalne forenzike, uz analizu stvarnih slučajeva. Razvoj računalne forenzike započeo je kao odgovor na prve slučajeve kompjuterskih prevara i hakiranja, a s ekspanzijom Interneta i razvojem digitalnih tehnologija postala je ključan dio kibernetičke sigurnosti. Osnovni principi forenzičke analize uključuju prikupljanje, očuvanje, analizu i izvještavanje o digitalnim dokazima. Računalna forenzika obuhvaća različite specijalizirane grane, poput forenzike tvrdih diskova, mrežne forenzike, forenzike mobilnih uređaja, cloud forenzike, forenzike zlonamjernog softvera i forenzike Interneta stvari, čime pokriva širok raspon digitalnih okruženja. Forenzička analiza pomoću alata *Autopsy*, provedena u praktičnom dijelu rada, omogućila je identifikaciju sumnjivih datoteka, analizu metapodataka te oporavak izbrisanih podataka. Time je demonstrirana primjena teorijskih koncepata u stvarnim istragama, čime se potvrdila važnost ovakvih alata u forenzičkoj praksi.

(43 stranica / 12 slika / 1 tablica / 35 literaturnih navoda / jezik izvornika: hrvatski)

Rad je pohranjen u digitalnom repozitoriju Knjižnice Veleučilišta u Šibeniku

Ključne riječi: Računalna forenzika, digitalni dokazi, forenzička analiza, Autopsy

Mentor: Zvonimir Klarin, mag. ing. comp., predavač

Rad je prihvaćen za obranu dana: 18.9.2024.

BASIC DOCUMENTATION CARD

Šibenik University of Applied Sciences Bachelor's thesis

Department of Business Informatics

Undergraduate professional study of Business informatics

# COMPUTER FORENSICS: METHODOLOGIES, TOOLS, AND APPLICATIONS IN DIGITAL EVIDENCE ANALYSIS

GORAN BUBALO

goranbubalo2422003@gmail.com

Computer forensics is a key discipline in modern investigations, enabling the collection, preservation, and analysis of digital evidence. This paper explores the history, methodologies, tools, and future trends of computer forensics, along with an analysis of real-world cases. The development of computer forensics began as a response to early cases of computer fraud and hacking, and with the expansion of the Internet and the advancement of digital technologies, it has become a crucial part of cybersecurity. The fundamental principles of forensic analysis include the collection, preservation, analysis, and reporting of digital evidence. Computer forensics encompasses various specialized branches, such as hard disk forensics, network forensics, mobile device forensics, cloud forensics, malware forensics, and Internet of Things (IoT) forensics, covering a wide range of digital environments. The forensic analysis using the *Autopsy* tool, conducted in the practical part of this paper, enabled the identification of suspicious files, metadata analysis, and the recovery of deleted data. This demonstrated the application of theoretical concepts in real-world investigations, confirming the importance of such tools in forensic practice.

(43 pages / 12 figures / 1 tables / 35 references / original in Croatian language)

Thesis deposited in Polytechnic of Šibenik Library digital repository

Keywords: Computer forensics, digital evidence, forensic analysis, Autopsy

Supervisor: Zvonimir Klarin, mag. ing. comp., lecturer

Paper accepted: 18.9.2024.

# SADRŽAJ

# 1. UVOD

Digitalno doba donosi brojne promjene u načinu komunikacije, kulturi, poslovanju, ljudskim pravima i demokraciji. Računalni sustavi postali su temelj modernog života, poboljšavajući produktivnost i efikasnost u različitim sektorima. No, istovremeno, uporaba računalnih sustava otvara vrata i za kriminalne radnje.

Računalna forenzika (engl. *Computer Forensics)* predstavlja ključnu disciplinu unutar forenzičkih znanosti, fokusiranju na prikupljanje, analizu i prezentaciju digitalnih dokaza u kontekstu pravnih postupaka. S obzirom na sve veću prisutnost digitalnih tehnologija u svakodnevnom životu i poslovanju, važnost računalne forenzike kontinuirano raste. Ova disciplina omogućuje stručnjacima da istraže i interpretiraju digitalne tragove, što je od presudne važnosti za rješavanje kriminalnih aktivnosti, zaštitu podataka i osiguravanje pravde.

Važnost računalne forenzike također se ogleda u njenoj sposobnosti da odgovori na izazove kibernetičkog kriminala, koji uključuje širok spektar aktivnosti poput hakiranja, krađe identiteta, prijevara i distribucije zlonamjernog softvera. S obzirom na sve veću sofisticiranost kibernetičkih prijetnji, računalna forenzika postaje neophodan alat za zaštitu kritične infrastrukture, poslovnih sustava i osobnih podataka.

Ciljevi ovog rada obuhvaćaju nekoliko ključnih područja istraživanja u računalnoj forenzici. Prvi cilj je detaljno analizirati različite metodologije koje se koriste u računalnoj forenzici, s posebnim naglaskom na njihove specifične karakteristike i kontekstualnu primjenjivost. Drugi cilj usmjeren je na identifikaciju i evaluaciju softverskih i hardverskih alata koji se primjenjuju u analizi digitalnih dokaza, pri čemu se ocjenjuju njihova učinkovitost, pouzdanost i praktičnost. Treći cilj je ilustrirati praktičnu primjenu teorijskih znanja kroz pregled stvarnih slučajeva u kojima je računalna forenzika bila ključna za rješavanje zločina. Konačno, četvrti cilj je istražiti suvremene izazove s kojima se suočavaju stručnjaci za računalnu forenziku te ponuditi predviđanja budućih trendova i razvoja u ovom području.

Odabir teme računalne forenzike, s fokusom na metodologije, alate i primjenu u analizi digitalnih dokaza, proizlazi iz sve veće važnosti i kompleksnosti digitalnih dokaza u suvremenom pravosudnom sustavu. U digitalnom dobu, kriminalne aktivnosti često uključuju upotrebu tehnologije, što zahtijeva specijalizirane metode za prikupljanje, analizu i prezentaciju digitalnih dokaza. Nadalje, razumijevanje različitih metodologija i alata koji se koriste u računalnoj forenzici, te analiza njihove učinkovitosti, pouzdanosti i praktičnosti, može značajno unaprijediti praksu u ovoj oblasti. Istraživanje stvarnih slučajeva u kojima je računalna forenzika igrala ključnu ulogu pruža vrijedne uvide u praktičnu primjenu teorijskih znanja i

metoda (Nacionalni CERT i LS&S, 2010).

Ostatak rada organiziran je na sljedeći način. U Poglavlju 2 prikazan je pregled povijesti i razvoja računalne forenzike kroz desetljeća, s posebnim naglaskom na razvoj alata i standardizaciju. Poglavlje 3 uvodi osnovne principe i metodologije forenzičke analize te daje pregled alata i tehnika koji se koriste u računalnoj forenzici, uključujući pravna i etička pitanja. Različite vrste računalne forenzike, kao što su forenzika tvrdih diskova, mrežna forenzika, forenzika mobilnih uređaja, cloud forenzika, i druge, detaljno su opisane u Poglavlju 4. U Poglavlju 5 analiziraju se stvarni slučajevi primjene računalne forenzike, čime se ilustrira praktična primjena teorijskih znanja i metoda. Izazovi s kojima se suočavaju stručnjaci za računalnu forenziku, kao i budući trendovi u ovom području, istraženi su u Poglavlju 6. Poglavlje 7 donosi praktičan primjer forenzičke analize pomoću alata *Autopsy*. Konačno, zaključak rada dan je u Poglavlju 8, gdje su sažeti glavni nalazi i refleksije o značaju ove discipline.

# 2. Povijest i razvoj računalne forenzike

Povijest i razvoj računalne forenzike svjedoče o dinamičnom razvoju ove discipline, koju obilježava niz tehnoloških i metodoloških inovacija. Kao odgovor na sve složenije izazove digitalnog doba, računalna forenzika se razvijala iz jednostavnih početaka u 1970-ima, kada su zabilježeni prvi slučajevi računalnih prijevara i hakiranja, do današnjih sofisticiranih tehnika i alata za analizu digitalnih dokaza. Ovaj razvojni put može se podijeliti u nekoliko ključnih faza, od kojih svaka odražava promjene u tehnologiji, zakonodavstvu i društvenim potrebama, čime je oblikovana suvremena praksa računalne forenzike. U nastavku se prikazuje detaljan pregled povijesnog razvoja računalne forenzike kroz desetljeća, s naglaskom na ključne događaje i inovacije koje su utjecale na evoluciju ove discipline.

## 2.1. Pregled povijesti i razvoja računalne forenzike kroz desetljeća

Računalna forenzika razvijala se kroz nekoliko desetljeća, reflektirajući dinamične promjene u tehnologiji, zakonodavstvu i društvenim potrebama. Počeci računalne forenzike datiraju iz kasnih 1970-ih i ranih 1980-ih, kada su se pojavili prvi dokumentirani slučajevi računalnih prijevara, hakiranja i neovlaštenog pristupa podacima. U tom razdoblju, kako su računala postala sastavni dio poslovanja i svakodnevnog života, pojavila se potreba za specijaliziranim metodama prikupljanja, analize i očuvanja digitalnih dokaza. Rani pokušaji forenzičke analize bili su često *ad hoc* i nedovoljno standardizirani, ali su postavili temelje za budući razvoj ove discipline.

U 1990-ima, razvoj interneta donosi novu eru ekspanzije računalne forenzike. Pojavljuju se specijalizirani alati i tehnike za analizu mrežnih aktivnosti, digitalnih tragova i elektroničke pošte (engl. *e-mail*), omogućujući detaljnije i sustavnije istrage digitalnih dokaza. Istovremeno, pojavljuju se prvi standardi i smjernice za provođenje računalne forenzike, poput onih koje je razvila američka FBI jedinica za računalni kriminal. Ova dekada obilježena je formalizacijom računalne forenzike i njenom sve češćom primjenom u pravnim i sigurnosnim kontekstima, od čega su mnoge metode i prakse danas standard.

Tijekom 2000-ih, računalna forenzika se sve više integrira u šire područje kibernetičke sigurnosti. Napredni alati za analizu složenih mrežnih napada, zlonamjernog softvera i drugih digitalnih prijetnji omogućuju stručnjacima da učinkovito istražuju i interpretiraju digitalne tragove. U ovom razdoblju dolazi do većeg korištenja forenzičkih metoda u korporativnim okruženjima za zaštitu osjetljivih podataka i upravljanje sigurnosnim incidentima. Također,

dolazi do daljnje profesionalizacije ovog područja, kroz uvođenje specijaliziranih certifikacija i obrazovnih programa koji standardiziraju znanja i vještine potrebne u računalnoj forenzici.

U 2010-ima, uz ekspanziju pametnih telefona i tehnologije računarstva u oblaku (engl. *cloud computing*), računalna forenzika prilagođava se novim izazovima. Razvijaju se specijalizirani alati za analizu podataka s mobilnih uređaja i oblaka, dok se stručnjaci suočavaju s problemima poput šifriranja i zaštite privatnosti. Upravljanje sve većim količinama podataka postaje ključno, kao i sposobnost integracije različitih izvora podataka u cjelovitu forenzičku analizu. Ovo razdoblje također donosi sve veće povezivanje računalne forenzike s drugim disciplinama unutar digitalne forenzike.

Razdoblje 2020-ih obilježeno je korištenjem naprednih tehnologija kao što su umjetna inteligencija (engl. *Artificial Intelligence, AI)*, strojno učenje (engl. *machine learning*) i automatizacija, što omogućuje analizu velikih količina podataka s većom brzinom i preciznošću. Ove tehnologije igraju ključnu ulogu u brzom otkrivanju, analizi i interpretaciji digitalnih dokaza, čime računalna forenzika postaje neizostavan alat u borbi protiv kibernetičkog kriminala i zaštiti kritične infrastrukture. Uvođenje interdisciplinarnih pristupa u analizu i upravljanje rizicima dodatno osnažuje poziciju računalne forenzike kao ključnog elementa u modernim sigurnosnim strategijama.

Ovaj evolucijski put računalne forenzike, kroz desetljeća tehnološkog napretka i rastuće kompleksnosti digitalnih prijetnji, pokazuje kako se disciplina razvijala da bi odgovorila na nove izazove i potrebe digitalnog doba (DataNumen, 2023),

Kako bi se bolje razumjela evolucija računalne forenzike i ključni trenuci koji su oblikovali ovu disciplinu, važno je razmotriti konkretne slučajeve računalnog kriminala i hakerskih napada koji su obilježili njezin razvoj. Tablica 1 prikazuje neke od najvažnijih incidenata koji su potaknuli tehnološke inovacije, uvođenje standardiziranih metoda i zakonskih okvira te unaprjeđenje praksi u računalnoj forenzici. Prikazani primjeri obuhvaćaju razdoblje od ranih dana računalnih prijevara i hakiranja do suvremenih napada koji koriste napredne tehnologije, pružajući uvid u to kako su se odgovori na digitalne prijetnje razvijali i prilagođavali kroz desetljeća.

*Tablica 1.* Ključni incidenti razvoj računalne forenzike poredani kronološki

| Godina | Počinitelj | Aktivnosti | Posljedice |
|---|---|---|---|
| 1981. | Ian Murphy (Captain Zap) | Neovlašteno pristupio u *American Telephone and Telegraph* (AT&T) sustav i promijenio unutarnji sat računalima, omogućujući korisnicima korištenje jeftinijih noćnih tarifa tijekom dana. | Postao prvi haker procesuiran za računalni kriminal. Ovaj slučaj je istaknuo potrebu za zakonskim okvirom za računalni kriminal i postavio presedan za buduće slučajeve. |
| 1986. | Clifford Stoll | Otkrio je hakersku aktivnost unutar mreže *Lawrence Berkeley National Laboratory* i pratio je do mreže sovjetskih hakera koji su provaljivali u računalne sustave radi špijunaže. | Stollova istraga je dokumentirana u knjizi "*The Cuckoo's Egg*". Ovaj slučaj pokazao je važnost mrežnog praćenja i analize dnevničkih zapisnika (engl. *log*) u otkrivanju i sprječavanju računalnog kriminala. |
| 1988. | Robert Tappan Morris | Stvorio je i pustio *Morris Worm*, prvi poznati računalni crv koji je zarazio internetske mreže 1988. godine | Crv je zarazio 10% računala na Internetu, uzrokujući mrežno zagušenje i velike financijske štete, što je dovelo do osnivanja prvih *Computer Emergency Response Team* (CERT) timova za organizirani odgovor na računalne incidente. |
| 1995. | Kevin Mitnick | Neovlašteno je pristupio mrežama velikih korporacija kao što su Nokia, Motorola i Fujitsu te je ukrao osjetljive podatke i softver. | Uhićen i optužen za višestruka hakiranja. Suđenje je istaknulo važnost računalne forenzike u pravosudnom sustavu i postavilo temelje za strože zakone protiv kibernetičkog kriminala. |
| 2020. | APT29 ili „Cozy Bear“ (hakerska skupina) | Napadači su uspjeli ubaciti zlonamjerni kôd (engl. *malware*) u ažuriranje softvera SolarWinds Orion, koji je zatim distribuiran korisnicima širom svijeta. | Napad je pogodio oko 18.000 organizacija, uključujući vladine agencije i tehnološke tvrtke, ističući potrebu za boljim sigurnosnim praksama u razvoju softvera i upravljanju opskrbnim lancem. |

*Izvor:* izrada autora

### 2.2. Razvoj forenzičkih alata

Razvoj alata za računalnu forenziku započeo je krajem 20. stoljeća kao odgovor na rastuću potrebu za učinkovitijim metodama prikupljanja, analize i očuvanja digitalnih dokaza. Prvi alati bili su jednostavni, često se oslanjajući na ručne metode analize, no s razvojem tehnologije i povećanjem složenosti digitalnih prijetnji, alati su postali sofisticiraniji i automatiziraniji. Kako

bi se osigurala dosljednost i pouzdanost u forenzičkim postupcima, pojavila se i potreba za standardizacijom alata i metoda. U nastavku ćemo predstaviti neke od najvažnijih alata koji se koriste u računalnoj forenzici, kao i standarde koji reguliraju njihovu upotrebu.

Razvoj alata i platformi za digitalnu forenziku prošao je kroz nekoliko ključnih faza, svaka obilježena napretkom u tehnologiji i sve složenijim potrebama za analizom digitalnih dokaza. Na samom početku, u ranim 1980-im i 1990-im godinama, računalna forenzika bila je fragmentirana disciplina s vrlo malo specijaliziranih alata. Većina alata bila je razvijena za specifične slučajeve i često su bili primitivni, oslanjajući se na osnovne metode prikupljanja i analize podataka.

