Forenzička analiza operacijskog sustava Windows 11

Vručina, Ivan

Undergraduate thesis / Završni rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:349853

Rights / Prava: Attribution 3.0 Unported / Imenovanje 3.0

Download date / Datum preuzimanja: 2025-03-17



Repository / Repozitorij:

Faculty of Organization and Informatics - Digital Repository





SVEUČILIŠTE U ZAGREBU FAKULTET ORGANIZACIJE I INFORMATIKE V A R A Ž D I N

Ivan Vručina

Forenzička analiza operacijskog sustava Windows 11

ZAVRŠNI RAD

Varaždin, 2024.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

VARAŽDIN

Ivan Vručina

Matični broj: 0336037543

Studij: Primjena informacijske tehnologije u poslovanju

Forenzička analiza operacijskog sustava Windows 11

ZAVRŠNI RAD

Mentor/Mentorica:

Doc. dr. sc. Igor Tomičić

Varaždin, rujan 2024.

Ivan Vručina

Izjava o izvornosti

Izjavljujem da je moj završni izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Tema ovog rada je forenzička analiza operacijskog sustava Windows 11. Rad istražuje metode digitalne forenzike primijenjene na ovu verziju Windowsa, uključujući teorijski pregled digitalne forenzike, razvoj sustava i sigurnosne značajke Windowsa 11. Korišteni alati uključuju FTK Imager, Registry Viewer, Event Viewer, Volatility, ProcMon, BitLocker i druge. Praktični dio sadrži kratki vodič kroz ključne komponente Windows operacijskog sustava relevantne za forenzičku analizu. Provedena je forenzička analiza koja obuhvaća analizu Windows Registry-a, logova događaja, procesa, memorijskog dumpa i povijesti web preglednika, uz izradu forenzičkog izvještaja za provedenu analizu. Zaključci naglašavaju važnost forenzičkih metoda u analizi operacijskih sustava te pružaju smjernice za buduća istraživanja u digitalnoj forenzici.

Ključne riječi: Windows, Forenzička analiza, Registry, FTK Imager, Event Viewer, Windows 11, disk, Event Viewer, Volatility, Volatility Workbench, BitLocker, ProcMon, BrowsingHistoryView, WebBrowserPassView

Sadržaj

Sadržajiii
1. Uvod 1
2. Metode i tehnike rada 2
3. Digitalna forenzika
4. Windows
4.1. Windows 11
4.1.1. Trusted Platform Module (TPM)9
4.1.2. UEFI Secure Boot
4.1.3. Virtualization-based security (VBS)10
4.1.3.1. Windows Hypervisor10
4.1.3.2. Windows Credential Guard 11
4.1.3.3. Hypervisor-Enforced Code Integrity (HVCI)11
5. Vodič12
5.1. Windows Registry 12
5.1.1. UserAssist
5.1.2. NTUSER.DAT
5.2. Logovi događaja 17
5.3. Povijest preglednika
5.4. BitLocker
6. Forenzička analiza27
6.1. Prikupljanje podataka s diska27
6.2. Analiza artefakata 30
6.2.1. Analiza registra
6.2.1.1. NTUSER.DAT
6.2.1.2. SYSTEM
6.3. Analiza log-ova događaja
6.4. Analiza procesa
6.5. Analiza memorijskog dumpa 41
6.6. Analiza povijesti web preglednika 44
6.7. Pisanje forenzičkog izvještaja
6.7.1. Forenzički izvještaj
7. Zaključak61
Popis literature
Popis slika64

1. Uvod

Tema ovog završnog rada je forenzička analiza operacijskog sustava Windows 11. Materija koja se istražuje u ovom radu od velike je važnosti jer operacijski sustavi, uključujući najnoviju verziju Windowsa, igraju ključnu ulogu u svakodnevnom korištenju računala, kako u osobnom, tako i u profesionalnom okruženju. Forenzička analiza operacijskih sustava je od velike važnosti za otkrivanje, razumijevanje i rješavanje sigurnosnih incidenata te za prikupljanje digitalnih dokaza koji mogu biti ključni u pravnim postupcima.

Temu forenzičke analize operacijskog sustava Windows 11 odabrao sam zbog osobnog interesa za područje digitalne forenzike, kao i iz želje za dubljim razumijevanjem kako moderni operacijski sustavi funkcioniraju i kako se mogu analizirati u kontekstu forenzičkih istraga. Windows 11, kao najnovija verzija jednog od najčešće korištenih operacijskih sustava na svijetu, predstavlja idealan subjekt za ovu vrstu analize zbog svojih naprednih sigurnosnih značajki i široke primjene.

2. Metode i tehnike rada

Za izradu ovog završnog rada korištene su različite metode i tehnike kako bi se postigli postavljeni ciljevi i obuhvatila forenzička analiza operacijskog sustava Windows 11. Koristio sam online baze podataka poput Google Scholar-a i Google-a za prikupljanje relevantne literature i informacija koje su poslužile kao teoretska osnova rada. Alat Zotero korišten je za organizaciju i prikazivanje izvora unutar rada, omogućujući precizno i učinkovito upravljanje referencama. U praktičnom dijelu rada korišten je niz forenzičkih alata ključnih za prikupljanje i analizu digitalnih dokaza. Korišteni su i alati FTK Imager za izradu forenzičkih kopija diskova i drugih digitalnih medija, Registry Viewer za pregled i analizu Windows registra, Event Viewer za pregled Windows logova događaja, Volatility Workbench i Volatility za analizu memorijskog dumpa, ProcMon za praćenje i analizu procesa, BitLocker za analizu šifriranih diskova, te BrowsingHistoryView i WebBrowserPassView za analizu povijesti pregledavanja i lozinki spremljenih u web preglednicima.

3. Digitalna forenzika

Digitalna forenzika je dio forenzičke znanosti koji je usmjeren na istragu, oporavak i prezentaciju digitalnih dokaza u pravnim postupcima. [1] Digitalna forenzika je ključna za moderno provođenje zakona i kibernetičku sigurnost a počela se razvijati ranih 1980-ih zbog sve veće upotrebe osobnih računala i potrebe za izvlačenjem digitalnih podataka. Isprva fokusirana na računalni kriminal, digitalna forenzika proširila je svoj opseg s razvojem tehnologije, uključujući pametne telefone, internet i cloud platforme, zahtijevajući sofisticiranije metode za ekstrakciju i analizu podataka.

U početku su alati i tehnike bili osnovni što je ograničavalo učinkovitost istraga. S napretkom tehnologije, alati za digitalnu forenziku su postali napredniji što je značilo i poboljšanje metoda izdvajanja podataka, analize i dokumentacije. Evoluciju ovog polja potaknuli su i novi zakoni i propisi usmjereni na borbu protiv kibernetičkog kriminala koji naglašavaju važnost pouzdanih i sofisticiranih forenzičkih alata i metodologija. [2]

Digitalna forenzika se koristi u kriminalnim istragama, građanskim parnicama, obavještajnim operacijama, administrativnim poslovima, krađi intelektualnog vlasništva, industrijskoj špijunaži i stečajnim istragama. Njezini ciljevi uključuju obnavljanje, analizu i očuvanje digitalnih materijala za sudsku prezentaciju, utvrđivanje motiva i identifikaciju počinitelja. Digitalna forenzika se primjenjuje na mjestima zločina kako bi se očuvao integritet dokaza, uključujući prikupljanje podataka, dupliciranje i oporavak izbrisanih datoteka. Digitalna forenzika brzo identificira dokaze, procjenjuje utjecaj zlonamjernih aktivnosti i izrađuje forenzička izvješća uz očuvanje lanca nadzora. [1] Digitalna forenzika se, ovisno o uređaju ili sustavu koji sadrži digitalne dokaze, dijeli na nekoliko grana. Te grane uključuju računalnu forenziku, forenziku mobilnih uređaja, mrežnu forenziku i forenziku baza podataka.[3]

Zbog prirode dokazivanja u digitalnoj forenzičkoj znanosti, neophodno je poštivati rigorozne standarde. Među izazovima s kojima se susreće digitalna forenzika su izvlačenje podataka iz zaključanih ili uništenih računalnih uređaja, pronalaženje specifičnih unosa podataka unutar velikih količina podataka pohranjenih lokalno ili u cloud-u, praćenje digitalnog lanca nadzora i osiguravanje integriteta podataka tijekom istrage.[1]

Računalna forenzika obuhvaća pronalaženje i analizu digitalnih informacija s računala i uređaja za pohranu. Policijske i korporativne istrage digitalnih prijevara i kršenja internih pravila oslanjaju se na stručnjake računalne forenzike za prikupljanje dokaza kada dođe do zločina. U ovom području digitalne forenzike, podaci iz forenzike mreže i tvrdog diska koriste se u ispitivanju od strane osoblja za provođenje zakona, poslovnih rukovoditelja i sudova.[2]

Računalna forenzika i kibernetička sigurnost su vrlo bliska područja u polju informatike. Oba se fokusiraju na slične ciljeve, poput zaštite digitalne imovine i primjene strategija oporavka podataka za forenzičke svrhe, no unatoč sličnostima, svako područje ima svoje ključne razlike. Računalna forenzika se bavi analizom podataka koji su već kompromitirani ili ukradeni, dok se kibernetička sigurnost usredotočuje na sprečavanje krađe, prijevare i drugih oblika gubitka podataka.[4]