S razvojem računalnih tehnologija i širenjem Interneta u 1990-ima, pojavila se potreba za robusnijim i sofisticiranijim alatima koji bi omogućili sveobuhvatnu analizu digitalnih dokaza. Tada su se počeli razvijati prvi komercijalni alati za forenzičku analizu, koji su omogućavali standardizirane postupke i metode analize, kao što su analiza datotečnih sustava, obnova izbrisanih podataka i analiza mrežnog prometa. Ti su alati postali temelj digitalne forenzike, omogućujući istražiteljima da primijene iste tehnike i procedure u različitim vrstama istraga.

U ranom 21. stoljeću dolazi do daljnje profesionalizacije područja digitalne forenzike. Razvijaju se specijalizirane platforme i alati otvorenog kôda koji su dostupni široj zajednici stručnjaka. Otvoreni kôd omogućio je forenzičarima da prilagode alate specifičnim potrebama svojih istraga i doprinesu njihovom kontinuiranom razvoju. Tako su platforme otvorenog kôda postale ključne za ubrzanje inovacija u ovom području, pružajući fleksibilnost i prilagodljivost koju komercijalni alati ponekad nisu mogli osigurati. Korištenje kombinacije komercijalnih i otvorenih alata omogućilo je istražiteljima sveobuhvatniji pristup analizi digitalnih dokaza.

### 2.3. Ključni standardi i smjernice za rukovanje digitalnim dokazima

Analiza i prikupljanje digitalnih dokaza predstavlja ključne aspekte pravnih i sigurnosnih istraga. Povijesno gledana, razvoj standarda i procedura u ovom području bio je od presudne važnosti za osiguravanje integriteta, pouzdanosti i prihvatljivosti digitalnih dokaza na sudu.

Jedan od najvažnijih standarda u ovom kontekstu je *ISO/IEC 27037*, koji pruža smjernice za identifikaciju, prikupljanje, akviziciju i očuvanje digitalnih dokaza,. Ovaj standard je ključan jer osigurava da su dokazi prikupljeni na način koji omogućava njihovu prihvatljivost na sudu. Prije uvođenja ovakvih standarda, postojala je značajna nesigurnost oko toga kako pravilno rukovati digitalnim dokazima, što je često dovodilo do njihovog odbacivanja u pravnim postupcima.

Nacionalni institut za standarde i tehnologiju (engl. *National Institute of Standards and* Technology, *NITS)* izdao je vodič *SP 800-86*, koji detaljno opisuje proces digitalne forenzike, uključujući prikupljanje, analizu i izvještavanje o digitalnim dokazima. Ovaj vodič je povijesno značajan jer je pružio sveobuhvatan okvir za digitalnu forenziku, omogućujući istražiteljima da sustavno i dosljedno pristupaju analizi digitalnih dokaza. Prije uvođenja ovakvih vodiča, pristupi digitalnoj forenzici bili su fragmentirani i često neadekvatni za potrebe pravnih postupaka.

Smjernice udruženja šefova policije (engl. *Association of Chief Police Officers, ACPO*) iz Ujedinjenog Kraljevstva također su od velike povijesne važnosti. Ove smjernice pružaju detaljne upute za rukovanje digitalnim dokazima, uključujući pravila za očuvanje integriteta dokaza. ACPO smjernice su postale *de facto* standard u mnogim zemljama, osiguravajući da su digitalni dokazi prikupljeni i analizirani na način koji je prihvatljiv na sudu. Prije uvođenja ovih smjernica, postojala je značajna raznolikost u pristupu različitih policijskih snaga prema digitalnim dokazima, što je često rezultiralo gubitkom ili kompromitiranjem dokaza.

Koncept lanca čuvanja (engl. *chain of custody*) također je ključan za povijest i razvoj digitalne forenzike. Ovaj koncept osigurava da svaki korak u rukovanju dokazima bude dokumentiran, čime se osigurava da dokazi nisu kompromitirani. Povijesno gledana, nedostatak adekvatne dokumentacije o rukovanju dokazima često je dovodio do njihovog odbacivanja na sudu. Uvođenjem koncepta lanca čuvanja dokaza, osigurano je da su digitalni dokazi pouzdani i prihvatljivi u pravnim postupcima.

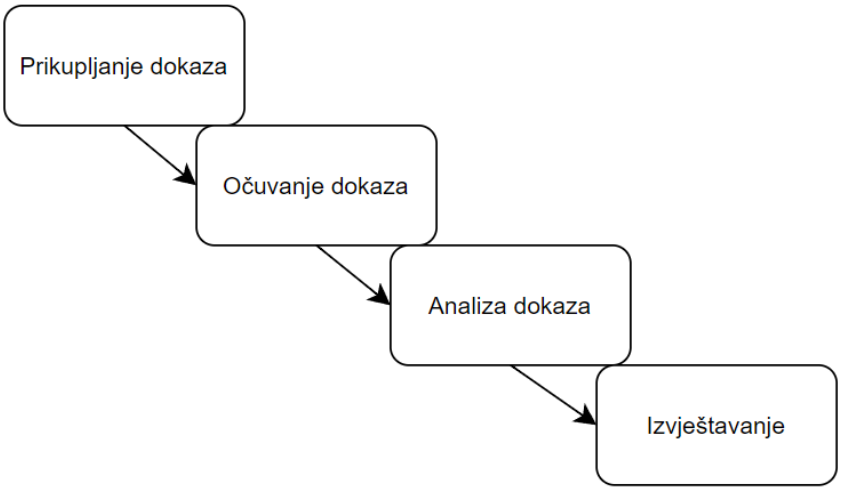
Razvoj ovih standarda i procedura bio je ključan za osiguravanje integriteta, pouzdanosti i prihvatljivosti digitalnih dokaza na sudu. Oni su omogućili istražiteljima da sustavno i dosljedno pristupaju analizi digitalnih dokaza, osiguravajući da su svi relevantni podatci identificirani, sačuvani i pravilno prezentirani u pravnim postupcima. Ovi standardi i procedure također su pomogli u izgradnji povjerenja u digitalne dokaze, omogućujući njihovu sve širu upotrebu u pravim i sigurnosnim istragama (Kent, Chevalier, Grance, & Dang, 2006; ISO/IEC, 2012).

# 3. Metodologije i alati u računalnoj forenzici

Razvoj metodologija i alata u računalnoj forenzici ključan je za omogućavanje sustavnog i dosljednog pristupa analizi digitalnih dokaza, čime se osigurava njihova prihvatljivost u pravnim postupcima. Standardizirani postupci prikupljanja, očuvanja, analize i izvještavanja jamče integritet, pouzdanost i točnost dokaza, dok specijalizirani alati omogućuju forenzičarima rekonstruiranje digitalnih tragova, oporavak izbrisanih podataka i detaljnu analizu složenih digitalnih struktura. Osim tehničke preciznosti, transparentno dokumentiranje svakog koraka osigurava vjerodostojnost dokaza pred sudom i omogućuje usporedivost rezultata među različitim istragama.

## 3.1. Osnovi principi i metodologije forenzičke analize

Digitalna forenzika temelji se na strukturiranom i metodološkom pristupu kako bi se osiguralo pravilno rukovanje i analiza digitalnih dokaza. Proces forenzičke analize sastoji se od nekoliko ključnih koraka, od prikupljanja dokaza pa sve do finalnog izvještavanja. Svaki korak u tom procesu igra kritičnu ulogu u očuvanju integriteta dokaza i osiguravanju pouzdanih rezultata koji se mogu koristiti u pravnim postupcima. Slika 1 prikazuje osnovne korake koji su ključni u digitalnoj forenzici: prikupljanje dokaza, očuvanje dokaza, analiza dokaza i izvještavanje. Ovaj strukturirani pristup omogućuje forenzičkim stručnjacima da identificiraju i dokumentiraju relevantne tragove, osiguravajući da nijedan dokaz ne bude ugrožen. U nastavku su detaljno objašnjeni svaki od ovih koraka, uključujući njihovu važnost i tehničke aspekte koji doprinose uspješnosti forenzičke istrage.




Slika 1. Proces Digitalne forenzike, izvor: Izrada autora

Prikupljanje dokaza predstavlja prvi korak u forenzičkoj analizi, gdje se digitalni dokazi prikupljaju s različitih uređaja i platformi. Ovaj proces mora biti izveden na način koji osigurava integritet dokaza, kako bi se spriječila bilo kakva izmjena ili oštećenje. Forenzički stručnjaci koriste specijalizirane alate za izradu točnih kopija podataka, poznatih kao forenzičke kopije, kako bi se originalni podaci sačuvali netaknuti. Ovaj pristup omogućuje daljnju analizu bez rizika za originalne dokaze.

Nakon prikupljanja, slijedi očuvanje dokaza, što je ključni korak u osiguravanju da dokazi ostanu nepromijenjeni i neoštećeni. To se postiže dokumentiranjem lanca čuvanja, koji bilježi svaki korak u rukovanju dokazima. Ovakav pristup jamči transparentnost i provjerljivost svih radnji s dokazima te osigurava pouzdanost dokaza kroz cijeli istražni proces.

Nakon očuvanja dokaza, dolazi analiza, gdje se prikupljeni podaci pregledavaju i interpretiraju s ciljem identificiranja relevantnih tragova. Analiza može uključivati obnovu izbrisanih podataka, analizu metapodataka te rekonstrukciju digitalnih tragova. Forenzički stručnjaci pritom koriste različite alate i tehnike, uključujući specijalizirani softver koji omogućuje detaljnu analizu podataka. Prednost ovih alata je njihova sposobnost da brzo i učinkovito identificiraju ključne informacije, prilagođavajući se različitim vrstama podataka i uređaja.

Na kraju, izvještavanje predstavlja završni korak u procesu forenzičke analize. Pripremaju se detaljni izvještaji koji jasno i sažeto objašnjavaju nalaze istrage. Ovi izvještaji moraju biti tehnički točni i razumljivi, kako bi se mogli koristiti u pravnim postupcima. Sadrže sve relevantne informacije o prikupljanju, očuvanju i analizi dokaza, kao i zaključke izvedene iz analize. Ovaj strukturirani pristup osigurava da se pružaju jasne i precizne informacije, što je ključno za pravne postupke (Johansen, 2017).

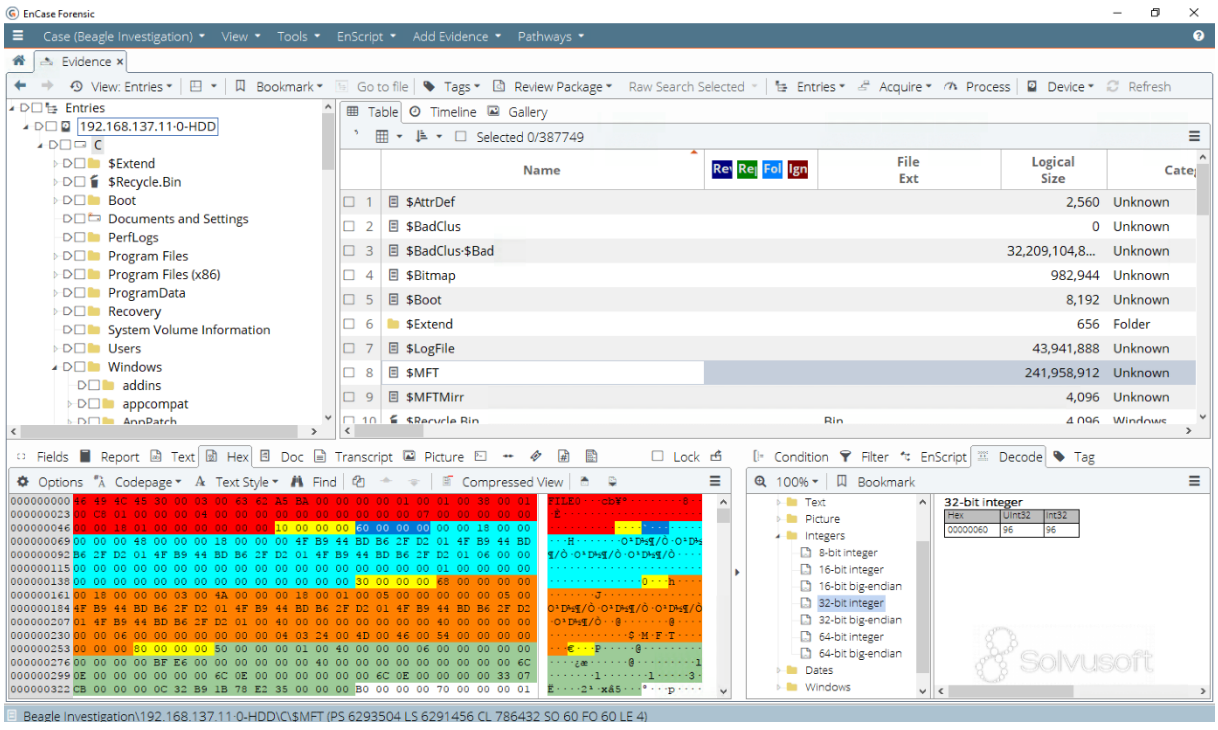
### 3.2. Pregled alata i platformi koji se koriste u računalnoj forenzici

U računalnoj forenzici, alati i platforme igraju ključnu ulogu u osiguravanju točnosti, pouzdanosti i prihvatljivosti digitalnih dokaza u pravnim postupcima. Razvoj forenzičkih alata tijekom godina bio je potaknut potrebom za preciznim metodama prikupljanja, očuvanja, analize i izvještavanja o digitalnim dokazima. U nastavku opisani su ključni alati i standardi koji su oblikovali praksu računalne forenzike, uključujući popularne softverske alate poput *EnCase, Sleuth Kit* i *Autopsy,* kao i integrirane platforme poput *Computer Aided Investigative Environment* (CAINE) i *SANS Investigative Forensic Toolkit* (SIFT) *Workstation*.

### 3.2.1. EnCase

Alat *EnCase* je prvi put predstavljen krajem 1990-ih godina kao odgovor na rastuću potrebu za alatima koji mogu učinkovito analizirati digitalne dokaze. Razvijen je od strane *Guidance Software*, a sada je u vlasništvu tvrtke *Open Text*. *EnCase* je jedan od prvih alata koji su omogućili sveobuhvatnu analizu dokaza. Prije njegova razvoja, digitalna forenzika je bila fragmentirane i nedovoljno standardizirana. Jedan od najvažnijih aspekata *EnCase-a* je njegovo priznanje u pravnim sustavim diljem svijeta. Njegova upotreba u sudskim postupcima osigurala je da digitalni dokazi budu posvećeni i pouzdani.

Slika 2 prikazuje sučelje *EnCase* alata, koje istražiteljima omogućuje detaljan pregled strukture datoteka, identifikaciju ključnih informacija i analizu digitalnih tragova. Ove funkcionalnosti značajno doprinose prikupljanju i interpretaciji digitalnih dokaza u forenzičkim istragama. Prikazani hijerarhijski pregled datoteka i mapa s deskriptivnim oznakama pomaže forenzičarima u navigaciji kroz potencijalno velike količine podataka, brzo prepoznavanje relevantnih dokaza i izdvajanje ključnih informacija. Funkcionalnosti poput kartica *Table*, *Timeline*, i *Cluster Map* omogućuju detaljniju analizu vremenskih tokova aktivnosti i vizualizaciju podataka na niskoj razini, što je posebno korisno za identifikaciju anomalija i uzoraka koji mogu ukazivati na prisutnost zlonamjernih aktivnosti. Ovakav pregled značajno unapređuje učinkovitost i točnost forenzičkih analiza u složenim istragama računalnog kriminala.




Slika 2. EnCase softver, izvor: (Open Text, 2021)

Uz pomoć ovog alata (Slika 2), istražitelji mogu rekonstruirati izbrisane datoteke, analizirati metapodatke i pregledavati podatke na niskoj razini, kao što su heksadecimalni i binarni prikazi, kako bi precizno identificirali promjene i anomalije u podacima. Ove mogućnosti omogućuju detaljnu analizu digitalnih tragova, što je ključno za razumijevanje tijeka događaja i prikupljanje valjanih dokaza koji mogu biti korišteni u pravnim postupcima (Open Text, 2021).

### 3.2.2. Sleuth Kit

*Sleuth Kit* je važan alat otvorenog kôda (engl. *open source*) u području računalne forenzike, razvijen za naprednu analizu datotečnih sustava i digitalnih dokaza. Razvoj ovog alata započeo je krajem 1990-ih godina pod vodstvom Briana Carriera, a tijekom godina postao je nezamjenjiv za mnoge digitalne forenzičare. *Sleuth Kit* je poznat po svojoj sposobnosti rada na više platformi, kao što su Windows, Linux i macOS, te po podršci za razne datotečne sustave, uključujući NTFS, FAT, EXT, HFS+ i druge.

Njegove ključne značajke uključuju mogućnost pretraživanja, pregleda i analize struktura datoteka, metapodataka i izbrisanih podataka, što je ključno za otkrivanje skrivenih ili zlonamjernih aktivnosti. Kao alat otvorenog kôda, *Sleuth Kit* omogućuje široku pristupačnost i prilagodljivost, što ga čini popularnim među istražiteljima i analitičarima koji ga mogu prilagoditi specifičnim potrebama svojih istraga. Često se koristi u kombinaciji s grafičkim sučeljem *Autopsy*, koje olakšava vizualizaciju i analizu složenih podataka.

Zahvaljujući svojoj prilagodljivosti i raznovrsnim funkcionalnostima, *Sleuth Kit* je postao široko korišten u akademskim, komercijalnim i pravosudnim okruženjima, gdje je prepoznat kao pouzdan alat za digitalnu forenziku (The Sleuth Kit, 2024).

### 3.2.3. Autopsy

*Autopsy* je predstavljen početkom 2000-ih godina kao besplatni alat otvorenog kôda za digitalnu forenziku, kojeg je razvio Brian Carrier. Ovaj alat služi kao grafičko sučelje (engl. *Graphical User Interface*) za *Sleuth Kit*, omogućujući korisnicima jednostavniji pristup snažnim forenzičkim funkcionalnostima za analizu digitalnih dokaza. *Autopsy* istražiteljima omogućuje pregled datoteka, povijesti pregledavanja, e-pošte i drugih podataka na računalima i mobilnim uređajima. Kao alat otvorenog kôda, besplatan je za korištenje i prilagodljiv specifičnim potrebama korisnika, što ga čini izuzetno pristupačnim i fleksibilnim, posebno za manje organizacije i agencije koje možda nemaju pristup skupljim komercijalnim alatima.

*Autopsy* je također priznat u pravnim sustavima diljem svijeta, jer njegova upotreba u sudskim postupcima osigurava da digitalni dokazi budu pouzdani i prihvaćeni. Njegova popularnost raste i zbog aktivne zajednice korisnika i programera koji kontinuirano doprinose razvoju i poboljšanju alata, integrirajući nove tehnologije i metode. S obzirom na svoju prilagodljivost i mogućnost integracije s drugim forenzičkim alatima, *Autopsy* je postao nezamjenjiv alat za mnoge digitalne forenzičare (Libby, 2023), (Kävrestad, Birath, & Clarke, 2024).

### 3.2.4. Computer Aided Investigative Environment (CAINE)

Platforma otvorenog kôda za digitalnu forenziku CAINE razvijena je kao *GNU/Linux* distribucija. Projekt je započeo 2008. godine pod vodstvom Giovannija Bassettija, s ciljem stvaranja sveobuhvatnog okruženja za digitalne istrage. CAINE se ističe svojom fleksibilnošću i nizom integriranih forenzičkih alata koji ga čine vrijednim resursom za istražitelje diljem svijeta. Ključni razlozi njegove povijesne važnosti uključuju (Lehr, n.d.), (Giustini, 2008):

- *Integracija Forenzičkih alata* – distribucija CAINE je dizajnirana kao sveobuhvatno okruženje koje integrira niz forenzičkih alata u jednu platformu. Ova integracija je omogućila forenzičarima korištenje različitih alata bez potrebe za prebacivanje između različitih sustava, čime se povećava učinkovitost i preciznost istraga. Time je CAINE postavio nove standarde u praksi digitalne forenzike.
- *Live Distribucija* – platforma CAINE se može pokrenuti s USB *flash* memorije ili optičkog diska bez potrebe za instalacijom na tvrdi disk (engl. *hard disk drive, HDD*). Ova značajka omogućuje forenzičarima analizu podataka bez promjene originalnog sustava, čime se osigurava integritet dokaza.
- *Podrška za Različite platforme* – platforma CAINE podržava analizu podataka s različitih operacijskih sustava, uključujući Windows, Linux te pojedine Unix sustave. Ova široka primjenjivost omogućuje forenzičarima analizu širokog spektra digitalnih dokaza, čime se povećava njihova sposobnost rješavanja složenih digitalnih istraga.

### 3.2.5. Sift Worskation

*SIFT Workstation* je sveobuhvatna platforma otvorenog kôda za digitalnu forenziku i odgovor na incidente, koju je razvio SANS Institute pod vodstvom Roba Leeja. Alat je osmišljen kao besplatno, ali moćno rješenje koje omogućuje forenzičarima diljem svijeta provođenje naprednih analiza i istraga digitalnih dokaza. SIFT Workstation podržava širok

spektar forenzičkih alata i tehnika, uključujući analizu datotečnih sustava, pretragu i analizu memorije, mrežnu forenziku te analizu malicioznog softvera.

Jedna od glavnih prednosti SIFT Workstationa je njegova modularnost, koja omogućava lako dodavanje i prilagodbu različitih forenzičkih alata prema specifičnim potrebama istraga. Fleksibilnost alata omogućava forenzičarima da integriraju nove tehnike i metode kako bi se nosili s novim vrstama prijetnji i napada u digitalnom okruženju. Zahvaljujući redovitom ažuriranju i podršci zajednice, SIFT Workstation ostaje relevantan i pouzdan alat u borbi protiv digitalnog kriminala.

SIFT Workstation također omogućuje forenzičarima analizu podataka s različitih operacijskih sustava (kao što su Windows, Linux i macOS), čime se povećava njihova sposobnost rješavanja složenih digitalnih istraga u različitim okruženjima. Ova platforma je prepoznata kao industrijski standard u edukaciji i obuci forenzičara, što je čini neophodnim alatom za profesionalce u području računalne forenzike i kibernetičke sigurnosti (Lee, n.d.), (Gann, 2023).

### 3.3. Pravna i etička pitanja

Pravna i etička pitanja igraju ključnu ulogu u forenzičkoj analizi. Prikupljanje i analiza digitalnih dokaza moraju biti izvedeni u skladu s pravnim propisima kako bi bili prihvatljivi na sudu. To uključuje poštivanje privatnosti i prava pojedinaca, kao i osiguranje da su svi dokazi prikupljeno zakonito. Osiguranje privatnosti je od iznimne važnosti, te forenzički stručnjaci moraju osigurati da prikupljanje dokaza ne krši prava na privatnost pojedinca. To podrazumijeva pridržavanje zakona o zaštiti podataka i privatnosti, kao što su Opća uredba o zaštiti podataka (engl. *General Data Protection Regulation, GDPR)* u Europskoj uniji. Prednost ovog pristupa leži u zaštiti prava pojedinaca, dok je specifičnost u potrebi za pažljivim balansiranjem između prikupljanja dokaza i poštivanja privatnosti.

Integritet dokaza je ključan za njihovu prihvatljivost na sudu. Svaki korak u rukovanju dokazima mora biti dokumentiran kako bi se spriječila manipulacija ili oštećenje dokaza. To uključuje vođenje lanca čuvanja dokaza, koji osigurava da su svi dokazi pravilno zabilježeni i pohranjeni. Prednost ovog pristupa je u osiguravanju pouzdanosti dokaza, dok je specifičnost u detaljnoj dokumentaciji svih radnji poduzetih s dokazima.

Osim integriteta dokaza, stručnost i kvalifikacije forenzičkih stručnjaka također su od vitalne važnosti. Stručnjaci moraju biti adekvatno obučeni i certificirani kako bi osigurali da njihovi postupci budu u skladu s najboljim praksama i standardima industrije. Na primjer,

certifikati kao što su Certificirani forenzički računalni ispitivač (engl. *Certified Forensic Computer Examiner, CFCE*) i Certificirani stručnjak za sigurnost informacijskih sustava (engl. *Certified Information System Security Professional, CISSP*) osiguravaju da stručnjaci posjeduju potrebna znanja i vještine. Prednost ovog pristupa je osiguranje visokog standarda rada, dok je specifičnost u kontinuiranoj potrebi za edukacijom i certificiranjem stručnjaka.

Zakonski okvir koji reguliraju forenzičku analizu uključuju različite zakone i propise o zaštiti podataka, privatnosti i kaznenom postupku. U Europskoj uniji, Opća uredba GDPR postavlja stroge zahtjeve za prikupljanje, obradu i pohranu osobnih podataka. U Sjedinjenim Američkim Državama, Zakon o privatnosti elektroničkih komunikacija (engl. *Electronic Communications Privacy Act, ECPA*) regulira pristup elektroničkim komunikacijama, dok Zakon o računalnim prijevarama i zlouporabi (engl. *Computer Fraud and Abuse Act, CFAA*) definira pravila o neovlaštenom pristupu računalnim sustavima i podatcima. Ovi zakoni osiguravaju da su svi dokazi prikupljeni zakonito i da se poštuju prava pojedinca, što je ključno za njihovu prihvatljivost u pravnim postupcima.

Ovi principi, metodologije, alati i pravna pitanja čine temelj forenzičke analize, osiguravajući da su digitalni dokazi prikupljeni, očuvani, analizirani i prezentirani na način koji je prihvatljiv na sudu koji podržava pravne timove u njihovim istragama. (European parliament, 2016; PBS, 2024; Minc, 2023; Gallagher, 2024).

# 4. Vrste računalne forenzike

Računalna forenzika je multidisciplinarno područje koje se bavi prikupljanjem, analizom i očuvanjem digitalnih dokaza kako bi se podržale pravne istrage. Zbog sve veće raznolikosti digitalnih uređaja i sustava, razvilo se nekoliko specijaliziranih područja unutar računalne forenzike, od kojih svako ima svoje specifičnosti, alate i metodologije. Ova područja omogućuju forenzičarima da ciljano analiziraju različite vrste digitalnih tragova i dokaza, prilagođavajući svoje pristupe prema vrsti uređaja ili okruženja iz kojeg se prikupljaju dokazi.

U ovom poglavlju istražit ćemo različita područja računalne forenzike, uključujući forenziku tvrdih diskova i pohrane podataka, mrežnu forenziku, forenziku mobilnih uređaja, *cloud* forenziku, forenziku zlonamjernog softvera i forenziku Interneta stvari (engl. *Internet of things, IoT*). Svako od ovih specijaliziranih područja ima svoje karakteristike, izazove i specifične tehnike koje se primjenjuju u analizi digitalnih dokaza. Cilj je pružiti uvid u jedinstvene aspekte svakog područja i razumjeti kako se oni primjenjuju u složenim forenzičkim istragama.

## 4.1. Forenzika tvrdih diskova i pohrane podataka

Forenzika tvrdih diskova i pohrane podataka fokusira se na analizu podataka pohranjenih na fizičkim medijima kao što su tvrdi diskovi, diskovi u čvrstom stanju (engl. *Solid State Drives, SSD*) te razni USB uređaji za pohranu. Ova vrsta forenzike bavi se identifikacijom, očuvanjem, analizom i obnovom podataka koji su pohranjeni ili izbrisani s ovih uređaja, kako bi se podržale pravne istrage ili incidentni odgovori. Analiza se provodi pomoću specijaliziranih alata i tehnika za pretraživanje datotečnih sustava, obnovu izbrisanih datoteka, analizu metapodataka i identifikaciju zlonamjernih aktivnosti.

Forenzika tvrdih diskova uključuje nekoliko ključnih koraka:

1. *Izrada forenzičke kopije* – prvi korak je izrada bit-po-bit kopije tvrdog diska kako bi se očuvali svi podatci, uključujući izbrisane datoteke i slobodan prostor.
2. *Analiza datotečnog sustava* – Analiziraju sve strukture datotečnog sustava. Na primjer *New Technology File System* (NTFS) i *File Allocation Table* (FAT32), kako bi se identificirali i rekonstruirali podaci.
3. *Pretraživanja i obnova podataka* – Koristi se specijalizirani alati za pretraživanje i obnavljanje izbrisanih ili skrivenih datoteka.
4. *Analiza metapodataka* – Pomoću metapodataka prikupljaju se dodatne informacije o

aktivnostima.

Važan koncept u forenzici tvrdih diskova je očuvanje integriteta dokaza, što je od presudne važnosti za njihovu prihvatljivost u pravnim postupcima. Forenzički alati poput *EnCase* i *Autopsy* igraju ključnu ulogu u analizi podataka pohranjenih na tvrdim diskovima, omogućujući istražiteljima izradu forenzičkih kopija, detaljno pretraživanje, identifikaciju i oporavak izbrisanih ili skrivenih datoteka. Pritom, istražitelji moraju osigurati da se svi podaci obrađuju na način koji poštuje zakonske i etičke standarde, kao što je zaštita privatnosti pojedinaca i zakonito rukovanje digitalnim dokazima, čime se osigurava njihova valjanost u sudskim postupcima (Rudeš, 2018).

### 4.2. Mrežna forenzika

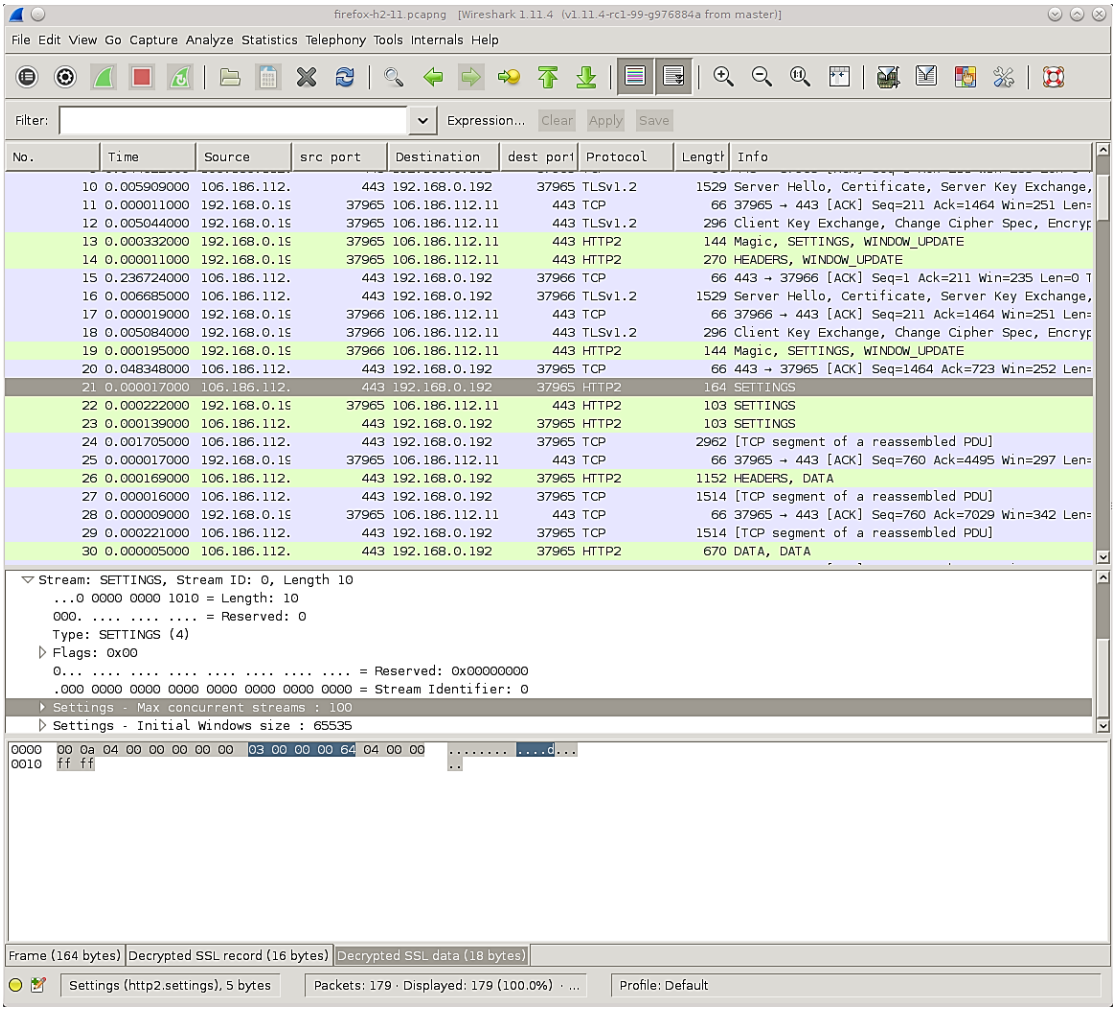
Mrežna forenzika bavi se prikupljanjem i analizom podataka koji se prenose preko mreža, uključujući internetski promet, s ciljem otkrivanja i istraživanja sigurnosnih incidenata. Ovo područje forenzike koristi specijalizirane alate za snimanje mrežnog prometa i analizu paketa podataka kako bi se identificirali sumnjivi događaji, potencijalne prijetnje i sigurnosne anomalije. Neki od popularnih alata u mrežnoj forenzici su *Wireshark*, koji omogućava detaljno snimanje i analizu mrežnog prometa, te *Network Miner*, koji pomaže u ekstrakciji informacija iz prikupljenih mrežnih podataka.