Budućnost digitalne forenzike usko je povezana s napretkom tehnologije, evolucijom pravnih okvira i rastućim kibernetičkim prijetnjama. Ključni trendovi u razvoju digitalne forenzike uključuju integraciju umjetne inteligencije i strojnog učenja, automatizaciju zadataka, prepoznavanje obrazaca i prediktivnu analitiku za anticipaciju prijetnji. Prilagodba cloud-u i Internet of Things okruženjima zahtijeva razvoj novih alata i tehnika za upravljanje složenim pravnim pitanjima. Blockchain tehnologija i kriptovalute donose izazove i prilike zbog potrebe za alatima koji prate transakcije i osiguravaju integritet dokaza. Kvantno računarstvo donosi i rizike i koristi te zahtijeva nove metode šifriranja. Pravna i etička pitanja zahtijevaju ravnotežu između temeljitih istraga i prava na privatnost, dok stalno usavršavanje vještina i interdisciplinarna obuka ostaju ključni za stručnjake u ovom polju.[2]

4. Windows

Microsoft Windows je operativni sustav razvijen za osobna računala koji se pojavio na tržištu 1985. godine. Windows je brzo postao dominantan na tržištu jer je nudio grafičko korisničko sučelje (GUI) za IBM računala. Danas oko 90 posto osobnih računala koristi neku verziju Windowsa. Prva verzija, temeljena na MS-DOS-u, omogućila je vizualno upravljanje radnim površinama. Kasnije verzije donijele su širu funkcionalnost uključujući ugrađene programe poput File Managera, Program Managera i Print Managera. Windows 95, objavljen 1995. godine, integrirao je Windows i DOS te dodao podršku za internet i web preglednik Internet Explorer.[5] Na slikama od 1. do 4. prikazana su korisnička sučelja Windows 95, Vista, 7 i 10.



Slika 1: Korisničko sučelje Windows-a 95 (Izvor: David Grossman, 2017)



Slika 2: Korisničko sučelje Windows-a XP (Izvor: Jo Best, 2014.)



Slika 3: Korisničko sučelje Windows-a 7 (Izvor: GFC Global, bez dat.)



Slika 4: Korisničko sučelje Windows-a 10 (Izvor: Michael Muchmore, 2022.)

Microsoft je 2001. godine predstavio Windows XP, koji je objedinio različite verzije za privatne korisnike , poslovne korisnike i programere. XP je predstavio bolju jezgru i poboljšano sučelje te naprednije upravljanje memorijom i aplikacijama. Windows Vista iz 2006. godine imao je problema s implementacijom i bio je percipiran kao spor i zahtjevan. Microsoft je 2009. odgovorio s Windows 7, koji je donio poboljšanja u brzini i zahtjevima sustava. Windows 8 iz 2012. godine imao je drugačije korisničko sučelje. Windows 10, objavljen 2015., uveo je digitalnog asistenta Cortanu i novi web preglednik Microsoft Edge. Windows 11, izdan 2021., karakteriziran je poboljšanim sučeljem i većom brzinom.[5]

4.1. Windows 11

Microsoft je 2021. predstavio Windows 11 koji je karakteriziran poboljšanim sučeljem i većom brzinom u radu u usporedbi s Windowsom 10. Međutim, Cortana je uklonjena iz OS-a zbog zaostajanja u performansama u usporedbi s konkurentnim virtualnim pomoćnicima poput Siri i Amazonove Alexe. Umjesto Cortane, Microsoft je uveo novu značajku nazvanu Copilot, koja koristi generativnu umjetnu inteligenciju (AI) kako bi se poboljšala produktivnost korisnika. kako bi generirao sadržaj na temelju korisničkih naredbi, Copilot koristi velike jezične modele inspirirane tehnologijom populariziranom od strane ChatGPT-a i Google Geminija. Ova

značajka integrirana je u aplikacije poput Microsoft 365, koji uključuje Word i PowerPoint, te Bing i u programsku traku sustava Windows.[5] Sučelje Windows-a 11 prikazano je na slici 5..



Slika 5: Korisničko sučelje Windows-a 11 (Izvor: Vlastita izrada, 2024.)

Microsoft tvrdi da je Windows 11 podigao sigurnosni baseline kako bi postao najsigurnija verzija do sad. Iskoristili su više od 8,2 trilijuna signala iz Microsoft threat intelligence, reverse engineering kao i savjete vodećih stručnjaka, poput NSA-a (National Security Agency), Nacionalnog centra za kibernetičku sigurnost Ujedinjenog Kraljevstva i Kanadskog centra za kibernetičku sigurnost, da bi dizajnirali security baseline u Windows 11 kako bi sustav mogao rješavati sve veće prijetnje s kojima se sam Windows 11 ne bi mogao boriti.[5] Neke od sigurnosnih značajki koje pomažu da podaci korisnika i operativni sustav ostanu zaštićeni su Virtualization-based security (VBS), UEFI Secure Boot i Trusted Platform Module (TPM). Neke od njih je potrebno aktivirati u BIOS-u da bi bilo moguće nadograditi s Windows 10 na Windows 11 i to je moguće vidjeti na slici 6..



Slika 6: Zahtjevi za nadogradnju na Windows 11 (Izvor: Rohan Pal, 2022.)

4.1.1.Trusted Platform Module (TPM)

Trusted Platform Module (TPM) je specijalizirana hardverska komponenta za povećanje sigurnosti u računalima. Može biti mikro kontroler na matičnoj ploči ili integriran u procesor (CPU). TPM koristi kriptografiju za sigurno pohranjivanje važnih informacija, poput lozinki, korisničkih podataka, otisaka prstiju i enkripcijskih ključeva, štiteći ih od vanjskih napada. Kao siguran kriptoprocesor, TPM integrira kriptografske ključeve u uređaje i nudi sigurnosne funkcije temeljene na hardveru. Nudi višu razinu sigurnosti jer pohranjuje kriptografske ključeve u hardver, čime su otporniji na neovlašteno mijenjanje i napade. TPM obavlja kriptografske funkcije poput generiranja ključeva, enkripcije i dešifriranja, podržavajući simetrične i asimetrične algoritme šifriranja. Tako osigurava da osjetljive informacije ostanu zaštićene i održava integritet i autentičnost platforme. Jedna od primarnih funkcija TPM-a je sigurno pohranjivanje kriptografskih ključeva, uključujući ključeve za šifriranje podataka i digitalne potpise. Također generira i sigurno pohranjuje dijelove enkripcijskih ključeva za osobna računala. Pri pokretanju računala, TPM igra ključnu ulogu u autentifikaciji, dajući kriptografski ključ za otključavanje enkriptanog diska. Ako je ključ potvrđen, sustav se normalno pokreće; u suprotnom računalo se neće pokrenuti, osiguravajući ovlašteni pristup i zaštitu sustava od prijetnji.[6]

Kao što je gore navedeno da bi se nadogradilo na Windows 11 potreban je TPM 2.0 koji za cilj ima podići sigurnosnu bazu Windows-a. TPM 2.0 omogućuje Windows-u da bude istinski operativni sustav bez lozinka, te time rješava phishing i druge napade koji se temelje na lozinkama.[7]

4.1.2.UEFI Secure Boot

UEFI Secure Boot je sigurnosna značajka koja je osmišljena za sprječavanje učitavanja neovlaštenog ili zlonamjernog softvera tijekom procesa pokretanja računala. Dio je UEFI firmware-a koji služi kao moderna zamjena za starije BIOS firmware sučelje. UEFI Secure Boot radi tako da koristi digitalne potpise kako bi se osiguralo da se samo pouzdani softver učitava tijekom boot proces. Svaki dio softvera, kao što je bootloader, kernel i upravljački programi, moraju imati priznati i pouzdani certifikat. UEFI firmware uključuje bazu podataka svih pouzdanih certifikata i hashova koji se koriste za provjeru digitalnog potpisa. Ako se potpis softvera podudara s certifikatom u bazi podataka firmware-a, dopušteno mu je pokretanje, u suprotnom je blokiran. Međutim, UEFI Secure Boot može predstavljati problem. Može uzrokovati probleme s kompatibilnošću s određenim operacijskim sustavima, upravljačkim programima ili starijim hardverom bez potpisanog firmware-a. Upravljanje ključevima i certifikatima može dodati složenost, posebno u poslovnim okruženjima. Osim

toga, napredni korisnici koji žele pokrenuti prilagođeni ili nepotpisani softver možda će morati onemogućiti Secure Boot, potencijalno smanjujući sigurnost.[8]

4.1.3. Virtualization-based security (VBS)

Virtualization-based security (VBS) koristi hardversku virtualizaciju za kreiranje i izoliranje sigurnog područja memorije od osnovnog operativnog sustava. Cilj je zaštititi operativni sustav i uređaj od zlonamjernog softvera i napada izolacijom procesa. VBS koristi Windows hypervisor za stvaranje izoliranog okruženja, omogućujući virtualizaciju hardvera i kreiranje virtualnih strojeva (VM) koji hostaju sistemske procese. Time se osigurava da napad na jedan proces ili aplikaciju ne može ugroziti druge aplikacije ili preuzeti kontrolu nad cijelim računalom.[9]

VBS izolira osjetljive informacije, otežavajući dohvaćanje ključnih podataka tijekom istrage. To može spriječiti analitičare u pristupu važnim dokazima unutar sigurnog okruženja VBS-a. Forenzički alati koji nisu dizajnirani za VBS mogu biti neučinkoviti, ostavljajući praznine u prikupljenim dokazima. VBS komplicira memory dump analizu, čineći standardne alate neučinkovitima u hvatanju zaštićenih regija. Potrebni su specijalizirani alati za pristup memoriji zaštićenoj VBS-om, što otežava forenzički proces. Također, izvođenje live response akcija na sustavima s VBS-om postaje izazovno jer zaštitne mjere ograničavaju izvršavanje naredbi i dohvaćanje podataka bez mijenjanja stanja sustava. Onemogućavanje VBS-a može ugroziti integritet istrage promjenom dokaza ili aktiviranjem zlonamjernog softvera.[10]

Ključne komponente VBS-a su **Hypervisor**, **HVCI** (Hypervisor-Enforced Code Integrity) i **Credential Guard.**

4.1.3.1. Windows Hypervisor

Windows Hypervisor služi kao temeljni sloj za omogućavanje VBS-a. On djeluje kao lagana, učinkovita iteracija hypervisora Hyper-V koji je izrađen posebno za upravljanje virtualnim strojevima i izoliranim okruženjima unutar operativnog sustava. Windows Hypervisor uspostavlja sigurno, izolirano područje memorije, odvojeno od općeg rada sustava, u kojem rad kritične sigurnosne usluge i osjetljivi podaci su zaštićeni. Iskorištavanjem hardverskih virtualizacijskih tehnologija kao što su Intel VT-x i AMD-V, učvršćuje izolirano okruženje, povećavajući otpornost na neovlašteno korištenje i time jača robusnost. Ovaj mehanizam

particioniranja djeluje kao bedem, štiteći osnovne komponente operativnog sustava od zlonamjernog softvera i sprječavajući napade koji žele iskoristiti ranjivosti kernela.[11]



Slika 7: Pojednostavljeni prikaz Hypervisora (Izvor: Jordan Macpherson, 2022.)

4.1.3.2. Windows Credential Guard

Windows Credential Guard je sigurnosna značajka koja služi kao obrana od prijetnji koje ciljaju identifikacijske podatke korisnika Windows-a. Izolira identifikacijske podatke kao što su hash lozinke NTLM, Kerberos ticket-granting tickets i druge tajne u sigurno područje memorije koje su nedostupne ostatku operativnog sustava. Ova izolacija pomaže kod sprečavanja napadača koji koriste uobičajene tehnike napada kao što su Pass-the-Hash ili Pass-the-Ticket gdje dobivaju pristup tokenima za autentifikaciju, te ih onda zloupotrebljavaju. Credential Guard osigurava da čak ako je i glavni operativni sustav ugrožen, identifikacijski podaci koisnika unutar izoliranog okruženja ostanu zaštićene, te to značajno smanjuje rizik lateralnog kretanja unutar mreže i neovlaštenog pristupa osjetljivim resursima.[12]

4.1.3.3. Hypervisor-Enforced Code Integrity (HVCI)

Hypervisor-Enforced Code Integrity (HVCI) je sigurnosna značajka koja koristi Windows Hypervisor za provođenje stroge kontrole integriteta koda. HVCI osigurava da se u kernel modu može izvršavati samo kod potpisan od pouzdanih autoriteta, sprječavajući time nepotpisan ili zlonamjeran kod. Provjerom integriteta koda, HVCI štiti sustav od malwarea i eksploatacija koje pokušavaju pokrenuti neovlašteni kod na najvišim razinama povlastica. Ova značajka pruža dodatni sloj obrane koji nadopunjuje druge sigurnosne mehanizme unutar operativnog sustava.[13]

Analitičarima može biti teško koristiti forenzičke alate na razini kernela koje HVCI ne prepoznaje te tako ograničava njihovu sposobnost dubinske analize. Zaobilaženje HVCI-ja je složeno i rizično jer može uključivati onemogućavanje sigurnosnih značajki i uništavanje dokaza. HVCI može blokirati prilagođene drivere koje forenzički alati koriste ako ne ispunjavaju njegove zahtjeve. Stoga analitičari moraju koristiti alate usklađene sa strogim sigurnosnim standardima HVCI-a, što može ograničiti izbor alata za istrage.

Zajedno, ove komponente rade usklađeno kako bi stvorile robusnu sigurnosnu arhitekturu koja značajno poboljšava zaštitu Windows 11. Ovakav višeslojni pristup pomaže ublažiti širok raspon sigurnosnih prijetnji i pruža sigurnije računalno okruženje za korisnike i poduzeća.

Zaobilaženje VBS-a i HVCI-a u forenzičke svrhe zahtijeva visoku specijalizaciju i rad s snažnim sigurnosnim mehanizmima. Neki softverski dobavljači nude forenzičke alate dizajnirane za rad u okruženjima zaštićenima VBS-om i HVCI-jem, koje operacijski sustav potpisuje i prepoznaje i tako omogućava rad bez onemogućavanja sigurnosnih značajki. Na primjer, Microsoftov Sysinternals Suite uključuje alate poput ProcDump-a i ProcMon-a za dubinsku analizu procesa i memorije. Certificirani forenzički alati usklađeni s HVCI standardima osiguravaju kompatibilnost i funkcionalnost. Kernel debugging alati, poput Windows Debugging Tools, pružaju duboke uvide u sustav i mogu raditi unatoč aktivnim VBS-u i HVCI-ju. Postavljanje debug veze preko serijske veze (USB ili mreža) ili korištenjem kernel debugging preko Ethernet-a omogućuje udaljeno debugging bez izravnog uplitanja u sustav.

5. Vodič

Ovaj sveobuhvatni vodič detaljno opisuje lokacije i značaj raznih forenzičkih artefakata u sustavu Windows 11, kao što su datoteke registra, logovi događaja i povijesti preglednika. Ovaj vodič služi kao vrijedan izvor forenzičkim istražiteljima koji analiziraju sustave Windows 11.

5.1. Windows Registry

Windows Registry je kritična komponenta Windows operativnih sustava, koja pohranjuje konfiguracijske postavke i opcije. To je centralizirana, hijerarhijska baza podataka koja upravlja resursima i pohranjuje konfiguracijske postavke za aplikacije u operacijskom sustavu Windows. Sadrži informacije, postavke i opcije za operativni sustav, instalirane aplikacije, usluge sigurnosnog računa, korisnička sučelja i drivere uređaja. Također pomaže u praćenju performansi sustava i dijagnosticiranju grešaka u sustavu. Forenzički istražitelji često analiziraju Registry kako bi otkrili dokaze o aktivnostima korisnika, konfiguraciji sustava i instaliranom softveru.[14]

Windows Registry podijeljen je na nekoliko logičnih odjeljaka koji se nazivaju košnice. Svaka košnica sadrži hijerarhiju ključeva i vrijednosti, slično mapama i datotekama. Primarne košnice koje su od interesa za forenzičku analizu su:

- HKEY_LOCAL_MACHINE (HKLM) sadrži lozinke, datoteke za pokretanje, datoteke za instalaciju softvera i sigurnosne postavke
- HKEY_CURRENT_USER (HKCU) sadrži postavke i konfiguracije specifične za korisnika
- HKEY_CLASSES_ROOT (HKCR) pohranjuje informacije o asocijacijama datoteka i postavkama povezivanja i ugrađivanja objekata (OLE)
- HKEY_USERS (HKU) Sadrži sve aktivno učitane korisničke profile na računalu
- HKEY_CURRENT_CONFIG (HKCC) sadrži informacije o hardverskom profilu koji koristi lokalno računalo pri pokretanju sustava

Unutar tih košnica nalazi se još mapa koje se nazivaju ključevi. Ključevi sadrže vrijednosti koje predstavljaju postavke. Postavke ključa su vrlo detaljne i sastoje se od brojeva i kodova. Za razliku od ključeva i vrijednosti, košnice se ne mogu kreirati, izbrisati ili preimenovati jer Registry Editor to ne dozvoljava. Microsoft ne sprječava da korisnik poboljša svoje računalo, nego nema potrebe da korisnik bilo šta radi sa košnicama. Ključevi i vrijednosti koji čine sve košnice je ono gdje je zapravo stvarna vrijednosti Windows registra. No, zato korisnik može dodavati, mijenjati i brisati ključeve i vrijednosti u registru.[15]

Da bi pronašli iznad navedene košnice potrebno je pokrenuti Registry Editor. On se pokreće na način da u tražilicu napišite "regedit" i odaberete Registry Editor, nakon toga Windows vas pita za dopuštenje i morate odabrati "Da", nakon toga se otvara prozor kao što je prikazano na slici 8.

Registry Editor				_	×
File Edit View Favorites Help					
Computer\HKEY_CLASSES_ROOT					
Computer Computer Computer HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_LOCAL_MACHINE HKEY_UCAL_MACHINE HKEY_USERS HKEY_CURRENT_CONFIG	Name	Type REG_SZ	Data (value not set)		

Slika 8: Sučelje Registry Editora (Izvor: Vlastita izrada, 2024.)

5.1.1. UserAssist

UserAssist je ključni forenzički artefakt unutar operacijskog sustava Windows koji pruža vrijedne informacije o aktivnostima korisnika na računalu. Ovi se podaci pohranjuju u Windows Registry i uključuju zapise o programima i aplikacijama koje je korisnik pokrenuo. UserAssist je ključ registra koji bilježi podatke o aplikacijama i programima koje pokreće korisnik. Windows Explorer ažurira ovaj ključ kad god se program pokrene, pohranjujući pojedinosti poput putanje programa, brojanja izvršenja i zadnjeg vremena izvršenja. U Windows registru UserAssist nalazi se pod putanjom " HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist", koja je prikazana na slici 9.[16]



Slika 9: Putanja do UserAssist u Windows Registry (Izvor: Vlastita izrada, 2024.)