Postupak mrežne forenzike obično započinje prikupljanjem mrežnih podataka, što se postiže snimanjem mrežnog prometa pomoću alata kao što je *Wireshark*, koji omogućava hvatanje paketa podataka i analizu njihovih sadržaja. Nakon prikupljanja, podaci se analiziraju kroz pregled mrežnih zapisa (engl. *log*) i izvješća s mrežnih uređaja kao što su usmjernici i preklopnici, kako bi se identificirali sumnjivi događaji i anomalije. Ova analiza uključuje prepoznavanje uzoraka napada, analizu protokola, korelaciju podataka i praćenje tragova napadača.

Pravna i etička pitanja igraju ključnu ulogu u mrežnoj forenzici, posebice u kontekstu prikupljanja podataka bez pristanka korisnika. Forenzički stručnjaci moraju se pridržavati zakona o privatnosti i nadzoru kako bi osigurali zakonitost postupaka i zaštitili prava pojedinaca. Na primjer, prikupljanje podataka s mreže bez odgovarajuće autorizacije može biti u suprotnosti sa zakonima o privatnosti, kao što su GDPR u Europskoj uniji.

Mrežna forenzika stoga predstavlja izazovan, ali ključan dio digitalnih istraga, omogućujući istražiteljima da detaljno analiziraju mrežne aktivnosti i utvrde potencijalne sigurnosne prijetnje. Stoga, alati za mrežnu analizu poput alata *Wireshark* (Slika 3) postaju

neophodni za prikupljanje i analizu mrežnog prometa, pružajući istražiteljima potrebne uvide za razumijevanje i rekonstrukciju događaja.




Slika 3. Prikaz mrežnog prometa. Izvor: (Stenberg, 2014)

Slika 3 prikazuje sučelje alata *Wireshark*, koji se koristi za prikupljanje, analizu i spremanje mrežnog prometa. Sučelje je podijeljeno u tri dijela:

1. *Gornji dio* – prikazuje popis svih snimljenih paketa. Svaki redak predstavlja jedan paket i sadrži informacije kao što su broj paketa, vrijeme snimanja, izvorišna i odredišna Internet protokol (IP) adresa, korišteni protokol, duljina paketa te dodatne informacije o prijenosu.
2. *Srednji dio* – prikazuje detaljne informacije o trenutno odabranom paketu. Ovdje se mogu vidjeti svi slojevi mrežnog protokola koji su uključeni u prijenos paketa, od fizičkog do aplikacijskom sloja.
3. *Donji dio* – prikazuje sirove podatke odabranog paketa u heksadecimalnom obliku. Ovaj dio omogućuje istražiteljima da vide stvarne bajtove koji čine paket.

Ovakvo detaljno prikazivanje podataka pomaže istražiteljima u rekonstrukciji događaja, što je ključni korak u mrežnoj forenzici. Analizom mrežnih paketa i zapisa, istražitelji mogu rekonstruirati slijed događaja koji su doveli do sigurnosnog incidenta, uključujući identifikaciju izvora napada, načina na koji je napad izveden i njegovih posljedica.

### 4.3. Forenzika mobilnih uređaja

Forenzika mobilnih uređaja fokusira se na prikupljanje i analizu podataka s mobilnih uređaja poput pametnih telefona i tableta. Ova grana forenzike koristi specijalizirani softver za ekstrakciju podataka iz mobilnih uređaja, omogućujući istražiteljima pristup informacijama koje mogu biti ključne za istragu. *Cellebrite* je jedan od alata koji se koristi za ekstrakciju i analizu podataka s mobilnih uređaja, ali i drugi alati poput *Oxygen Forensic* ili *XRY* također su popularni i pružaju dodatne mogućnosti za istražitelje.

Postupak forenzike mobilnih uređaja započinje fizičkom i logičkom ekstrakcijom podataka. Fizička ekstrakcija uključuje kopiranje cijele memorije uređaja, uključujući izbrisane podatke i skrivene particije, omogućujući istražiteljima pristup svim podacima pohranjenim na uređaju, bez obzira na to jesu li trenutno dostupni korisniku. Logička ekstrakcija, s druge strane, obuhvaća samo aktivne podatke koji su vidljivi korisniku, kao što su kontakti, poruke, pozivi i aplikacije.

Nakon ekstrakcije podataka, često je potrebno dešifriranje podataka ako su šifrirani. Mnogi mobilni uređaji koriste napredne metode šifriranja kako bi zaštitili podatke korisnika. Forenzički alati kao što je *Cellebrite* imaju ugrađene funkcije za dešifriranje koje omogućuju istražiteljima pristup šifriranim podacima. Ovaj korak je ključan za osiguranje cjelovitosti i dostupnosti svih relevantnih informacija.

Sljedeći korak u postupku forenzike mobilnih uređaja je analiza podataka iz aplikacija. Mobilne aplikacije često pohranjuju velike količine podataka, uključujući poruke, fotografije, videozapise i podatke o lokaciji. Forenzički alati omogućuju istražiteljima da pregledaju i analiziraju podatke iz aplikacija, identificirajući ključne informacije koje mogu biti relevantne za istragu. Na primjer, analiza aplikacija za razmjenu poruka može otkriti komunikaciju između osumnjičenih osoba, dok analiza aplikacija za društvene mreže može pružiti uvid u aktivnosti i veze korisnika.

Obnova izbrisanih podataka još je jedan važan aspekt forenzike mobilnih uređaja. Iako korisnici mogu izbrisati podatke sa svojih uređaja, ti podaci često ostaju pohranjeni u memoriji uređaja dok se ne prepišu novim podacima. Forenzički alati koriste napredne tehnike za

vraćanje izbrisanih podataka, omogućujući istražiteljima pristup informacijama koje su korisnici pokušali sakriti.

Pravna i etička pitanja u forenzici mobilnih uređaja uključuju osiguravanje zakonitosti pristupa podacima i poštivanje privatnosti korisnika. Prikupljanje i analiza podataka s mobilnih uređaja mora biti u skladu s relevantnim zakonima i propisima, uključujući zakone o zaštiti podataka i privatnosti. Istražitelji moraju osigurati da imaju odgovarajuće ovlasti za pristup podacima i da poštuju prava korisnika na privatnost. Ovo je posebno važno s obzirom na osjetljive informacije koje se često nalaze na mobilnim uređajima, kao što su osobne fotografije, poruke i podaci o lokaciji (Mrkonjić, 2022).

### 4.4. Cloud forenzika

*Cloud* forenzika predstavlja specifično područje digitalne forenzike koje se bavi prikupljanjem, analizom i očuvanjem digitalnih dokaza pohranjenih u oblačnim okruženjima. Ovo područje forenzike suočava se s nizom izazova koji proizlaze iz same prirode oblačnih servisa. U nastavku su detaljno opisani ključni izazovi s kojima se istražitelji susreću u *cloud* forenzici (Sayada Sonia Akter, 2023; Pichan, 2015):

1. *Pristup podacima* – Jedan od najvažnijih izazova u *cloud* forenzici je pristup podacima pohranjenima na udaljenim poslužiteljima. Za razliku od tradicionalne forenzike, gdje istražitelji imaju fizički pristup uređajima, u *cloud* forenzici podaci su pohranjeni na poslužiteljima koji mogu biti geografski udaljeni i pod kontrolom trećih strana. To može otežati prikupljanje podataka, posebno ako pružatelj *cloud* usluga ne surađuje ili ako postoje pravne prepreke za pristup podacima.
2. *Očuvanje integriteta podataka* – Očuvanje integriteta podataka ključno je u forenzičkim istragama. U *cloud* okruženju, podaci se često repliciraju i distribuiraju preko više poslužitelja, što može otežati osiguranje da podaci nisu promijenjeni tijekom prikupljanja. Istražitelji moraju koristiti specijalizirane alate i metode kako bi osigurali da prikupljeni podaci ostanu nepromijenjeni i da se može dokazati njihov integritet.
3. *Pravna i regulatorna pitanja* – Cloud forenzika suočava se s posebnim pravnim izazovima zbog globalne prirode oblačnih poslužitelja. Podaci mogu biti pohranjeni u različitim pravnim nadležnostima, svaka sa svojim zakonima i propisima o zaštiti podataka i privatnosti. Istražitelji moraju biti svjesni tih zakonskih okvira i osigurati da njihovo prikupljanje podataka bude u skladu s relevantnim zakonima. To može uključivati dobivanje sudskih naloga ili drugih pravnih ovlasti za pristup podacima.

4. *Šifriranje podataka* – Mnogi *cloud* servisi koriste napredne metode šifriranja kako bi zaštitili podatke korisnika. Iako je šifriranje ključno za sigurnost podataka, ono također predstavlja izazov za forenzičke istrage. Istražitelji moraju imati alate i metode za dešifriranje kako bi mogli pristupiti relevantnim informacijama. Ovo može uključivati suradnju s pružateljima *cloud* usluga ili korištenje naprednih tehnika dešifriranja.
5. *Dinamičnost i skalabilnost – Cloud* okruženja su dinamična i skalabilna, što znači da se podaci mogu brzo mijenjati i premještati između različitih poslužitelja i lokacija. Ovo može otežati praćenje i prikupljanje podataka, posebno u stvarnom vremenu. Istražitelji moraju koristiti alate koji mogu pratiti ove promjene i osigurati da prikupljeni podaci budu točni i relevantni.
6. *Nedostatak standardizacije* – Postoji nedostatak standardizacije u *cloud* forenzici, što može otežati prikupljanje i analizu podataka. Različiti pružatelji *cloud* usluga koriste različite tehnologije, formate i metode za pohranu podataka, što može otežati interoperabilnost i usporedbu podataka. Istražitelji moraju biti upoznati s različitim tehnologijama i alatima kako bi mogli učinkovito prikupljati podatke iz različitih izvora.
7. *Privatnost i etička pitanja* – Prikupljanje podataka iz oblaka mora biti u skladu s etičkim smjernicama i zakonima o privatnosti. Istražitelji moraju osigurati da imaju odgovarajuće ovlasti za pristup podacima i da poštuju prava korisnika na privatnost. Ovo je posebno važno s obzirom na osjetljive informacije koje se često pohranjuju u oblaku, kao što su osobni podaci, financijske informacije i poslovne tajne.
8. *Suradnja s pružateljem cloud usluga* – Suradnja s pružateljem *cloud* usluga može biti ključna za uspjeh forenzičkih istraga. Pružatelji usluga mogu pružiti tehničku podršku, pristup alatima i podacima te pomoći u dešifriranju podataka. Međutim, ova suradnja može biti izazovna ako pružatelj usluga ne surađuje ili ako postoje pravne prepreke za dijeljenje podataka.

*Cloud* forenzika predstavlja jedno od najizazovnijih područja digitalne forenzike zbog svoje složenosti i specifičnih problema vezanih uz pristup podacima, očuvanje njihovog integriteta, šifriranje, pravna ograničenja te suradnju s pružateljima usluga u oblaku. Istražitelji moraju biti vješti u upotrebi naprednih alata i metoda te biti dobro upućeni u relevantne pravne i etičke smjernice kako bi uspješno proveli istrage u ovim dinamičnim i često nepredvidivim okruženjima. Unatoč brojnim izazovima, učinkovita *cloud* forenzika može pružiti ključne dokaze u složenim istragama, a njezin daljnji razvoj i standardizacija bit će ključni za sigurnost i pravednost u digitalnom dobu.

### 4.5. Forenzika zlonamjerna softvera

Forenzika zlonamjernog softvera predstavlja specifično područje digitalne forenzike koje se bavi analizom i istraživanjem zlonamjernog softvera kako bi se razumjelo njegovo ponašanje, utjecaj i mehanizmi djelovanja. Ovo područje forenzike koristi niz specijaliziranih tehnika i alata za prikupljanje, analizu i očuvanje digitalnih dokaza. U nastavku su opisane ključne metode koje se koriste u forenzici zlonamjernog softvera.

Dinamička analiza uključuje pokretanje zlonamjernog softvera u kontroliranom okruženju kako bi se promatralo njegovo ponašanje. Ova metoda omogućuje istražiteljima da identificiraju promjene koje zlonamjerni softver uzrokuje u sustavu, kao i njegove mrežne aktivnosti. Alat poput *Cuckoo Sandbox* često se koristi za ovu vrstu analize. Postupci uključuju postavljanje izoliranog okruženja (engl. *sandbox*) za pokretanje zlonamjernog softvera, promatranje promjena u sustavu, mrežnog prometa i ponašanja softvera te bilježenje svih aktivnosti koje zlonamjerni softver izvodi.

Statička analiza uključuje ispitivanje zlonamjernog softvera bez njegovog pokretanja, analizom njegovog koda i strukture. Ova metoda omogućuje istražiteljima da identificiraju ključne dijelove kôda, funkcije i algoritme koje zlonamjerni softver koristi. Alat poput *IDA Pro* često se koristi za statičku analizu. Postupci uključuju dekompilaciju (engl. *decompilation*) ili disasembliranje (engl. *disassembly*) zlonamjernog softvera kako bi se dobio uvid u njegov izvorni kod, analizu binarnih datoteka kako bi se identificirali ključni dijelovi kôda te pretraživanje poznatih obrazaca i potpisa zlonamjernog softvera.

Analiza ponašanja fokusira se na razumijevanje kako zlonamjerni softver komunicira s okolinom i koje akcije poduzima. Ova metoda omogućuje istražiteljima da identificiraju mrežne komunikacije, promjene u sustavu i druge aktivnosti koje zlonamjerni softver izvodi. Alat poput *Process Monitor* često se koristi za analizu ponašanja. Postupci uključuju praćenje procesa (engl. *processes*) i dretve (engl. *threads*) koje zlonamjerni softver pokreće, analizu mrežnog prometa kako bi se identificirale komunikacije s komandnim i kontrolnim poslužiteljima te bilježenje promjena u sustavu.

Reverzno inženjerstvo (engl. *reverse engineering*) je mnogo dublji i sveobuhvatniji pristup koji uključuje analizu unutarnjih mehanizama zlonamjernog softvera na niskoj razini. Ono omogućuje istražiteljima da dekompiliraju ili disasembliraju softver kako bi proučili njegov izvorni kôd, algoritme, i logiku. Cilj je razumjeti kako zlonamjerni softver funkcionira, identificirati korištene tehnike šifriranja ili prikrivanja, i stvoriti potpise za buduću detekciju. Reverzno inženjerstvo zahtijeva napredne tehničke vještine i korištenje specijaliziranih alata te

je često ključan korak u razumijevanju sofisticiranih zlonamjernih prijetnji.

Pravna i etička pitanja u forenzici zlonamjernog softvera ključna su za osiguranje zakonitosti forenzičkih istraga. Istražitelji moraju osigurati da njihova analiza bude u skladu s relevantnim zakonima i propisima te da imaju odgovarajuće dozvole i ovlasti za analizu zlonamjernog softvera. Također, analiza mora poštivati prava intelektualnog vlasništva, posebno ako je softver zaštićen autorskim pravima. Istražitelji moraju osigurati da njihova analiza ne krši prava intelektualnog vlasništva te da poštuju etičke smjernice i standarde u analizi zlonamjernog softvera (Microsoft, 2024; Shakeel, 2019).

### 4.6. Forenzika Interneta stvari

Forenzika Interneta stvari usredotočuje se na prikupljanje i analizu podataka s različitih uređaja koji se povezuju i razmjenjuju informacije preko mreže. Ova grana digitalne forenzike suočava se s jedinstvenim izazovima zbog raznolikosti IoT uređaja, njihovih specifičnih protokola i različitih tehnologija koje koriste. IoT uređaji uključuju sve, od pametnih kućanskih uređaja do industrijskih senzora, što forenzičku analizu čini složenom i zahtijeva prilagodljive metode.

Specifični izazovi IoT forenzike uključuju:

- *Raznolikost uređaja i protokola* – IoT uređaji koriste različite komunikacijske protokole i tehnologije, što otežava standardizaciju procesa forenzike. Prikupljanje podataka može uključivati rad sa senzorima, pristup ugrađenim sustavima i analizu specifičnih mrežnih protokola.
- *Ograničeni resursi uređaja* – Mnogi IoT uređaji imaju ograničene procesorske resurse i pohranu, što može otežati prikupljanje i analizu podataka bez kompromitiranja funkcionalnosti uređaja.

Alati i tehnike koje se koriste u IoT forenzici uključuju softvere poput *IoT Inspector*, koji omogućuje analizu podataka s različitih IoT uređaja. Postupci forenzike obuhvaćaju prikupljanje podataka iz različitih senzora, analizu mrežnog prometa i rekonstrukciju događaja kako bi se identificirali potencijalni sigurnosni propusti ili prijetnje. Zbog raznolikosti uređaja i okruženja, istražitelji često moraju koristiti prilagodljive i specijalizirane alate za prikupljanje podataka u realnom vremenu.

Prednosti IoT forenzike odnose se na mogućnost prikupljanja detaljnih podataka iz različitih izvora, što može značajno ubrzati istrage i povećati njihovu točnost. S druge strane,

mane ove grane forenzike uključuju složenost analize koja proizlazi iz raznolikosti uređaja i protokola, kao i izazove povezane s očuvanjem integriteta podataka. Uz to, često se pojavljuju i potencijalni problemi s privatnošću i zaštitom podataka.

Pravna i etička pitanja u IoT forenzici igraju ključnu ulogu u osiguravanju zakonitosti pristupa podacima i zaštite privatnosti korisnika. Istražitelji moraju osigurati da se pridržavaju zakonskih okvira, uključujući GDPR, ECPA, Zakon o zaštiti autorskih prava (engl. *Digital Millennium Copyright Act, DMCA*) i Direktivu o mrežnoj i informacijskoj sigurnosti (engl. *Network and Information Security, NIS*). Ovi zakoni i propisi definiraju pravila o prikupljanju, analizi i očuvanju podataka te postavljaju etičke smjernice koje istražitelji moraju poštovati.s

IoT forenzika je zbog svoje dinamičnosti i raznolikosti uređaja jedno od najzahtjevnijih područja digitalne forenzike. Razvoj učinkovitih metoda, alata i standarda ključan je za uspješno rješavanje sigurnosnih incidenata u sve kompleksnijem IoT okruženju (Stoyanova, Nikoloudakis, Panagiotakis, Pallis, & Markakis, 2020), (Atlam, Hemdan, Alenezi, Alassafi, & Wills, 2020).

# 5. Stvarni slučajevi i primjene računalne forenzike

U digitalnom dobu, računalna forenzika postala je ključan alat u borbi protiv različitih oblika kibernetičkog kriminala, od financijskih prijevara do sofisticiranih napada na korporativne i državne sustave. S razvojem tehnološkog ekosustava, raste i složenost prijetnji s kojima se suočavaju stručnjaci za sigurnost i pravosudni sustavi. Prikupljanje, analiza i očuvanje digitalnih dokaza sada su neizostavni dijelovi modernih istraga, omogućujući forenzičarima da otkriju skrivene digitalne tragove ključne za rješavanje slučajeva. Brojni stvarni slučajevi računalne forenzike pokazali su kako primjena specifičnih tehnika i alata može biti presudna za identifikaciju počinitelja i razumijevanje dinamike digitalnih zločina.

Ovo poglavlje donosi pregled nekoliko poznatih slučajeva u kojima je računalna forenzika odigrala ključnu ulogu u razotkrivanju i procesuiranju složenih digitalnih zločina. Ovi primjeri, poput financijskih prijevara, kibernetičkih napada i otkrivanja kriminalnih aktivnosti, pokazuju važnost i učinkovitost forenzičkih metoda.

Slučaj *Enron Corporation* iz 2001. godine ostaje jedan od najozloglašenijih primjera financijske prijevare u povijesti. *Enron*, nekada jedan od najvećih energetskih konglomerata, propao je zbog masovne manipulacije financijskim izvještajima. Računalna forenzika igrala je ključnu ulogu u ovom slučaju, posebno kroz analizu elektroničke pošte i financijskih dokumenata. Korištene su tehnike prikupljanja i analize e-pošte, forenzike baza podataka i mrežne forenzike, što je omogućilo istražiteljima da razotkriju opsežnu prijevaru. Ovaj slučaj je ne samo doprinio razvoju naprednijih tehnika za analizu velikih količina podataka, već je i postavio temelje za strože regulacije u financijskom sektoru, povećavajući potrebu za transparentnošću i odgovornošću.

Drugi značajan slučaj uključuje serijskog ubojicu Dennisa Radera, koji je desetljećima izbjegavao pravdu, sve do svog uhićenja 2005. godine zahvaljujući digitalnim tragovima ostavljenim na disketi. Dennis Rader, koji je u razdoblju između 1974. i 1991. godine počinio niz brutalnih ubojstava u području Wichite u saveznoj državi Kansas (Sjedinjene Američke Države), izazivao je policiju i medije, vjerujući da neće biti uhvaćen. Međutim, u svojoj komunikaciji s istražiteljima poslao je disketu misleći da je obrisao sve podatke koji bi mogli otkriti njegov identitet. Istražitelji su, koristeći računalnu forenziku, uspjeli povratiti izbrisane podatke i analizirati metapodatke s diskete, što je otkrilo tragove koji su ga nepobitno povezali sa zločinima. Ovaj slučaj pokazao je kako digitalni tragovi, čak i oni koji su bili namjerno izbrisani, mogu igrati ključnu ulogu u kriminalističkim istragama. Primjena računalne forenzike u ovom slučaju naglasila je važnost pažljive analize digitalnih dokaza i potaknula daljnji razvoj

tehnika za oporavak podataka.

Kompanija *Sony Pictures Entertainment* bila je žrtva velikog kibernetičkog napada 2014. godine, što je rezultiralo krađom i objavom povjerljivih podataka, uključujući filmove i osobne informacije zaposlenika. Forenzička analiza napada uspjela je identificirati sjevernokorejsku grupu kao počinitelje. U ovom slučaju korištene su mrežna forenzika, analiza zlonamjernog softvera i forenzika dnevničkih datoteka. Napad na *Sony Pictures* potaknuo je mnoge korporacije na preispitivanje i poboljšanje svojih sigurnosnih politika te na razvoj naprednijih tehnika za analizu zlonamjernog softvera.

Sljedeći slučaj koji zaslužuje pozornost je *Silk Road,* ilegalna *online* tržnica koja je zatvorena 2013. godine. Osnivač tržnice, Ross Ulbricht, uhvaćen je zahvaljujući digitalnim tragovima pronađenim na njegovom računalu. Istražitelji su primijenili tehnike analize mrežnog prometa, forenzike mobilnih uređaja i analize kripto valuta. Ovaj slučaj je naglasio važnost analize mrežnog prometa i pratnje digitalnih transakcija u borbi protiv kibernetičkog kriminala i ilegalne trgovine, posebno na tamnom webu (engl. *dark web*).

Na posljetku, slučaj koji je imao značajan utjecaj na računalnu forenziku bio je napad na web stranicu *Ashley Madison*, poznatu po pružanju usluga za izvanbračne afere. U napadu 2015. godine, napadači su uspjeli objaviti osobne podatke milijuna korisnika, izazivajući veliku medijsku pažnju i javne skandale. Istražitelji su koristili forenziku baza podataka, analizu zlonamjernog softvera i mrežnu forenziku kako bi pokušali utvrditi počinitelje i metode napada. Kao posljedica, ovaj slučaj je doveo do značajnog poboljšanja sigurnosnih mjera za zaštitu osobnih podataka i razvoja naprednijih tehnika za analizu baza podataka.

Ovi slučajevi jasno ilustriraju ključnu ulogu računalne forenzike u modernim istragama i njezin snažan utjecaj na razvoj forenzičkih tehnika i sigurnosnih politika. Svaki slučaj pridonio je razvoju novih metoda i alata koji se danas koriste u borbi protiv kibernetičkog kriminala, pokazujući koliko je važna stalna evolucija forenzičkih metoda u odgovor na sve sofisticiranije prijetnje i napade u digitalnom prostoru.

# 6. Izazovi i budući trendovi računalne forenzike

Računalna forenzika suočava se s nizom izazova i prilika koji će oblikovati njezinu budućnost. Razvoj novih tehnologija i sve veća količina digitalnih podataka zahtijevaju stalnu prilagodbu i inovaciju u ovoj disciplini. Uz rastuću složenost kibernetičkih prijetnji, forenzičari moraju razvijati nove tehnike i alate kako bi učinkovito analizirali podatke i osigurali integritet digitalnih dokaza.

Jedan od ključnih trendova je integracija umjetne inteligencije u forenzičke procese. Umjetna inteligencija može značajno ubrzati analizu velikih količina podataka, prepoznati obrasce i anomalije te automatizirati rutinske zadatke. Na primjer, algoritmi strojnog učenja mogu se koristiti za prepoznavanje zlonamjernog softvera ili analizu mrežnog prometa. Sustavi umjetne inteligencije mogu analizirati ogromne količine podataka u kratkom vremenu, što omogućuje brže donošenje odluka i učinkovitije istrage. Međutim, izazovi leže u osiguravanju točnosti i pouzdanosti tih sustava, kao i u etičkim pitanjima vezanim uz privatnost i sigurnost podataka. Potrebno je razviti standarde i protokole koji će osigurati da sustavi umjetne inteligencije djeluju unutar zakonskih i etičkih okvira.

Obrada velikih podataka (engl. *big data*) također igra ključnu ulogu u budućnosti računalne forenzike. S obzirom na eksponencijalni rast digitalnih podataka, forenzičari moraju razviti nove metode i alate za učinkovitu analizu i pohranu tih podataka. Tehnike poput distribucije obrade podataka, korištenja naprednih analitičkih alata i algoritama za pretraživanje postaju sve važnije. Na primjer, distribuirani sustavi omogućuju paralelnu obradu velikih količina podataka, što značajno smanjuje vrijeme potrebno za analizu. Izazovi uključuju upravljanje velikim količinama podataka te osiguravanje njihove integriteta i sigurnosti, uz poštivanje privatnosti korisnika.

Daljnji razvoj *cloud* forenzike predstavlja još jedan značajan trend. Kako sve više organizacija prelazi na cloud infrastrukturu, forenzičari se suočavaju s izazovima vezanim uz pristup i analizu podataka pohranjenih u oblaku. Potrebno je razviti specijalizirane alate i tehnike za forenzičku analizu cloud okruženja, uzimajući u obzir specifične sigurnosne i pravne aspekte. Cloud forenzika zahtijeva razumijevanje različitih *cloud* modela, kao što su *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) i *Software as a Service* (SaaS), te njihove sigurnosne implikacije. Izazov leži u osiguravanju integriteta podataka i zaštiti privatnosti korisnika. Forenzičari moraju biti svjesni pravnih ograničenja i regulacija koje se primjenjuju na podatke pohranjene u oblaku, posebno u kontekstu međunarodnih istraga.

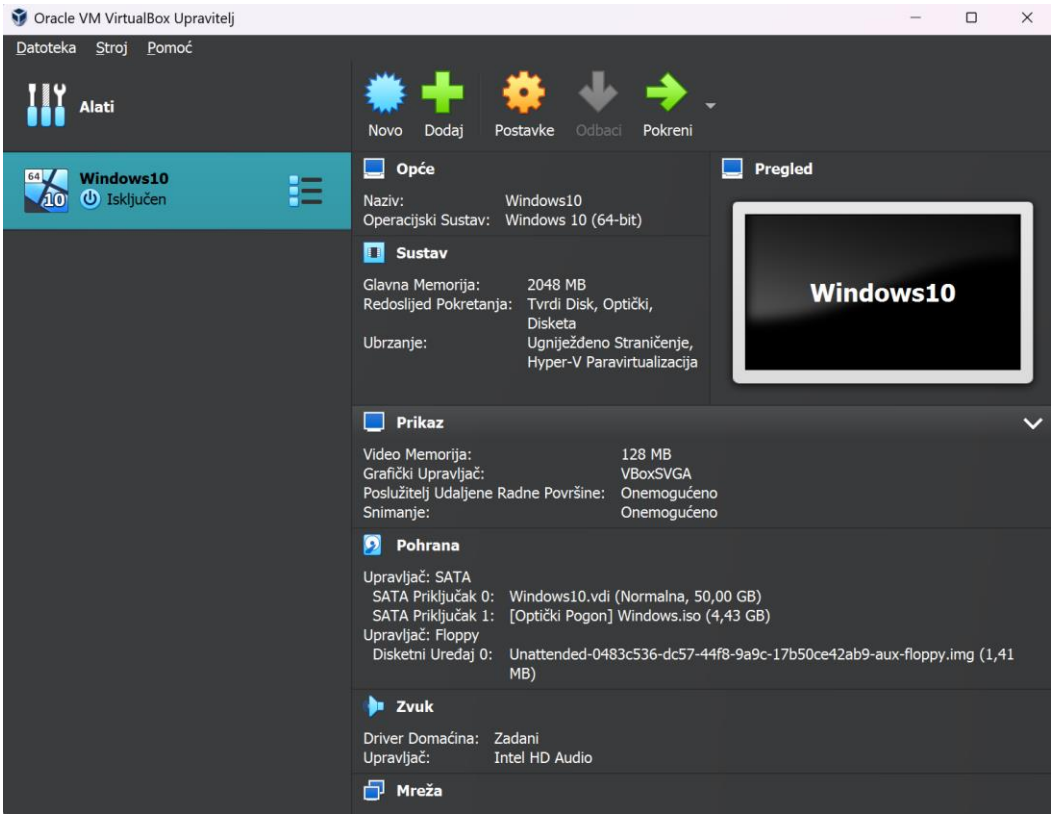
Forenzika Interneta stvari donosi nove izazove i prilike za računalnu forenziku. IoT uređaji

generiraju ogromne količine podataka koji mogu biti ključni dokazi u istragama. Međutim, forenzička analiza IoT uređaja zahtijeva specifične alate i metode zbog raznolikosti uređaja i protokola. IoT uređaji često koriste različite operacijske sustave i komunikacijske protokole, što otežava standardizaciju forenzičkih postupaka. Izazov je u osiguravanju pristupa i očuvanju podataka s ovih uređaja, kao i u zaštiti njihove sigurnosti. Forenzičari moraju razviti metode za prikupljanje i analizu podataka s IoT uređaja bez narušavanja njihovog integriteta.

Budući trendovi u računalnoj forenzici uključuju integraciju novih tehnologija i razvoj specijaliziranih alata i metoda. Očekuje se da će umjetna inteligencija, obrada velikih podataka, cloud forenzika i forenzika Interneta stvari igrati ključne uloge u budućnosti računalne forenzike. No, s tim trendovima dolaze i novi izazovi, uključujući pitanja privatnosti, sigurnosti i etike, koja će zahtijevati stalnu prilagodbu i inovaciju. Forenzičari će morati kontinuirano educirati i usavršavati svoje vještine kako bi mogli učinkovito odgovoriti na nove prijetnje i izazove u digitalnom okruženju.

# 7. Forenzička analiza računala pomoću alata Autopsy

Cilj praktičnog dijela ovog rada je provesti detaljnu analizu računala pomoću digitalnog forenzičkog alata *Autopsy*. Analiza je uključivala identifikaciju sumnjivih predmeta (engl. *Suspicious items*), loših predmeta (engl. *Bad items)* te izbrisanih podataka (engl. *Deleted Files*). Prvi korak bio je osigurati sigurno okruženje za provedbu digitalne forenzičke analize. To je uključivalo korištenje virtualnog okruženja ili izoliranog sustava kako bi se spriječio bilo kakav utjecaj na izvorne podatke i osigurala integritet analize. Za kreiranje virtualnog okruženja korišten je *Oracle VM VirtualBox* na operacijskom sustavu Windows 10. Slika 4 prikazuje sučelje *Oracle VM VirtualBox Managera* gdje su vidljivi svi relevantni detalji o virtualnom stroju. Ovi koraci su važni jer predstavljaju temelje digitalne forenzičke analize. Bez sigurnog i kontroliranog okruženja, postoji rizik od kompromitiranja podataka, što može dovesti do netočnih rezultata i potencijalno ugroziti cijelu istragu.