Forenzički značaj UserAssist podataka leži u njegovoj sposobnosti da pruži detaljan uvid u aktivnost korisnika na Windows sustavu. Ispitivanjem unosa UserAssist-a, istražitelji mogu identificirati koje je programe i aplikacije korisnik pokrenuo, uključujući učestalost i vrijeme tih izvršavanja. Ove su informacije neprocjenjive za rekonstrukciju ponašanja korisnika i razumijevanje obrazaca aktivnosti, što može pomoći u prepoznavanju sumnjivih ili zlonamjernih radnji. Dodatno, podaci UserAssist-a mogu potkrijepiti druge oblike dokaza, kao što su vremena pristupa datotekama i zapisnici događaja, pružajući sveobuhvatniju sliku interakcije korisnika sa sustavom. To čini UserAssist ključnim artefaktom u forenzičkim istragama, osobito kada se prati neovlaštena upotreba softvera ili istražuju sigurnosni incidenti.[16]

5.1.2. NTUSER.DAT

U svakom korisničkom profilu nalazi se datoteka "**NTUSER.DAT**". Ova datoteka sadrži korisničke postavke, stoga nema potrebe da ju korisnik briše ili editira, jer Windows automatski učitava, mijenja i sprema ovu datoteku. Svaki put kada korisnik napravi neku promjenu na svojem računalu, bilo da se radi o promjeni rezolucije ili o promjeni bolje korisničkog sučelja, Windows mora zapamtiti te postavke kada se sljedeći put učita. On postiže tako da prvo te informacije pohrani u Registry, točnije u HKEY_CURRENT_USER košnicu. To znači da kada korisnik ugasi računalo, Windows tada sprema te informacije u datoteku koja se naziva "NTUSER.DAT". Te kada korisnik sljedeći puta upali računalo, Windows može učitati tu datoteku i postavke korisnika može ponovno učitati u Registry. To omogućuje da svaki profil na jednom računalu ima zasebne postavke. Da biste pronašli i pristupili datoteci, potrebno je otvoriti File Explorer, te napisati putanju do mape korisnika, kao što je prikazano na slici 10..[17]



Slika 10: Pretraživanje File Explorera do datoteke (Izvor: Vlastita izrada, 2024.)

ivanv	× +				—	
\leftrightarrow \rightarrow \uparrow (C 🖵 > This PC > Local Disk (C:)	> Users > ivan	ı >		Search ivanv	م
⊕ New ~ 🐰 0	[] [] [] [] [] [] [] [] [] [] [] [] [] [rt ~ 🔳 View ~				🕕 Details
A Home	Name	Date modified	Туре	Size		
	DpenVPN OpenVPN	13.5.2023. 18:51	File folder			
🗾 Gallery	Z Pictures	27.9.2023. 17:43	File folder			
	Saved Games	19.12.2023. 13:42	File folder			
🛄 Desktop 🛛 🖈	Searches	28.8.2023. 3:06	File folder			
🚽 Downloads 🖈	- venv	6.6.2023. 23:32	File folder			
📕 Documents 🏾 🖈 🛛	🗾 🗾 Videos	28.8.2023. 3:06	File folder			
🔀 Pictures 🛛 🖈	VirtualBox VMs	13.5.2023. 15:29	File folder			
🕖 Music 🛛 🖈	Zotero	24.5.2024. 18:05	File folder			
🗾 Videos 🛛 🖈	.recently-used.xbel	6.11.2022. 19:11	XBEL File	2 KB		
Counter-strike 2	NTUSER.DAT	24.5.2024. 2:11	DAT File	12.544 KB		
2024-04	Sti_Trace	31.10.2023. 11:40	Tekstni dokument	0 KB		I
31 items						

Slika 11: Pronalazak datoteke "NTUSER.DAT" (Izvor: Vlastita izrada, 2024.)

Nakon toga trebali bi pronaći datoteku. U slučaju da ju ne pronađete, potrebno je uključiti da se prikazuju skrivene stvari, kao što je prikazano na slici 12. Da biste mogli otvoriti datoteku potrebno je koristiti RegRipper, Registry Explorer ili FTK Imager alate.

ivanv	× +		– o x
← → ↑ C	💭 > This PC > Local Disk (::) > Users > ivanv >	Search ivanv Q
⊕ New ~ 🔏 🕻		Sort ~ 🗮 View ~ 🚥	🖪 Details
in Home	Name OpenVPN	Extra large icons Extra large icons Consequence Extra large icons folder	
🛄 Desktop 🛛 🖈	Saved Games	Medium icons folder Small icons folder	
🛓 Downloads 🖈	venv	≣≣ List folder	
📔 Documents 🖈 '	Videos VirtualBox VMs	E Details folder S= Tiles folder	
🕖 Music 🛛 🖈	Totero	8= Content folder	
🔀 Videos 🛷	recently-used.xbel	Details pane :L File 2 KB	
Counter-strike 2	NTUSER.DAT	Preview pane File 12.544 KB	
2024-04	Sti_Trace	Show > 🗸 🗔 Navigation pane	
31 items		*≣ Compact view	
		🕞 Item check boxes	
		🕒 File name extensions	
		✓	

Slika 12: Uključivanje postavke za prikazivanje skrivenih datoteka (Izvor: Vlastita izrada, 2024.)

Istražitelji mogu pronaći dokaze zlonamjerne aktivnosti unutar te datoteke, uključujući tragove zlonamjernog softvera i programa postavljenih za pokretanje pri pokretanju. Datoteka pomaže u stvaranju vremenske trake aktivnosti korisnika kroz vrijeme zadnjeg pisanja ključeva registra i pretpostavljena vremena prijave i odjave. Osim toga, sadrži internetsku povijest, kao što su postavke preglednika i povijest pregledavanja weba. Sve u svemu, datoteka je zlatni rudnik informacija u forenzičkim istragama, pružajući uvid u ponašanje korisnika, konfiguraciju

sustava i potencijalne sigurnosne incidente. Njegovi detaljni zapisi korisničkih postavki i aktivnosti čine ga neprocjenjivim resursom za rekonstrukciju radnji poduzetih na Windows računalu.

5.2. Logovi događaja

Logovi događaja ključne su komponente u forenzičkim istragama na Windows sustavima. Bilježe značajne događaje kao što su promjene sustava, sigurnosni incidenti, pogreške u aplikaciji i aktivnosti korisnika. Analizirajući log-ove događaja, forenzički istražitelji mogu rekonstruirati vremenski slijed događaja, otkriti neovlaštene radnje i razumjeti ponašanje korisnika i aplikacija u sustavu. Windows pohranjuje log-ove događaja u standardni format koji omogućuje jasno razumijevanje informacija. Glavni elementi log-a događaja su:

- Naziv
- Datum i vrijeme
- Kategorija zadatka
- ID događaja
- Izvor
- Razina
- Korisnik
- Računalo.[18]

Da biste pronašli log-ove događaja potrebno je otvoriti File Explorer, zatim u tražilicu napisati putanju do mape "Log", a putanja izgleda ovako "C:\Windows\System32\winevt\Logs". Nakon toga otvara se mapa koja izgleda kao na slici 13.

🗖 Logs	× +					- 0 ×
$\leftarrow \rightarrow \uparrow$	C	> Windows >	System32 > wi	nevt > Logs	Search Logs	٩
⊕ New × 🐰	பிடி திழை தி	rt ~ 🗮 View ~				🕕 Details
A	Name	Date modified	Туре	Size		
A Home	Microsoft-Windows-WinRM%4Operatio	28.4.2024. 13:47	Event Log	1.028 KB		
🗾 Gallery	Microsoft-Windows-WMI-Activity%4Op	28.4.2024. 13:47	Event Log	1.028 KB		
	Microsoft-Windows-WorkFolders%4WHC	28.8.2023. 5:49	Event Log	68 KB		
🛄 Desktop 🛛 🖈	Microsoft-Windows-WPD-ClassInstaller	18.10.2023. 1:57	Event Log	68 KB		
🚽 Downloads 🛛 🖈	Microsoft-Windows-WPD-MTPClassDriv	28.4.2024. 18:10	Event Log	68 KB		
📑 Documents 🖈	 B OAlerts	16.4.2024. 11:05	Event Log	1.028 KB		
🔀 Pictures 🛛 🖈	🛃 Security	25.5.2024. 12:35	Event Log	20.484 KB		
🕖 Music 🛛 🖈	🛃 Setup	27.4.2024. 13:33	Event Log	68 KB		
🔯 Videos 🛛 🖈	🛃 System	25.5.2024. 19:03	Event Log	17.476 KB		
🦰 Counter-strike 2 🖈	🛃 Visual Studio	28.8.2023. 5:49	Event Log	68 KB		1
2024-04	🛃 Windows PowerShell	14.5.2024. 12:08	Event Log	7.236 KB		I
176 items 1 item selected	20.0 MB					

Slika 13: Prikaz mape Logs (Izvor: Vlastita izrada, 2024.)

Na slici 14. prikazani su log-ovi događaja, u Event Viewer-u, koji prikazuju log-ove vezane za Security. Na primjer Log vezan za login i za specijalni login. Preko tog log-a možemo

Event Viewer							- 0	×
File Action View Help								
💠 🔿 🙍 📰 📓 📰								
Event Viewer (Local)	Security Numb	ber of events: 33.550					Actions	
> Custom Views	Level	Date and Time	Source	Event ID	sk Category		Security	
Windows Logs	() Information	25.5.2024.23:18:28	Micros	5379	er Account Management	111	Open Saved Log	
Saved Logs	(i) Information	25.5.2024. 23:16:01	Micros	5379	er Account Management		Treate Custom View	
Security	Information	25.5.2024. 23:15:16	Micros	4672	ecial Logon		Import Cuttom View	
🛗 Subscriptions	UInformation	25.5.2024. 23:15:16	Micros.	4624	igon			
	() Information	25.5.2024. 23:15:16	Micros	4672	ecial Logon		Y Filter Current Log	
	Information	25.5.2024. 23:15:16	Micros	4624	igon		Properties	
	() Information	25.5.2024, 23:12:59	Micros	5379	er Account Management		Pind	
		25.5.2024.23.07.22	Micros	5379	er Account Management		Save All Events As	
	() Information	25.5.2024. 23:07:22	Micros	5379	er Account Management		View	•
	() Information	25.5.2024. 23:07:22	Micros	5379	er Account Management		X Delete	
	(i) Information	25.5.2024. 23:07:22	Micros	5379	er Account Management		Bename	
	Information	25.5.2024. 23:07:22	Micros	5059	ther System Events			
	() Information	25.5.2024. 23:07:22	Micros	5061	stem Integrity		Ca Kerresh	
	() Information	25.5.2024. 23:07:22	Micros	5058	her System Events		2 Help	,
	() Information	25.5.2024. 23:07:22	Micros	5379	er Account Management		Event 4624, Microsoft Windows security auditing.	
	Defermation	23.3.2024. 23:07:22	Micros	5379	er Account Management		Event Properties	
	Information	25.5.2024. 23.07.22	Micros	5379	er Account Management		S. Com	
	() Information	25.5.2024. 23:07:21	Micros	5379	er Account Management			'
	(1) Information	25.5.2024. 23:07:21	Micros	5379	ier Account Management		hell save selected events	
	(i) Information	25.5.2024. 23:07:17	Micros	5379	er Account Management		G Refresh	
	Information	25.5.2024. 23:07:17	Micros	5379	er Account Management		Help	•
	() Information	25.5.2024. 23:07:17	Micros	5379	er Account Management			
	() Information	25.5.2024. 23:07:16	Micros	5379	er Account Management			
	() Information	25.5.2024, 23:07:16	Micros	5379	er Account Management			
	Information	25.5.2024. 23:07:16	Micros	23/9	er Account Management	_		
	Event 4024, Micro	osoft Windows security au	iating.			<u> </u>		
	General Detai	is						
	An account v	was successfully logged or	n.					
	Subject							
	Sec	urity ID: SY	STEM					
	Acc	ount Name: DE ount Domain: W	ESKTOP-KM4ICFI ORKGROUP	ES				
	Log Name	Security						
	Source:	Microsoft Windows	security Loga	ed:	5.2024. 23:15:16			
	Event ID:	4624	Task (Category:	pon			
	Level:	Information	Keyw	ords:	dit Success			
	User	N/A	Comp	puter:	SK70P-KM4ICFE			
	OpCode	Info						
	More Informat	tion: Event Log Online H	telp					
	1							

Slika 14: Prikaz log-ova u Event Viewer-u (Izvor: Vlastita izrada, 2024.)

vidjeti kada se korisnik ulogirao i kada se dodijelila specijalna prava računu. Pritiskom na željeni log, možemo vidjeti ime log-a, izvor, datum prijave, računalo, korisnik, id događaja i ostalo. Također postoje i log-ovi još za sustav, aplikacije, Powershell i slično. Na slici 15. i 16. prikazani su log-ovi događaja za sustav i aplikacije.

😹 Event Viewer										- 0	×
File Action View Help											
🗢 🔿 🙋 📰 📓 📷											
Event Viewer (Local)	System Number of	events: 32.080							Actions		
> Custom Views	Level		Date and Time		Source	Event ID	Task Category		System		
Applications and Services Lo	(1) Information		25.5.2024. 23:4	4:08	Service Control Manager	7040	None	11	🍯 Open Saved Log		
✓ I Saved Logs	(1) Information		25.5.2024. 23:4	11:31	Service Control Manager	7040	None		Create Custom View		
Application	A Warning		25.5,2024. 23:4	10:35	DistributedCOM	10016	None		Import Custom View		
Security	A Warning		25.5.2024. 23:4	10:34	DistributedCOM	10016	None				
System	(1) Information		25.5.2024. 22:4	15:53	Service Control Manager	7040	None		Filter Current Log		
23 Subscriptions	(1) Information		25.5.2024. 22:4	13:40	Service Control Manager	7040	None		Properties		
	A Warning		25.5.2024. 22:4	12:53	DistributedCOM	10016	None		🙀 Find		
	Warning		25.5.2024. 22:4	12:48	DistributedCOM	10016	None		Save All Events As		
	() Information		25.5.2024. 22:4 25.5.2024. 22:4	12:31	Service Control Manager Winlogon	7045	None (1101)		View		•
		-					(🗙 Delete		
	Event 1014, DNS Clier	nt Events						<u>×</u>	📑 Rename		
	General Details							- 1	G Refresh		
	Name resolution	for the name woad timed ou	t after none of the	configured DNS servers responded. Client PID	2768.				Help		•
									Event 1014, DNS Client Events		
								- 1	Event Properties		_
									R. Com		
									Cons Calendard Constants		
									Save selected Events		
									G Refresh		
									? Help		•
	Log Name:	System									
	Source	DNS Client Events	Logged:	25.5.2024. 22:41:54							
	Event ID:	1014	Task Category:	(1014)							
	Level:	Warning	Keywords:	(268435456)							
	User:	NETWORK SERVICE	Computer:	DESKTOP-KM4ICFE							
	OpCode	Info									
	More Information:	Event Log Online Help									
1											

Slika 15: Prikaz log-ova za sustav (Izvor: Vlastita izrada, 2024.)

😹 Event Viewer							- 0 ×
File Action View Help							
🗢 🔿 🙍 📰 📓 📰							
Event Viewer (Local)	Application Nu	umber of events: 29,210	Actions				
> G Custom Views	Level	Date and Time	Source	Event ID	Tesk Ca	Application	-
Applications and Services Lo	Information	26.5.2024. Q:18:56	Securit	16384	None	Open Saved Log	
✓ I Saved Logs	Information	26.5.2024. 0:18:25	Securit	16394	None	Y Create Custom View	
Application	() Information	25.5.2024. 23:44:34	Securit	16384	None	Import Custom View	
Security	Information	25.5.2024. 23:44:04	Securit	16394	None	Tilter Current Log-	
Subscriptions		25.5.2024. 23:09:07	Securit	16394	None	Properties	
	(1) Information	25.5.2024. 23:07:46	Securit	16384	None	20 Find	
	Information	25.5.2024. 23:07:16	Securit	1003	None	Stun All Eventr Ar	
	(i) Information	25.5.2024. 23:07:16	Securit	1003	None	E Street and the state	
	Information	25.5.2024. 23:07:15	Securit	16394	None	view	,
	Event 16384, Seco	urity-SPP			×	X Delete	
	Court au					E Rename	
	Detail	15				G Refresh	
	Successfully	scheduled Software Protecti	on service for n	re-start at 2	124-05-01722:18:56Z. Resson: RulesEngine.	2 Help	•
						Event 16384, Security-SPP	-
						Event Properties	
						Big Copy	•
						Save Selected Events	
						G Refresh	
						7 Help	
							,
	Log Name:	Application					
	Sources	Security-SPP	Logge	ed:	26.5.2024. 0:18:56		
	Event ID:	16384	Task C	ategory:	None		
	Level	information	Keywo	ords:	LMSSIC		
	User:	N/A	Comp	outer:	DESK (UP-KMBR, PE		
	More laforma	tion: Event Los Online Hel	h.				
	More morma	con: Event Log Online He	1				

Slika 16: Prikaz log-ova za aplikacije (Izvor: Vlastita izrada, 2024.)

Kao što je moguće vidjeti na slikama iznad, postoji više vrsta logova kao što su sigurnosni, aplikacijski i sistemski. Sigurnosni logovi bilježe događaje koji se odnose na sigurnosne aspekte sustava. To uključuje prijave korisnika, pokušaje pristupa resursima, promjene u sigurnosnim postavkama i neuspjele pokušaje autentifikacije. Sigurnosni logovi su ključni za praćenje i analiziranje potencijalnih sigurnosnih prijetnji. Primjeri događaja u sigurnosnim logovima uključuju prijave i odjave korisnika, bilo uspješne ili neuspješne. Također, evidentiraju se promjene u korisničkim privilegijama ili dozvolama. Logovi bilježe i aktivnosti povezane s enkripcijom ili izmjenom sigurnosnih politika. Osim toga, pristupi zaštićenim datotekama ili resursima također su zabilježeni u ovim logovima. Logovi su često prvi izvor informacija kada se istražuju sigurnosni incidenti, kao što su pokušaji probijanja lozinki, neovlašteni pristupi ili promjene u postavkama sigurnosti. [19]