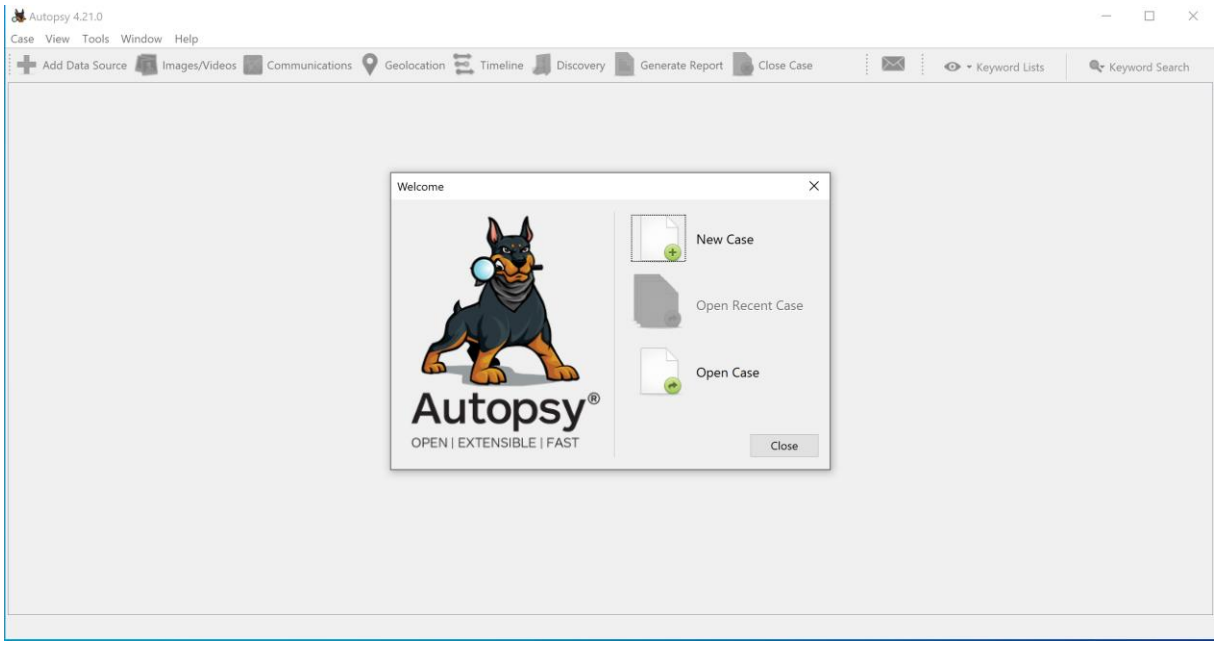

*Slika 4.* Sučelje Oracle VM VirtualBox Managera, izvor: Izrada Autora

Nakon postavljanja sigurnog okruženja, sljedeći korak je instalacija digitalno-forenzičke platforme *Autopsy*. Ovaj alat je izuzetno koristan za analizu diskova i mobilnih uređaja te omogućava oporavak podataka, poput fotografija s memorijskih kartica. Njegova svestranost čini ga neophodnim u forenzičkim istragama koje uključuju različite izvore podataka. *Autopsy*

nudi intuitivno grafičko sučelje koje olakšava navigaciju i upotrebu, čak i onima koji nisu stručnjaci u digitalnoj forenzici, čime omogućuje bržu i učinkovitiju analizu podataka, što je presudno u vremenski osjetljivim situacijama.

Instalacija softvera iz službenih izvora osigurava korištenje najnovije verzije, koja donosi sve sigurnosne nadogradnje i značajke potrebne za pouzdanu forenzičku analizu. *Autopsy* također omogućava oporavak izbrisanih podataka, što može biti ključno za razotkrivanje kriminalnih aktivnosti i pružanje dodatnih dokaza, čineći ga nezamjenjivim alatom u digitalnoj forenzici.

Nakon uspješne instalacije, pokreće se alat *Autopsy* i prikazuje početno sučelje programa (Slika 5) koje nudi opcije za kreiranje novog slučaja (engl. *New Case*) ili otvaranje postojećeg (engl. *Open Case*). Kreiranje novog slučaja omogućuje organizaciju i strukturiranje podataka koji će biti analizirani, pri čemu se precizno definiraju opseg i ciljevi analize.

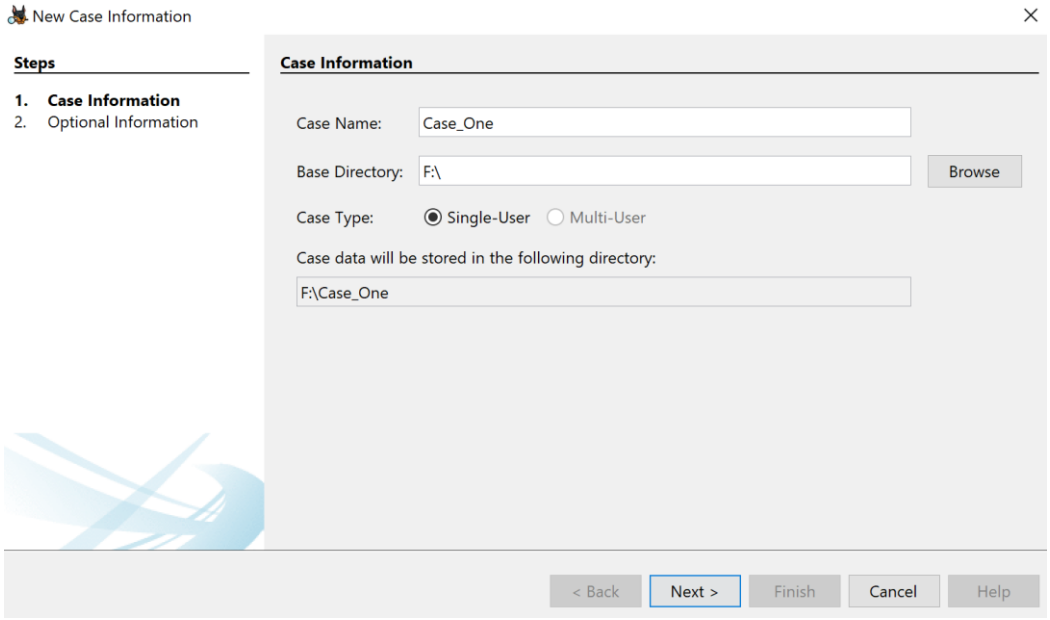



Slika 5. Početni ekran Softvera Autopsy, izvor: Izrada Autora

Nakon odabira opcije *New Case,* otvara se prozor *Case Information* za unos osnovnih podataka o slučaju (Slika 6). U ovom prozoru unose se podaci poput naziva slučaja (engl. *Case Name*), lokacije za pohranu rezultata analize (engl. *Base Directory*) i tipa slučaja (engl. *Case Type*), pri čemu je u ovom primjeru odabran tip *Single-User*, jer je slučaj namijenjen jednom istražitelju. Ovaj korak omogućuje alatu prepoznavanje i učitavanje svih relevantnih podataka za daljnju analizu.

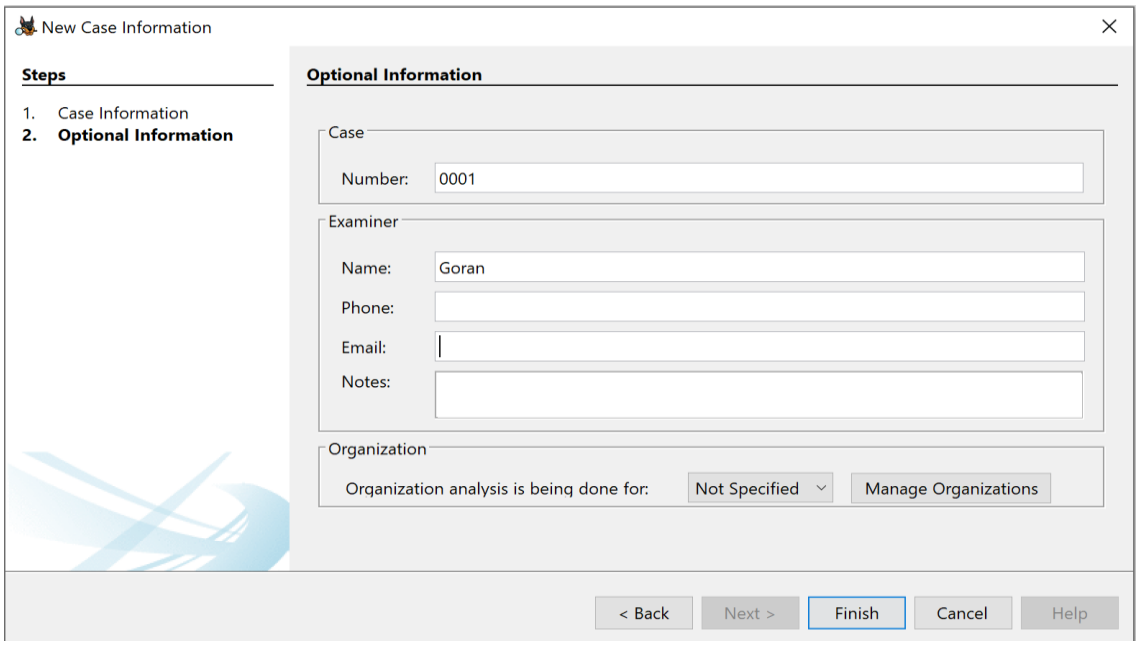
Kreiranje novog slučaja (Slika 6) i dodavanje izvora podataka postavlja temelje za daljnju analizu i interpretaciju rezultata. Ovi koraci osiguravaju da svi relevantni podaci budu uključeni

u analizu, čime se povećavaju šanse za pronalaženje ključnih dokaza. Na taj način, *Autopsy* omogućava analitičarima da učinkovito i precizno provode digitalne forenzičke istrage.



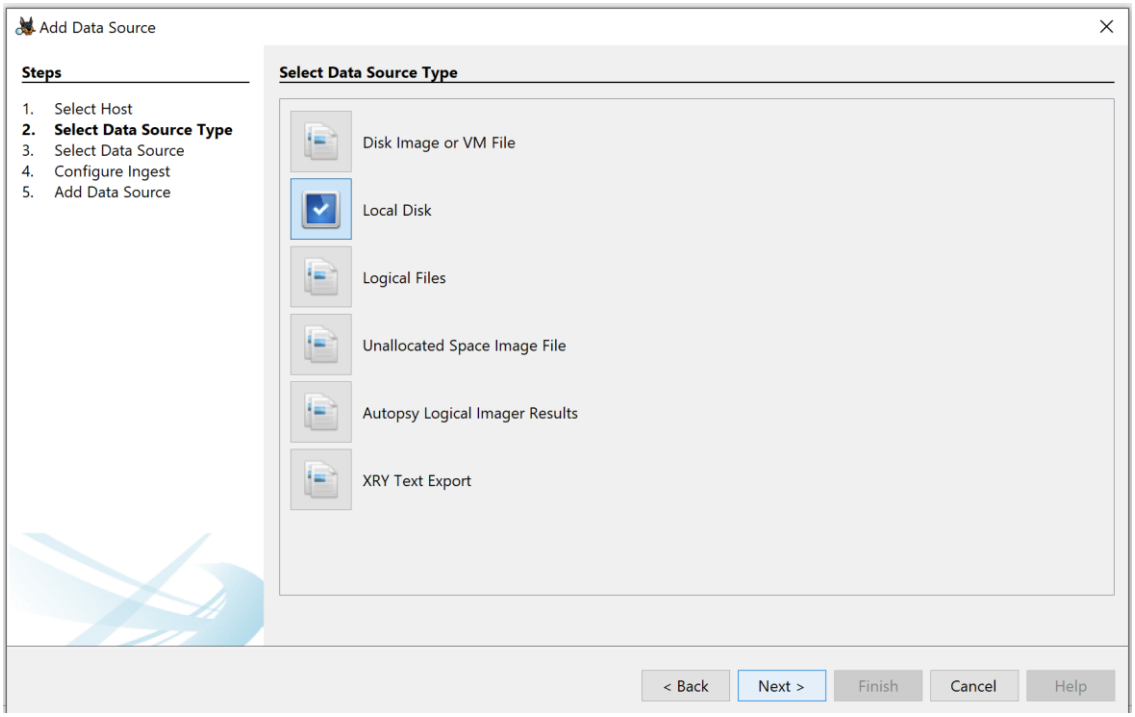

Slika 6. *Case Information* sučelje, izvor: Izrada autora

Slika 7 prikazuje prozor *Optional Information* u alatu *Autopsy*, koji omogućava unos dodatnih informacija o slučaju. Ovaj korak omogućuje alatu prepoznavanje i učitavanje svih relevantnih podataka za analizu. Organizacija i strukturiranje podataka unutar novog slučaja ključni su za održavanje reda i jasnoće tijekom cijelog procesa analize, što je presudno za uspješnu forenzičku istragu.




Slika 7. *Optional Information* sučelje, izvor: Izrada autora

Sljedeći korak nakon unosa informacija o slučaju je dodavanje izvora podataka koji će se analizirati (Slika 8). Otvaranjem prozora za dodavanje izvora podataka, omogućuje se odabir između različitih tipova izvora. Ti tipovi uključuju diskovnu sliku ili datoteku virtualnog stroja (engl. *Disk Image or VM File*), lokalni disk (engl. *Local Disk*), logičke datoteke (engl. *Logical Files*), sliku nealociranog prostora (engl. *Unallocated Space Image File*), rezultate *Autopsy* logičkog imagera (engl. *Autopsy Logical Imager Results*) i XRY tekstualni izvor (engl. *XRY Text Export*).




Slika 8. Sučelje Autopsy sofvera za dodavanje izvora tipa izvora podataka, izvor: Izrada autora

Diskovna slika ili datoteka virtualnog stroja odnosi se na potpunu kopiju fizičkog diska ili na datoteku koja sadrži virtualni stroj. Analizom diskovne slike, forenzičari mogu pregledati cjelokupan sadržaj diska, uključujući sistemske datoteke, skrivene particije i ostatke izbrisanih podataka. Ovaj pristup je ključan za očuvanje originalnih podataka, jer omogućava rad s kopijom, čime se sprječava rizik od izmjena na originalnom disku. Također, forenzičari mogu pregledati virtualne strojeve kako bi analizirali simulirana okruženja korištena na istraživanom uređaju.

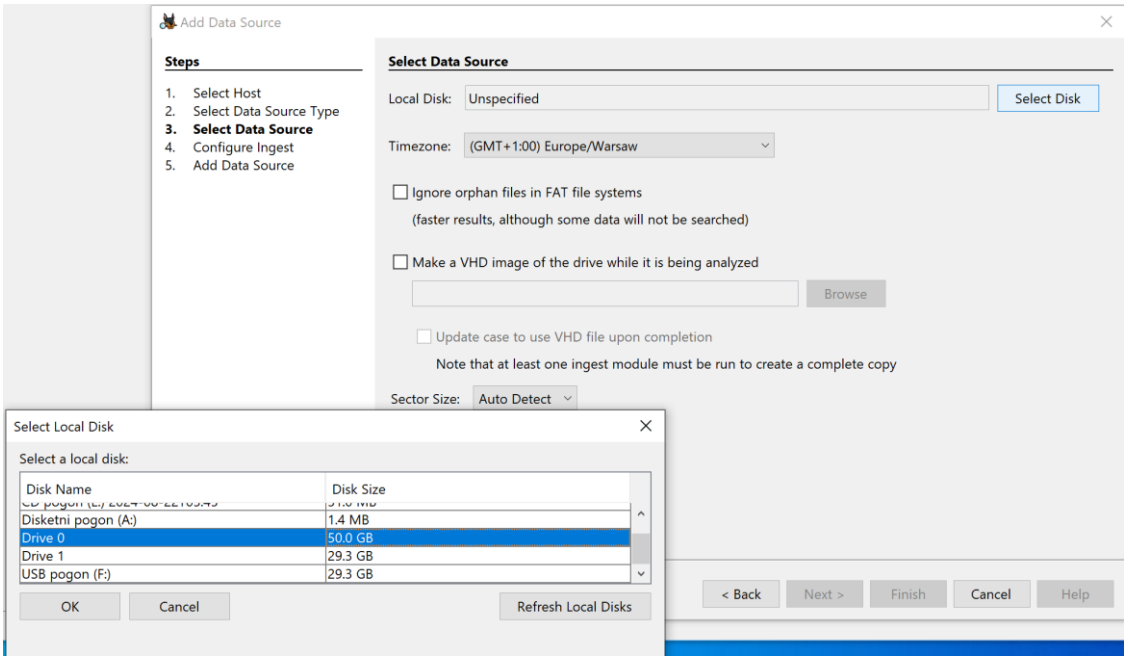
Logičke datoteke odnose se na pojedinačne datoteke ili grupe datoteka koje se analiziraju bez potrebe za pristupom cijelom disku. Ova opcija je korisna kada je potrebno brzo analizirati specifične dokumente ili mape bez analiziranja cjelokupnog diska. Logička analiza omogućava ciljani pregled podataka, što je praktično kada fizički disk nije dostupan

ili kada postoji potreba za analizom manjih setova podataka.