Aplikacijski logovi bilježe aktivnosti specifičnih aplikacija koje se izvršavaju na sustavu. Ovi logovi su korisni za praćenje funkcioniranja aplikacija, dijagnosticiranje problema, praćenje performansi i razumijevanje ponašanja aplikacija. Primjeri događaja u aplikacijskim logovima uključuju greške u aplikacijama, kao što su rušenja ili iznimke, promjene u konfiguraciji aplikacija, upite prema bazi podataka i njihove rezultate, te korištenje specifičnih funkcionalnosti unutar aplikacije. Koriste se za dijagnostiku problema u aplikacijama, optimizaciju performansi i analizu kako korisnici koriste aplikaciju. Oni su ključni za razvojne inženjere i sistemske administratore kada se pojave problemi s aplikacijama.[19]

Sistemski logovi prate aktivnosti operativnog sustava i njegove komponente. Oni obuhvaćaju informacije o pokretanju i gašenju sustava, radu drivera, greškama hardvera i općim operativnim događajima. Primjeri događaja u sistemskim logovima uključuju pokretanje i gašenje operativnog sustava, što omogućava praćenje rada računala. Također, evidentira

pokretanje, zaustavljanje ili padovi sistemskih servisa, što je ključno za održavanje stabilnosti sustava. Hardverske greške, poput problema s diskom ili memorijom, također su zabilježene u logovima kako bi se olakšalo prepoznavanje i rješavanje tih problema. Uz to, sistemski logovi bilježe instalaciju i ažuriranje sistemskih komponenti, što je važno za održavanje sigurnosti i funkcionalnosti sustava. [19]

Log-ovi događaja bogat su izvor forenzičkih podataka koji bilježe širok raspon aktivnosti sustava i korisnika. Analizirajući te zapisnike, forenzički istražitelji mogu otkriti dokaze o neovlaštenom pristupu, promjenama sustava, problemima s aplikacijama i ponašanju korisnika. Razumijevanje strukture, uobičajenih ID-ova događaja i alata za analizu zapisa događaja ključno je za provođenje temeljitih i učinkovitih forenzičkih istraga na Windows sustavima.

5.3. Povijest preglednika

Povijest preglednika kritična je komponenta u forenzičkim istragama, koja nudi uvid u online aktivnosti korisnika. Ovi podaci uključuju posjećene web stranice, upite za pretraživanje, preuzimanja i druge interakcije temeljene na webu. Analiza povijesti preglednika može pomoći istražiteljima da razumiju ponašanje korisnika, identificiraju potencijalne sigurnosne incidente i prikupe dokaze o nezakonitim aktivnostima.[20]

Povijest preglednika bilježi posjećene web stranice, upite za pretraživanje i preuzete datoteke. Ove informacije omogućuju forenzičkim istražiteljima da rekonstruiraju online aktivnosti korisnika, pružajući uvid u njegove radnje, interese i obrasce ponašanja. Analiza povijesti može otkriti posjete sumnjivim ili zlonamjernim web stranicama, što može ukazivati na pokušaje krađe identiteta, pristup nedopuštenom sadržaju ili izloženost zlonamjernom softveru. Ovo je posebno korisno u odgovoru na incident, gdje je ključno razumjeti početni vektor kibernetičkog napada. [21]

U pravnim istragama, povijest preglednika može poslužiti kao uvjerljiv dokaz na sudu. Ona može pokazati korisnikovo znanje, namjere i radnje, što može biti kritično u kaznenim i građanskim slučajevima. Ispravno prikupljena i dokumentirana povijest preglednika može pomoći u utvrđivanju vremenskih okvira, potvrđivanju alibija te opovrgnuti ili poduprijeti tvrdnje uključenih strana. [21]

Google Chrome, razvijen od strane Googlea, jedan je od najpopularnijih preglednika, kompatibilan sa svim platformama. Chrome nudi integraciju sa Google uslugama, sinkronizaciju lozinki, širok raspon dodataka, proširenja i anonimni način rada. U IT-u artefakti su tragovi na računalu koji pomažu u identifikaciji zlonamjernog prometa i napada. Chrome pohranjuje ove artefakte u specifične mape unutar operativnog sustava, uključujući povijest

navigacije, podatke automatskog dovršavanja, bookmarkove, informacije o dodacima, cache podatke, informacije o prijavama korisnika, podatke unesene u web-obrasce, favikone, podatke o sesiji, minijature i favorite.[20]

Postoji puno artefakata koje Chrome pohranjuje a u nastavku biti će prikazane lokacije par artefakata koje se mogu pregledati tijekom forenzičke istrage na Chrome-u:

- C:\Users\UserName\AppData\Local\Google\Chrome\User Data\Default\Historyputanja do datoteke koja sadrži povijest pretraživanja, povijest navigacije i preuzimanja
- C:\Users\UserName\AppData\Local\Google\Chrome\User Data\Default\Bookmarks putanja do datoteke koja sadrži bookmark korisnika
- C:\Users\UserName\AppData\Local\Google\Chrome\User Data\Default\Login Dana putanja do datoteke koja sadrži podatke o prijavama

					—	
Default	× +					
← → ↓ C	🖵 > … Local > Google >	Chrome > Use	er Data > Default		Search Default	م
(†) New - 🔏 🗘	ῗ @) & Ū ∿ Sor	t ~ 🛛 🗮 View ~				Details
A Home I	Name	Date modified	Туре	Size		
	🧧 Google Profile Picture	4.4.2024. 0:31	PNG File	3 KB		
	🧿 Google Profile	25.5.2024. 22:42	ICO File	193 KB		
	heavy_ad_intervention_opt_out	8.8.2022. 15:04	Data Base File	16 KB		
Desktop 📌	heavy_ad_intervention_opt_out.db-journal	8.8.2022. 15:04	DB-JOURNAL File	0 KB		
Uownloads 📌	History	27.5.2024. 16:32	File	144.704 KB		
🖹 Documents 🖈	History-journal	27.5.2024. 16:32	File	0 КВ		
🔀 Pictures 🛛 🖈	InterestGroups	27.5.2024. 14:35	File	1.632 KB		
🕖 Music 🔹 🖈	InterestGroups-iournal	27.5.2024. 14:35	File	0 KB		
🔀 Videos 🛛 🖈		27.5 2024 14:25	File	20 10		
🗖 Counter-strike 2 🖈	- NANONYMILYSERVICE	27.3.2024. 14:55	riie	20 KD		I
	KAnonymityService-journal	27.5.2024. 14:35	File	0 KB		
2024-05	Поск	8 8 2022 15-04	File	0 KR		

Slika 17: Putanja do datoteke History (Izvor: Vlastita izrada, 2024.)

× +				_	
🖵 > … Local > Google >	Chrome > User [Data > Default		Search Default	Q
Ĩì &] & Ū́i ∿ Son	rt ~ 🗮 View ~				Details
Name	Date modified	Туре	Size		
Affiliation Database-journal	27.5.2024. 9:39	File	0 KB		
AggregationService	27.5.2024. 14:32	File	68 KB		
AggregationService-journal	27.5.2024. 14:32	File	0 KB		
Bookmarks	27.5.2024. 16:27	File	1.180 KB		
Bookmarks.bak	26.5.2024. 1:17	BAK File	1.179 KB		
BrowsingTopicsSiteData	22.9.2023. 15:47	File	28 KB		
BrowsingTopicsSiteData-journal	22.9.2023, 15:47	File	0 KB		'
BrowsingTonicsState	22 5 2024 0-32	File	2 KB		
	26.5.2024 1.10	Data Rasa Fila	160 KB		
	20.3.2024. 1:18	Data base File	100 KB		
CdmStorage.db-journal	26.5.2024. 1:18	DB-JOURNAL File	0 KB		
Conversions MB	27 5 2024 14:35	File	352 KR		
	× + □ > ···· Local > Google > □ ● ···· Local > Google > □ ● ···· Local > Google > □ ● ···· □ 1 Sor Name - ···· ···· Sor Name - ···· ···· Sor AggregationService - ···· ···· ···· AggregationService - ···· ···· ···· Bookmarks BrowsingTopicsSiteData ···· ···· ···· BrowsingTopicsSiteData ···· ···· ···· ···· BrowsingTopicsSiteData ···· ···· ···· ···· CdmStorage ···· ···· ···· ···· ···· Conversions ···· ···· ···· ···· ···· ···· O ···· ···· ···· ···· ···· ···· ····	× + □ > ···· Local > Google > Chrome > User II □ > ··· Local > Google > Chrome > User II □ ● ● ● ● A Sort × = View × Name Date modified 27.5.2024.9.39 4 4 4 4 4.32 4 4.32 4 4 4.32 4 4.32 4 4.33 4.33 4.33 4.33 4.33 4.3	× + □ > ··· Local > Google > Chrome > User Data > Default □ ··· Image: Chrome > User Data > Default Image: Chrome > ··· ··· ··· ··· Name Image: Chrome > View > ··· ··· Name Image: Chrome > View > ··· ··· Affiliation Database-journal 27.5.2024. 14:32 File ··· AggregationService 27.5.2024. 14:32 File ··· Bookmarks 27.5.2024. 14:32 File ··· Bookmarks.bak 26.5.2024. 11:2 File ··· BrowsingTopicsSiteData 22.9.2023. 15:47 File ··· BrowsingTopicsSiteData 22.9.2023. 15:47 File ··· BrowsingTopicsSiteData 22.5.2024. 1:18 Data Base File CdmStorage 26.5.2024. 1:18 Data Base File CdmStorage.db-journal 26.5.2024. 1:18 DB-JOURNAL File	× + □ > ··· Local > Google > Chrome > User Data > Default > □ • • □ • • □ • • □ • • □ • • • • •<	× + Search Default Search Default □ > • • Search Default □ • • • • Name Date modified Type Size Affiliation Database-journal 27.5.2024. 9.39 File 0 KB AggregationService 27.5.2024. 14:32 File 68 KB AggregationService 27.5.2024. 14:32 File 0 KB Bookmarks 27.5.2024. 14:32 File 0 KB Bookmarks 27.5.2024. 14:32 File 0 KB Bookmarks 22.5.2024. 14:32 File 0 KB Bookmarks 22.5.2024. 14:32 File 1.180 KB Bookmarks 22.5.2024. 12 File 1.180 KB BrowsingTopicsSiteData 22.9.2023. 15:47 File 0 KB BrowsingTopicsSiteData 22.9.2023. 15:47 File 0 KB BrowsingTopicsSiteData 22.5.2024. 0:32 File 2 KB BrowsingTopicsSiteData 26.5.2024. 1:18 Data Base File 160 KB CdmStorage 26.5.2024. 1:18 DB-JOURNAL File

Slika 18: Putanja do datoteke Bookmarks (Izvor: Vlastita izrada, 2024.)

Default	× +				_	o x
← → ↑ C	· ↓ ··· Local > Google >	Chrome > User I	Data > Default	>	Search Default	۹
⊕ New × 🔏 🗘	î @ @ Ū ∿ so	rt ~ 🗮 View ~				🕕 Details
🔥 Home 🔰	Name	Date modified	Туре	Size		
	KAnonymityService-journal	27.5.2024. 14:35	File	0 KB		
	LOCK	8.8.2022. 15:04	File	0 KB		
	LOG	26.5.2024. 12:38	File	0 KB		
E Desktop 📌	LOG.old	25.5.2024. 22:42	OLD File	0 KB		
🚽 Downloads 🖈	Login Data	27.5.2024. 13:48	File	320 KB		
📑 Documents 🖈	Login Data For Account	13.12.2023. 12:24	File	52 KB		
🔀 Pictures 🛛 🖈	Login Data For Account-iournal	13.12.2023. 12:24	File	0 KB		
🕗 Music 🛛 🖈	Login Data-iournal	27.5.2024, 13:48	File	0 KB		
🗾 Videos 🛛 🖈	MediaDeviceSalts	27 5 2024 16:25	File	52 KB		
🚞 Counter-strike 2 🖈	MediaDeviceSalta	27.5.2024, 16:25	F11-	J2 KB		
2024-05	WediaDeviceSaits-journal	27.3.2024. 16:25	File	0 KB		
107 items 1 item selected 320	Network Action Predictor KB	27.5.2024. 16:27	File	1.024 KB		

Slika 19: Putanja do datoteke Login Data (Izvor: Vlastita izrada, 2024.)

Povijest preglednika vitalni je artefakt u forenzičkim istragama zbog mogućnosti da pruži detaljne i kontekstualne uvide u online aktivnosti korisnika. Rekonstruiranjem online ponašanja, identificiranjem zlonamjernih radnji, razumijevanjem namjere korisnika, potkrepljivanjem drugih dokaza i praćenjem krađe podataka, povijest preglednika igra ključnu ulogu u otkrivanju istine i podržavanju pravnih postupaka. Učinkovita analiza povijesti

preglednika ključna je forenzičkim istražiteljima za izgradnju sveobuhvatnih i pouzdanih slučajeva.

5.4. BitLocker

BitLocker je sigurnosna funkcija integrirana u Microsoft Windows koja šifrira sve tvrde diskove, uključujući operativni sustav, sistemske datoteke i korisničke podatke. Cilj šifriranja je zaštita osjetljivih podataka na računaru od neovlaštenog pristupa, krađe ili napada hakera. BitLocker se često koristi u kombinaciji s TPM-om, hardverskim čipom ugrađenim u mnoge moderne računala, koji omogućava sigurno pohranjivanje kriptografskih ključeva. BitLocker koristi TPM za provjeru autentičnosti sustava prije pokretanja operativnog sustava, čime se osigurava integritet šifriranih podataka. Kada se BitLocker aktivira, on šifrira sve datoteke pohranjene na tvrdim diskovima, pretvarajući ih u nečitljiv kod koji se može dešifrirati samo pomoću određenog ključa. Ovaj ključ za šifriranje može se otključati pomoću korisničke lozinke ili pametne kartice. BitLocker koristi napredni enkripcijski standard (AES) sa 128-bitnim ili 256-bitnim ključevima, koji je prepoznat kao jedan od najsigurnijih algoritama za šifriranje. Dodatno, BitLocker je osmišljen da besprijekorno funkcionira s drugim značajkama Windowsa, kao što su Microsoft Management Console, Group Policy i Active Directory. [22]

BitLocker sučelje otvara se pomoću Windows tražilice te se nakon toga otvara prozor prikazan na slici 20.

RitLocker Drive Encry		o x
$\leftrightarrow \rightarrow \vee \uparrow$	Image: System and Security > BitLocker Drive Encryption > C Search Control Panel > C	
Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.	0
	Operating system drive	
	C: BitLocker off	
	Turn on BitLocker	
	Fixed data drives	
	Local Disk (D:) BitLocker off	
	New Volume (V:) BitLocker off	
	Removable data drives - BitLocker To Go	
See also	ZAS (H:) BitLocker off	
 TPM Administration Disk Management Privacy statement 	Turn on BitLocker	

Slika 20: Sučelje Bitlocker-a (Izvor: Vlastita izrada, 2024.)

Nakon otvaranja prozora, prikazane su nam particije nad kojima je moguće koristiti BitLocker. U našem slučaju koristiti ćemo particiju H: koja je zapravo prijenosni disk. Nakon odabira particije otvara nam se prozor u kojem možemo odlučiti kako ćemo nakon šifriranja otvarati disk, što je prikazano na slici 21.

~	Real BitLocker Drive Encryption (H:)	×
	Choose how you want to unlock this drive	
	Use a password to unlock the drive	
	Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.	
	Enter your password	
	Reenter your password	
	Use my smart card to unlock the drive	
	You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.	
	Next Cancel	

Slika 21: Odabir otvaranja diska (Izvor: Vlastita izrada, 2024.)

U ovom slučaju odabrati ćemo lozinku koja će biti "Test1234!" i nakon upisivanja lozinke otvara se novi prozor u kojem je moguće odabrati kamo će se spremiti ključ za oporavak, što je moguće vidjeti na slici 22.



Slika 22: Odabir spremanja ključa za oporavak (Izvor: Vlastita izrada, 2024.)

Ako se odlučimo na drugu opciju tada će se ključ spremiti u datoteku na odabrano mjesto. Te će datoteka izgledati kao na slici 23.



Slika 23: Datoteka s ključem za oporavak (Izvor: Vlastita izrada, 2024.)

Nakon što smo BitLocker uključili, kada bismo disk željeli otvoriti na drugom računalo, pojavila bi se obavijest o nemogućnosti pristupa disku i bilo bi potrebno unijeti lozinku kao što je prikazano na slikama 24. i 25.



Slika 24: Obavijest o nemogućnosti pristupa disku (Izvor: Vlastita izrada, 2024.)



Enter password to unlock this drive.



Slika 25: Prozor za unos lozinke (Izvor: Vlastita izrada, 2024.)

BitLocker predstavlja izazov za forenzičku analizu jer šifrira sve podatke na disku, čineći ih nedostupnima bez odgovarajućeg ključa za dešifriranje, kao što su Recovery Key, TPM modul ili PIN. Ključevi za dešifriranje mogu se nalaziti na različitim mjestima, poput TPM modula, USB sticka, ili u Microsoftovom oblaku, što često zahtijeva suradnju s vlasnikom sustava ili sudski nalog kako bi se do njih došlo. U slučajevima kada je računalo aktivno i BitLocker već dešifrirao disk, istražitelji imaju priliku pristupiti podacima. Međutim, ova vrsta analize mora biti izvedena brzo i precizno, jer ponovno pokretanje sustava ili gubitak napajanja može rezultirati gubitkom pristupa. Budući da su BitLocker ključevi često pohranjeni u RAM-u, istražitelji mogu pokušati doći do njih analizom memorije, ali ovo zahtijeva specijalizirane alate i tehnike koje nisu uvijek pouzdane. Neki komercijalni forenzički alati, poput EnCase ili FTK, nude mogućnosti rada s BitLocker šifriranim diskovima, ali samo ako istražitelj već ima odgovarajuće ključeve za dešifriranje. No, čak i tada su mogućnosti alata često ograničene na situacije u kojima su ključevi dostupni.[22]

Pristupanje šifriranim podacima bez dozvole vlasnika može biti ilegalno, stoga je uvijek važno osigurati da posjedujete odgovarajuće dozvole ili naloge za pristup takvim podacima. U mnogim zemljama postoji zakonska obaveza zaštite privatnosti korisnika, što znači da prilikom pristupanja šifriranim podacima morate poduzeti sve potrebne mjere kako biste zaštitili osjetljive informacije. Pristup šifriranim podacima nosi sa sobom veliku odgovornost. Trebalo bi raditi isključivo u interesu zaštite podataka i privatnosti, izbjegavajući bilo kakve radnje koje bi mogle narušiti povjerenje korisnika. S obzirom na to da šifriranje podataka često služi zaštiti od zloupotrebe, etički je važno ne zloupotrijebiti pristup tim podacima.