Slika nealociranog prostora odnosi se na dijelove diska koji trenutno nisu dodijeljeni nijednoj datoteci ili mapi. Iako ovaj prostor nije vidljiv korisniku, on može sadržavati ostatke izbrisanih podataka koji nisu fizički prepisani. Analiza nealociranog prostora je ključna za otkrivanje podataka koje je korisnik možda pokušao izbrisati ili sakriti, ali koji su još uvijek dostupni za oporavak.

Rezultati *Autopsy* logičkog imagera odnose se na podatke prikupljene korištenjem *Autopsy* alata za kreiranje logičkih slika diska. Ovi rezultati omogućavaju forenzičarima da analiziraju sadržaj diska bez fizičkog pristupa disku. Logičke slike omogućavaju sigurno rukovanje podacima u situacijama kada je disk oštećen ili kada je potrebno raditi s kopijama podataka kako bi se očuvala vjerodostojnost originala.

XRY tekstualni izvor odnosi se na podatke prikupljene iz mobilnih uređaja korištenjem XRY softverskog alata. Ovi podaci mogu uključivati tekstualne poruke, kontakte, zapisnike poziva i druge relevantne informacije koje su ključne za mobilne forenzičke istrage. Ova vrsta analize pomaže u otkrivanju ključnih dokaza na mobilnim uređajima koji su često centralni u digitalnim istragama.

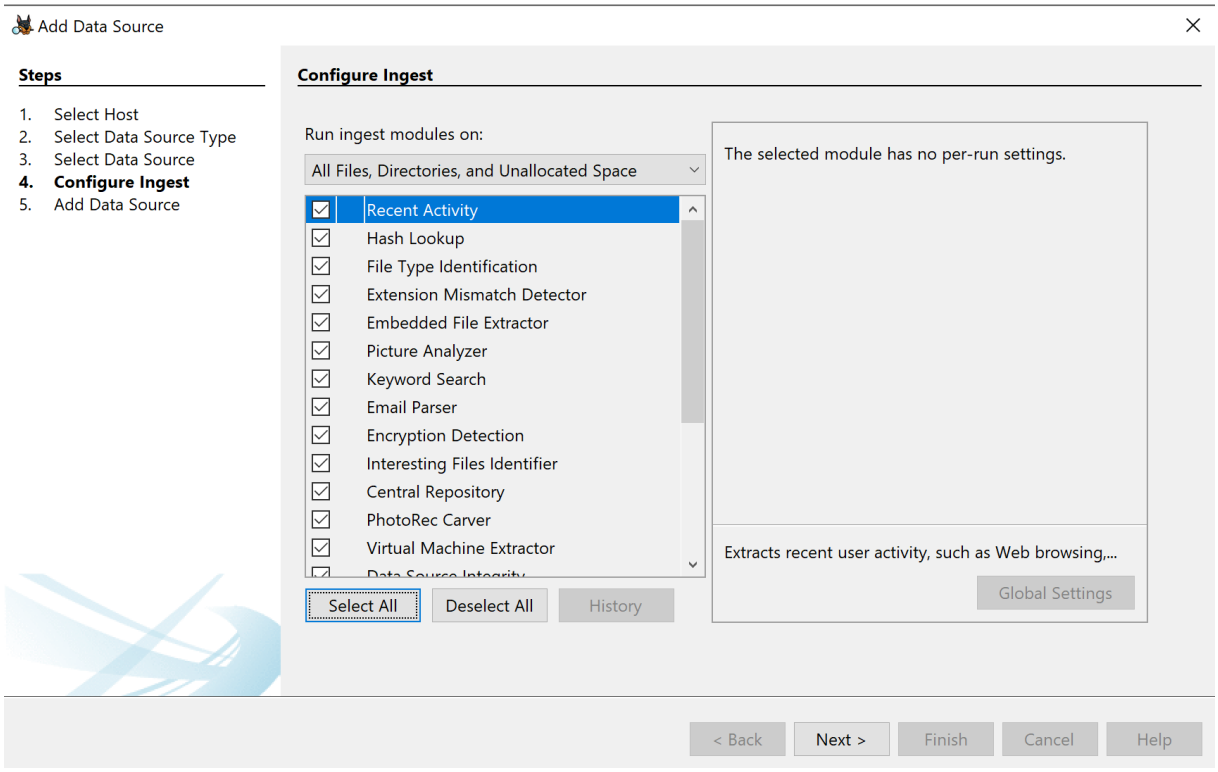



Slika 9. sučelje Autopsy softvera za izbor analize lokalnog diska, izvor: Izrada autora

Za potrebe demonstracije u ovom radu odabrana je opcija *Local Disk* kako bi se nastavilo s analizom. Nakon odabira opcije, otvara se prozor za odabir lokalnog diska (Slika 9). U prikazanom prozoru nalazi se popis dostupnih diskova, uz informacije o njihovim veličinama i

drugim relevantnim podacima. Ovaj pregled omogućava forenzičaru da identificira i odabere odgovarajući disk za analizu. Odabir ispravnog diska ključan je za osiguravanje da se analiza provodi na ispravnom izvoru podataka, što povećava točnost i relevantnost rezultata istrage. Nakon što je odgovarajući disk odabran, proces analize može započeti, omogućujući forenzičaru detaljan pregled sadržaja diska, uključujući potencijalno sumnjive aktivnosti.

Sljedeći korak nakon odabira izvora podataka je konfiguracija *ingest* modula (Slika 10). Otvaranjem prozora za konfiguraciju omogućuje se odabir različitih modula za analizu podataka, poput *Recent Activity*, *Hash Lookup*, *File Type Identification*, *Extension Mismatch Detector* i drugih. Svaki modul ima specifičnu ulogu i doprinosi sveobuhvatnoj analizi podataka.




Slika 10. Prozor za odabir modula za analizu podataka, izvor: Izrada autora

Prvi na popisu, modul *Recent Activity* omogućava izvlačenje informacija o nedavnim korisničkim aktivnostima, kao što su pregledavanje weba, otvaranje datoteka i korištenje aplikacija. Ovaj modul je ključan jer pomaže forenzičaru da rekonstruira radnje korisnika neposredno prije incidenta, što može pružiti važne tragove i smjerove za daljnju istragu.

Nadalje, *Hash Lookup* modul koristi se za usporedbu *hash* vrijednosti analiziranih datoteka s bazama poznatih vrijednosti. Ova funkcionalnost omogućava forenzičaru da brzo prepozna poznate zlonamjerne ili sumnjive datoteke na temelju njihovih jedinstvenih identifikatora, čime

se značajno ubrzava proces identifikacije ključnih dokaza.

Sljedeći važan modul je *File Type Identification*, koji pomaže u prepoznavanju tipova datoteka na temelju njihovih unutarnjih karakteristika, umjesto samo ekstenzije. Ovo je posebno korisno kada su datoteke preimenovane kako bi sakrile svoju pravu prirodu. Također, ovaj modul može otkriti potencijalno sumnjive datoteke koje na prvi pogled izgledaju bezopasno.

*Extension Mismatch Detector* nadopunjuje modul za identifikaciju tipova datoteka. Njegova uloga je da označi datoteke čija ekstenzija ne odgovara stvarnom tipu datoteke. Ovaj modul je od iznimne važnosti kada postoji sumnja da su datoteke namjerno maskirane kako bi se prikrila njihova stvarna funkcija, što može biti znak zlonamjernih aktivnosti.

Umjesto obrade svih funkcionalnosti modula, fokus je stavljen na one najvažnije za većinu forenzičkih analiza. Njihova pravilna primjena od suštinskog je značaja za dobivanje uvida u korisničke aktivnosti, otkrivanje zlonamjernih datoteka i prepoznavanje nepravilnosti, što direktno doprinosi uspješnosti digitalne istrage. Konfiguracija *ingest* modula omogućava forenzičaru prilagodbu analize specifičnim potrebama slučaja. Pažljiv odabir modula osigurava da svi relevantni podaci budu temeljito prepoznati i analizirani na učinkovit i sveobuhvatan način, maksimizirajući uspjeh istrage.

Nakon odabira modula za analizu podataka, *Autopsy* započinje proces analize. Ovaj korak je ključan jer omogućuje softveru automatsko pretraživanje sumnjivih, zlonamjernih i izbrisanih podataka. *Autopsy* koristi napredne algoritme za pretraživanje relevantnih ključnih riječi koje mogu biti važne za istragu, uključujući nazive datoteka, fraze ili druge indikatore sumnjivih aktivnosti. Identifikacija potencijalno sumnjivih datoteka temelji se na njihovom sadržaju, ponašanju ili drugim karakteristikama.

Autopsy također analizira metapodatke datoteka, kao što su datumi kreiranja i izmjene, veličina datoteka i njihova lokacija na disku. Uz to, koristi *hash* vrijednosti za usporedbu datoteka s poznatim bazama podataka zlonamjernog softvera, čime se ubrzava identifikacija kompromitiranih datoteka. Ovi koraci pomažu forenzičaru da brzo identificira datoteke koje mogu biti relevantne za istragu. Još jedan ključan aspekt analize je pokušaj oporavka izbrisanih datoteka. *Autopsy* koristi tehnike oporavka podataka kako bi povratio datoteke izbrisane s medija za pohranu. Te tehnike uključuju pretraživanje slobodnog prostora na disku i analizu fragmentiranih podataka. Oporavljene datoteke često predstavljaju ključne dokaze koje su korisnici pokušali sakriti ili uništiti.

Kada Autopsy prepozna sumnjive ili kompromitirane podatke, to može značiti nekoliko stvari za istragu. Takvi podaci mogu uključivati zlonamjerni softver, neovlaštene pristupe ili

druge oblike kompromitiranih podataka. *Autopsy* koristi različite tehnike, poput *hash* pretraživanja, analize metapodataka i prepoznavanja obrazaca, kako bi identificirao ove podatke.

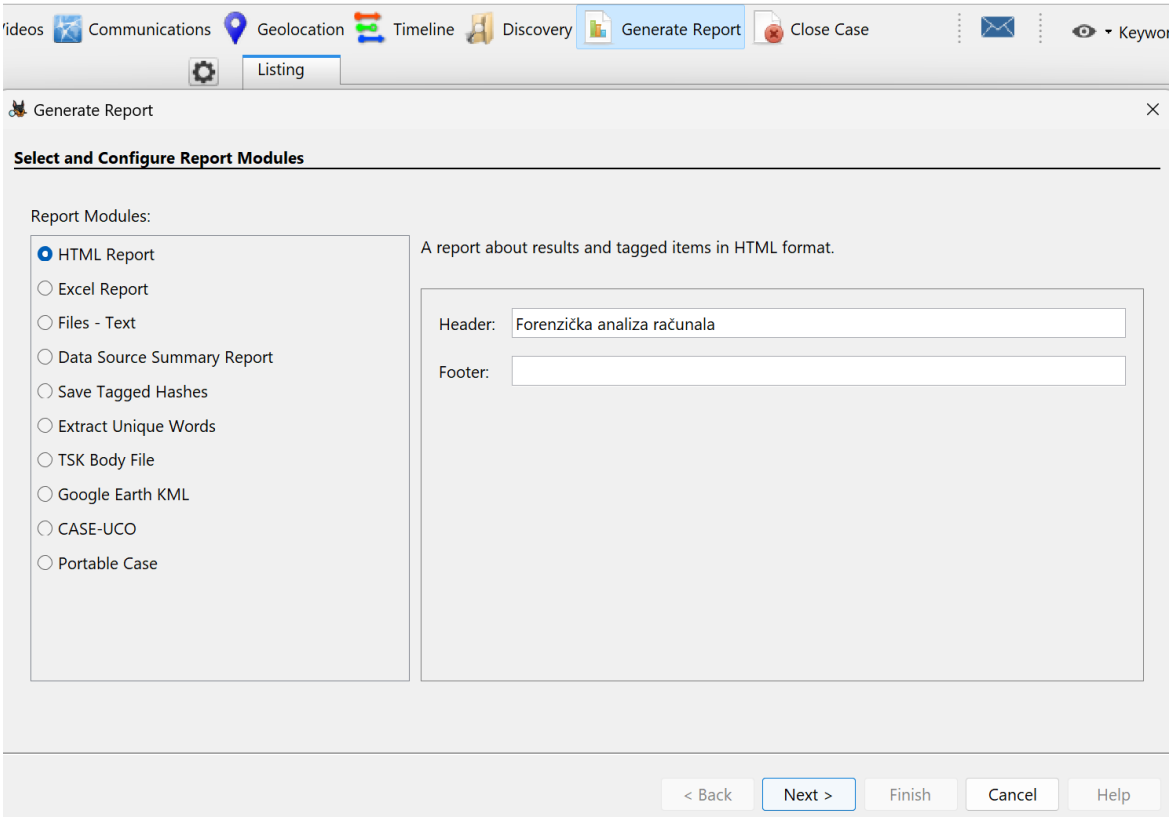
Rezultati analize mogu imati značajan utjecaj na daljnji tijek istrage. Primjerice, identificirane sumnjive datoteke mogu dovesti do utvrđivanja izvora napada, bilo da se radi o otkrivanju IP adrese napadača, kompromitiranih računala ili mreža povezanih s napadom. Nadalje, analiza može pomoći u identifikaciji počinitelja putem podataka o korisničkim aktivnostima, kao i putem analize digitalnih tragova koji otkrivaju tko je imao pristup određenim datotekama u kritičnim trenucima. Osim toga, uspješno identificiranje i analiza sumnjivih podataka može omogućiti prikupljanje dodatnih dokaza koji se mogu koristiti u sudskim postupcima ili daljnjim fazama istrage. Ovi dokazi mogu uključivati povijest pregledavanja, poruke e-pošte, zapisnike korištenih aplikacija ili oporavljene izbrisane datoteke, a sve to može biti ključno za dokazivanje ili pobijanje tvrdnji unutar digitalne istrage.

U konačnici, korištenje ovih tehnika unutar alata *Autopsy* ne samo da omogućuje detaljnu analizu podataka, već i osigurava forenzičarima pouzdane rezultate koji mogu direktno utjecati na uspjeh istrage, pridonoseći prikupljanju ključnih dokaza i otkrivanju relevantnih informacija koje su od kritičnog značaja za cjelokupni ishod istrage.

Nakon završetka analize, *Autopsy* generira detaljan izvještaj koji obuhvaća sve pronađene podatke. Ovaj izvještaj je ključan jer pruža sveobuhvatan pregled rezultata analize, uključujući popis sumnjivih datoteka, oporavljene podatke i druge relevantne informacije. Izvještaj se može izvesti u različitim formatima, kao što su *Portable Document Format* (PDF) ili *HyperText Markup Language* (HTML), što omogućuje daljnju analizu ili prezentaciju rezultata.

Na slici 11 je prikazan prozor za generiranje izvještaja u alatu *Autopsy*, gdje se mogu odabrati različiti moduli izvještaja. Na primjer, opcija *HTML Report* omogućava generiranje izvještaja u HTML formatu, koji može sadržavati rezultate analize i označene stavke. Ovaj format je posebno koristan za pregled rezultata u pregledniku i za jednostavno dijeljenje s drugim članovima tima. U prozoru je moguće prilagoditi zaglavlje i podnožje izvještaja kako bi odgovarali specifičnostima istrage, što omogućava dodavanje informacija kao što su naziv istrage, ime forenzičara ili dodatne bilješke.

Generiranje izvještaja je važan korak jer omogućuje forenzičarima da dokumentiraju svoje nalaze na strukturiran i pregledan način. Ti izvještaji mogu biti korišteni kao dokaz u sudskim postupcima ili kao referenca za daljnje istraživanje.




Slika 11. Prozor za generiranje izvještaja, izvor: Izrada autora

Cilj ove forenzičke analize bio je identificirati sumnjive, loše i izbrisane podatke korištenjem alata *Autopsy*. Na temelju prikazanih rezultata, može se zaključiti da je taj cilj uspješno ostvaren. *Autopsy* je pretraživao ključne riječi relevantne za istragu, identificirao datoteke koje su bile sumnjive na temelju njihovog sadržaja ili ponašanja te pokušao oporaviti izbrisane datoteke s medija za pohranu.

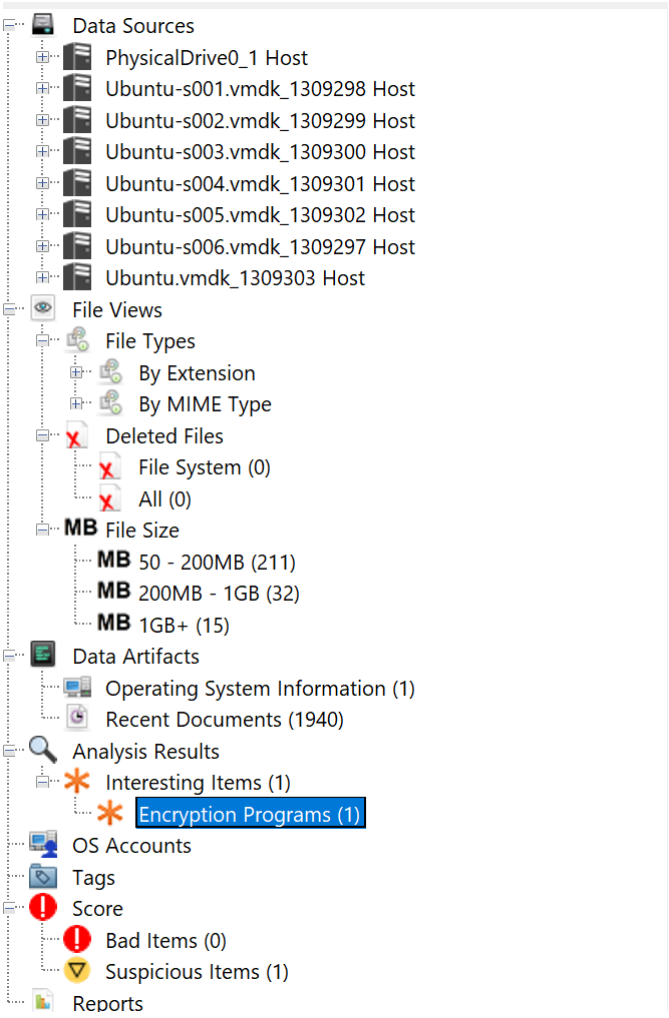
Na slici 12 je prikazan pregled rezultata forenzičke analize u alatu *Autopsy*, organiziran u nekoliko kategorija. U odjeljku *Data Sources*, prikazani su različiti izvori podataka, uključujući fizički disk (*PhysicalDrive0_1 Host*) i više virtualnih diskova (*vmdk* datoteka). Ovi izvori predstavljaju okruženje koje je forenzički analizirano, pri čemu se svaka datoteka i particija pažljivo ispituju radi pronalaska relevantnih podataka.

U odjeljku *File Views*, datoteke su razvrstane prema raznim kriterijima:

- *By Extension* i *By MIME Type* prikazuju datoteke organizirane po vrsti ekstenzije i njihovim MIME tipovima, što omogućava forenzičaru jednostavno filtriranje i pregled datoteka na temelju njihovih karakteristika.
- *Deleted Files* ukazuje na datoteke koje su izbrisane, a *Autopsy* pokušava oporaviti takve datoteke pomoću naprednih tehnika za oporavak podataka. U ovom slučaju, u trenutku analize nije pronađena nijedna izbrisana datoteka, no ovaj segment ostaje ključan za

pronalaženje skrivenih tragova.

- *File Size* omogućava pregled datoteka po veličini, pri čemu se ističu datoteke veće od 1 GB, što može biti posebno važno za analizu velikih datoteka, poput multimedijskih ili komprimiranih arhiva koje mogu sadržavati bitne podatke.




Slika 12. Prikaz rezultata analize, izvor: Izrada autora

Kategorija *Data Artifacts* sadrži ključne podatke o sustavu, uključujući informacije o operacijskom sustavu (engl. *Operating System Information*) te nedavni dokumenti (engl. *Recent Documents*), pri čemu je otkriveno 1940 nedavnih dokumenata. Ovi artefakti mogu biti presudni za otkrivanje korisničkih aktivnosti i potencijalno sumnjivih radnji.

Pod sekcijom *Analysis Results*, alat prikazuje rezultate analize ključnih stavki, pri čemu se ističu zanimljive stavke (engl. *Interesting Items*) i programi za šifriranje (engl. *Encryption Programs*). Obje stavke su od posebnog značaja, jer *zanimljive stavke* često označavaju datoteke ili programe koji su identificirani kao relevantni za istragu na temelju svog sadržaja, ponašanja ili učestalosti korištenja. S druge strane, programi za šifriranje mogu ukazivati na

pokušaje prikrivanja podataka, što je posebno relevantno u slučajevima koji uključuju neovlaštene aktivnosti ili zlonamjerni softver.

Odjeljci *Tags* i *Score* pružaju dodatni uvid u ocjenjivanje i označavanje datoteka. Ovdje se prikazuju stavke koje su označene kao "Loše" (engl. *Bad Items*) ili "Sumnjive" (engl. *Suspicious Items*), čime se forenzičarima olakšava fokusiranje na kritične stavke koje mogu biti presudne za ishod istrage.

Prikazana forenzička analiza jasno pokazuje kako *Autopsy* omogućuje temeljitu i detaljnu obradu digitalnih dokaza. Alat je pokazao sposobnost pretraživanja različitih izvora podataka, organiziranja prema tipu i veličini, te identifikacije potencijalno sumnjivih stavki, poput programa za šifriranje, zlonamjernog softvera i nedavno korištenih dokumenata. Osim toga, *Autopsy* omogućuje oporavak izbrisanih datoteka, čime osigurava da se niti jedan važan dokaz ne izgubi tijekom analize. U prikazanoj analizi rezultata, *Autopsy* omogućuje brzo prepoznavanje i ocjenjivanje ključnih stavki relevantnih za istragu. Kategorizacija podataka prema tipu i statusu, uz mogućnost filtriranja i označavanja, olakšava daljnje korake u istražnom procesu. Identifikacija sumnjivih i kompromitiranih podataka doprinosi utvrđivanju izvora napada, identifikaciji počinitelja i prikupljanju dodatnih dokaza.

Zbog svoje mogućnosti prilagodbe i opsežnih mogućnosti analize, *Autopsy* predstavlja važan alat u digitalnim forenzičkim istragama. Rezultati dobiveni iz analize mogu značajno doprinijeti daljnjem tijeku istrage, omogućujući forenzičarima i pravnim stručnjacima da donesu informirane odluke na temelju prikupljenih dokaza. Korištenje ovog alata pruža čvrstu osnovu za analizu podataka, otkrivanje ključnih informacija i osiguranje pravne valjanosti prikupljenih dokaza, čime se dodatno osigurava uspjeh forenzičke istrage.

# 8. Zaključak

Računalna forenzika predstavlja ključnu disciplinu u suvremenim istragama, omogućujući prikupljanje, analizu i očuvanje digitalnih dokaza koji su često presudni za rješavanje složenih slučajeva. Razvoj standarda i smjernica, poput ISO/IEC 27037 i NIST SP 800-86, osigurao je prikupljanje digitalnih dokaza na način koji omogućuje njihovu prihvatljivost na sudu, dok alati poput *EnCase, Sleuth Kit* i *SIFT Workstation* omogućuju sveobuhvatnu analizu. Praktični dio rada, koji se bavio forenzičkom analizom pomoću alata *Autopsy*, pokazao je kako ovaj alat omogućuje preciznu identifikaciju sumnjivih datoteka, analizu metapodataka te oporavak izbrisanih podataka. Ovaj praktični primjer potvrdio je važnost korištenja specijaliziranih alata u digitalnim istragama i dao uvid u primjenjivost teoretskih koncepata u stvarnim slučajevima.

Budućnost računalne forenzike oblikovat će integracija novih tehnologija, kao što su umjetna inteligencija, obrada velikih podataka, cloud forenzika i forenzika Interneta stvari. Ovi trendovi otvaraju nove prilike, ali i izazove, uključujući pitanja privatnosti, sigurnosti i etike. Forenzičari će se morati kontinuirano educirati i usavršavati kako bi mogli učinkovito odgovoriti na rastuće prijetnje i izazove u digitalnom okruženju.

Računalna forenzika će i dalje igrati ključnu ulogu u pravnim i sigurnosnim istragama, osiguravajući da su digitalni dokazi pouzdani, očuvani i prihvatljivi na sudu. Daljnji razvoj tehnologija i metoda omogućit će forenzičarima da se uspješno suoče s novim izazovima i prijetnjama, osiguravajući pravdu i sigurnost u sve digitalnijem svijetu.

# PRILOZI

## Popis slika



## Popis Tablica

# LITERATURA


Atlam, H. F., Hemdan, E. E., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2020). Internet of things forensics: A review. *Internet of Things, 11*, 10.

Barnum, P. (5. Prosinac 2014). *ony Pictures Hack (2014) - Technical, and Financial, and Legal Analysis*. Dohvaćeno iz security.inedo.com: https://security.inedo.com/library/incidents/Sony-2014

Columbia University. (Studeni 2022). *The Hacking of Sony Pictures: A Columbia University Case Study*. Dohvaćeno iz www.sipa.columbia.edu: https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf

DataNumen. (27. Listopad 2023). *Računalna forenzika: Uvod i budući izgledi*. Dohvaćeno iz www.datanumen.com: https://www.datanumen.com/hr/blogovi/uvod-u-ra%C4%8Dunalnu-forenziku-i-budu%C4%87nost/

European parliament. (27. Travanj 2016). *Uredba (EU) 2016/679 Europskog parlamenta*. Dohvaćeno iz eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32016R0679

Gallagher, M. (2. Sijačanj 2024). *What Is CISSP Certification? Qualifications, Benefits And Salary*. Dohvaćeno iz www.forbes.com: https://www.forbes.com/advisor/education/it-and-tech/what-is-cissp/

Gann, M. (25. Rujan 2023). *How To Use SIFT Workstation*. Dohvaćeno iz robots.net: https://robots.net/tech/how-to-use-sift-workstation/

Giustini, G. (2008). *History of the Project - CAINE Live*. Dohvaćeno iz www.caine-live.net: https://www.caine-live.net/page4/history.html

ISO/IEC. (15. Listopada 2012). *Guidelines for identification, collection, acquisition and preservation of digital evidence (first edition)*. Dohvaćeno iz www.iso27001security.com: https://www.iso27001security.com/html/27037.html

Johansen, G. (2017). *Digital Forensics and Incident Response.* Birmingham: Packt Publishing Ltd.

Kävrestad, J., Birath, M., & Clarke, N. (2024). Autopsy Forensics. U *Fundamentals of Digital Forensics* (str. 179-193). Springer. Dohvaćeno iz link.springer.com.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (Kolovoz 2006). *Computer Security Resource Center*. Gaithersburgu: National Institute of Standards and Technology (NIST). Dohvaćeno iz csrc.nist.gov: https://csrc.nist.gov/pubs/sp/800/86/final

Lee, R. (n.d.). *SIFT Workstation*. Dohvaćeno iz www.sans.org: https://www.sans.org/tools/sift-workstation/

Lehr, J. (n.d.). *computer forensics digital forensics*. Dohvaćeno iz www.caine-live.net: https://www.caine-live.net/

Libby, K. (3. Listopad 2023). *Autopsy: The Digital Forensics Toolkit*. Dohvaćeno iz eforensicsmag.com: https://eforensicsmag.com/autopsy-the-digital-forensics-toolkit/

Microsoft. (2024). *Što je zlonamjerni softver*. Dohvaćeno iz www.microsoft.com/hr-hr: https://www.microsoft.com/hr-hr/security/business/security-101/what-is-malware

Minc, A. (31. Srpanj 2023). *Understanding the Electronic Communications Privacy Act:*

*Safeguarding Internet Freedom & Liability*. Dohvaćeno iz www.minclaw.com: https://www.minclaw.com/electronic-communications-privacy-act/

Mrkonjić, D. (15. Rujan 2022). *Mrežna forenzika: metode i alati.* Dohvaćeno iz repozitorij.forenzika.unist.hr: https://repozitorij.forenzika.unist.hr/islandora/object/forenzikast:194

Nacionalni CERT i LS&S. (2010). *Računalna forenzika. dokument NCERT-PUBDOC-2010-05-301*. Zagreb. Dohvaćeno iz www.cert.hr: https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-05-301.pdf

Open Text. (11. Ožuljak 2021). *Announcing OpenText Security and Protection Cloud CE 21.1*. Dohvaćeno iz blogs.opentext.com: https://blogs.opentext.com/announcing-opentext-security-protection-cloud-ce-21-1/

Open Text. (2021). *OpenText EnCase Forensic*. Dohvaćeno iz www.opentext.com: https://www.opentext.com/file_source/OpenText/en_US/PDF/opentext-po-encase-forensic-en.pdf

PBS. (2024). *Who's Responsible? - Computer Crime Laws*. Dohvaćeno iz www.pbs.org: https://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html

Pichan, A. (2015). *Cloud forensic: Technical challenges, solutions and comparative analysis*. Dohvaćeno iz espace.curtin.edu.au: https://espace.curtin.edu.au/handle/20.500.11937/33937

Rudeš, H. (2018). *Forenzična analiza i antiforenzične mjere nad NTFS datotečnim sustavom.* Dohvaćeno iz repozitorij.forenzika.unist.hr: https://repozitorij.forenzika.unist.hr/islandora/object/forenzikast%3A14/datastream/PDF/view

Sayada Sonia Akter, M. S. (10. Ožuljak 2023). *Cloud Forensic: Issues, Challenges and Solution.* Dohvaćeno iz arxiv.org: https://arxiv.org/pdf/2303.06313

Shakeel, I. (06. Srpanj 2019). *Computer Forensics: Overview of Malware Forensics*. Dohvaćeno iz www.infosecinstitute.com: https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-overview-malware-forensics/

Simataa, S. (01. Ožuljak 2023). *The Enron case-Digital forensics summary*. Dohvaćeno iz www.linkedin.com: https://www.linkedin.com/pulse/enron-case-digital-forensics-summary-simasiku-lifuna-simataa

Smith, B. H. (29. Kolovoz 2018). *How A Floppy Disk Exposed Dennis Rader As The BTK Killer*. Dohvaćeno iz www.oxygen.com: https://www.oxygen.com/snapped/crime-time/floppy-disk-exposed-dennis-rader-btk-killer

Stenberg, D. (24. Travanj 2014). *Wireshark dissector work*. Dohvaćeno iz daniel.haxx.se: https://daniel.haxx.se/blog/2014/04/24/wireshark-dissector-work/

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (06. Siječanj 2020). *A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues.* Dohvaćeno iz ieeexplore.ieee.org: https://ieeexplore.ieee.org/document/8950109

The Federal Bureau Of Investigation. (13. Prosinac 2006). *Crime in the Suites*. Dohvaćeno iz archives.fbi.gov: https://archives.fbi.gov/archives/news/stories/2006/december/enron_121306

The Sleuth Kit. (2024). *About*. Dohvaćeno iz sleuthkit.org: https://sleuthkit.org/about.php

U.S. Attorney's Office. (05. Veljača 2015). *Ross Ulbricht, The Creator And Owner Of The "Silk Road" Website, Found Guilty In Manhattan Federal Court On All Counts*. Dohvaćeno iz www.justice.gov: https://www.justice.gov/usao-sdny/pr/ross-ulbricht-creator-and-owner-silk-road-website-found-guilty-manhattan-federal-court

Zbrog, M. (2. Kolovoz 2019). *Forensics Casefile: Cracking the Silk Road*. Dohvaćeno iz www.forensicscolleges.com: https://www.forensicscolleges.com/blog/forensics-casefile/silk-road

Zbrog, M. (04. Veljača 2020). *Forensics Casefile: Catching the BTK Strangler*. Dohvaćeno iz www.forensicscolleges.com: https://www.forensicscolleges.com/blog/forensics-casefile-btk-strangler