6. Forenzička analiza

U ovom dijelu rada provest će se forenzičku istragu na sustavu Windows 11 u fiktivnom slučaju neovlaštenog dijeljenja povjerljivih informacija. Ovaj proces uključuje tri glavne faze: prikupljanje podataka, analizu artefakata i pisanje izvješća. Cilj je pružiti praktičan uvid u forenzički proces i istaknuti osobitosti rukovanja Windows 11 sustavima.

Scenarija je da tvrtka sumnja da je zaposlenik odavao povjerljive informacije konkurenciji. Zaposlenikovo računalo sa sustavom Windows 11 zaplijenjeno je radi forenzičke analize. U nastavku biti će prikazani postupci koji se koriste u forenzičkoj analizi, a to su prikupljanje podataka s diska koristeći adekvatne alate, analiza registra sustava i logo-va događaja, na kraju napraviti kratki izvještaj o ovoj forenzičkoj analizi.

6.1. Prikupljanje podataka s diska

Prikupljanje podataka kritičan je korak u forenzičkoj istrazi. Uključuje snimanje bit-pobit kopije medija za pohranu kako bi se osigurala točna replika izvornih podataka. Ovaj proces osigurava očuvanje cjelovitosti dokaza, a izvorni podaci ostaju nepromijenjeni. Forenzičku sliku diska, nad kojim ćemo napraviti lažnu forenzičku analizu, kreirati ćemo s alatom FTK Imager. FTK Imager je jedan od najboljih alata za kreiranje slika tvrdih diskova nad kojima se želi napraviti forenzička analiza.

Da bismo napravili sliku diska osumnjičenog potrebno je u FTK Imager preko File → Create Disk Image napravimo sliku željenog diska, kao što je prikazano na slici 26.



Slika 26: Kreiranje slike diska (Izvor: Vlastita izrada, 2024.)

Nakon toga, otvara nam se prozor koji nas pita koja je vrsta izvora dokaza. Postoje fizički disk, logički disk, slikovna datoteka, sadržaj mape ili CD/DVD. U našem slučaju disk nad kojim radimo forenzičku analizu je USB stick i on je fizički, kao što je prikazano na slici 27.

Select Source	×
Please Select the Source Evidence Type	
Physical Drive	
O Logical Drive	
O Image File	
 Contents of a Folder (logical file-level analysis only; excludes deleted, unallocated, etc.) 	
Femico Device (multiple CD/DVD)	
< Back Next > Cancel Help	

Slika 27: Odabir vrstu izvora dokaza (Izvor: Vlastita izrada, 2024.)

Zatim iskače prozor u kojem trebamo odabrati za koji disk želimo napraviti sliku i odabiremo u našem slučaju USB stick. Nakon odabira diska pojavljuje se prozor, prikazan na slici 28., na kojem trebamo odabrati mapu u kojoj će se spremiti slika.

Nakon pritiska na gumb "Add" otvara se novi prozor u kojem je potrebno odabrati kojeg tipa da slika bude, mi ćemo odabrati E01 jer izvorno podržava kompresiju te to obično rezultira da je slikovna datoteka manje veličine.[23].

Nakon upisivanja informacija o slici, pojavljuje se novi prozor kod kojeg je potrebno odabrati u koju mapu želimo da se dijelovi slike spreme i pod kojim nazivom. I nakon što smo sve prethodne korake odradili, vraćamo se na prozor sa slike 28., ali je sada dodana mapa za spremanje slike i moguće je sada pokrenuti stvaranje slike diska, tj. u našem slučaju USB stick-a osumnjičenog.

Create Image		×
Image Source		
\\. \PHYSICALDRIVE0		
Image Destination(s)	Starting Evidence Number: 1	
Add	Edit Remove]
 Verify images after the Create directory listings 	y are created Precalculate Progress Statistics of all files in the image after they are created Start Cancel	

Slika 28: Pokretanje stvaranje slike diska (Izvor: Vlastita izrada, 2024.)

Nakon kreiranja slike diska, moguće je vidjeti dijelove slike u mapi koju smo sami odabrali. Nakon toga je moguće sliku pokrenuti na drugom računalu bez da smo u riziku da originalne podatke promijenimo ili obrišemo. Da bi se dodala nova kreirana slika USB stick-a potrebno je ići na File \rightarrow Image Mounting i odaberemo prvi dio slike koju smo kreirali i odaberemo da je podatke moguće samo pregledavati zbog toga jer se radi o istrazi. Postupak je prikazan na slici 29.

Mount Image To Dr	ive		×
Add Image Image File:			
E: \AnalizaF\Anali	za.E01		
Mount Type:	Physical & Logical	~	
Drive Letter:	Next Available (G:)	~	
Mount Method:	Block Device / Read Only	~	

Slika 29: Montiranje novo kreirane slike (Izvor: Vlastita izrada, 2024.)

Nakon uspješnog montiranja slike, u File Exploreru moguće je vidjeti da je Windows dodijelio novu particiju. Kada ju otvorimo možemo vidjeti da su podaci isti kao i na originalnom disku, što je prikazano na slici 24. Jedina razlika je u tome da u novo dodijeljenoj particiji nije moguće dodavati ili mijenjati datoteke zbog toga što smo to odredili kod montiranja slike, to znači da možemo otvarati datoteke, mape i aplikacije isto kao što bi i na originalnom disku samo što je ovako sigurnije raditi s podacima jer nema rizika da bismo mogli naštetiti istrazi. Sada možemo vidjeti je li korisnik na ovom disku pohranio neke informacije koje je potencijalno

mogao odati nekom izvan tvrtke. Također u alatu FTK Imager možemo dodati montiranu sliku kao "Evidence Item" i tada možemo vidjeti neke datoteke koje je osumnjičeni obrisao, a prethodno nam nisu bile vidljive. To je vidljivo na slici 30..

🦰 [root]	× +			- 🗆 X	📫 ESC	D-USB (H:)	× +			- 0 X
← → ↑ C	🖵 > This PC > Removable D	isk (F:) > [root] >			÷		🖵 🔸 This PC	> ESD-USB (H:) >		
⊕ New ~ 🔏 🕡	(๊) @) @ î∳ s	ort ~ 🔳 View ~		📑 Details	🕀 Net	•• × @		© 1↓ Sort ∽	≣ View ~	📑 Details
🧰 analiza	Name	Date modified	Туре	Size		Name		Date modified	Type S	ize
🚞 desktop	🚞 boot	26.7.2023. 19:24	File folder			🚞 boot		26.7.2023. 17:24	File folder	
	🧰 efi	26.7.2023. 19:24	File folder		•	🧰 efi		26.7.2023. 17:24	File folder	
🗸 💻 This PC	Carl Primjer 1	27.2.2024. 16:03	File folder			🧰 Primjer 1		27.2.2024. 14:03	File folder	
> ៉ Local Disk (C:)	sources	26.7.2023. 19:25	File folder			sources		26.7.2023. 17:25	File folder	
> 👝 Local Disk (D:)	🚞 support	26.7.2023. 19:40	File folder		•	support		26.7.2023. 17:40	File folder	
> 👝 Local Disk (E:)	System Volume Information	26.7.2023. 19:24	File folder			🔊 autorun		5.5.2023. 19:24	Informacije o post	
> 🗂 Removable Disk (F	autorun 📄	5.5.2023. 21:24	Informacije o post		~ I	🗋 bootmgr		5.5.2023. 19:24		405 KB
> 👝 Removable Disk (C	📄 bootmgr	5.5.2023. 21:24		405 KB		🗋 bootmgr.efi		5.5.2023. 19:24		1.536 KB
> 📫 ESD-USB (H:)	📄 bootmgr.efi	5.5.2023. 21:24		1.536 KB		🧿 OsnovnaSredstvaP	opis Imovine	22.2.2024. 14:24	Chrome HTML Do	744 KB
New Volume (V-)	OsnovnaSredstvaPopis Imovine	22.2.2024. 16:24	Chrome HTML Do	744 KB		📑 Posel		27.2.2024. 14:03	OpenDocument T	722 KB
14 items					13 items	1				

Slika 30: Prikaz podataka kod montirane slike i originalnog diska (Izvor: Vlastita izrada, 2024.)

Kod prikupljana podataka na Windows 11 moguće je naići na neke poteškoće jer je Windows 11 uveo nekoliko novih značajki i promjena koje mogu utjecati na forenzičku analizu. Jedna od tih značajka je BitLocker koji je često omogućen i on šifrira cijeli disk radi zaštite podataka od neovlaštenog pristupa. Praktičan uvid bi bio da za disk koji je šifriran od strane BitLocker-a nabavimo ključeve za šifriranje. Ključevi se mogu dobiti od korisnika, IT odjela poduzeća ili putem Active Directory-a ako je stroj pridružen domeni.

Također jedna od značajka Windows-a 11 je Standby koji održava sustav u stanju niske potrošnje energije dok održava mrežnu povezanost. Praktičan uvid bi bio da on može ometati forenzičko snimanje tako što bi stavio uređaj u stanje niske potrošnje energije. Jedna od radnji bila bi da deaktiviramo tu značajku ili da pokušamo sustav održati budnim uz pomoć nekih postavki ili alata.

6.2. Analiza artefakata

Analiza artefakata ključna je faza u forenzičkim istragama u kojima se ispituju digitalni dokazi kako bi se otkrile relevantne informacije o korisničkim aktivnostima, događajima u sustavu i potencijalnim zlonamjernim aktivnostima

6.2.1. Analiza registra

Analiza registra uključuje ispitivanje Windows registra, koji sadrži vrijedne informacije poput aktivnosti korisnika, konfiguracije sustava i pojedinosti o instaliranim programima.

Prilikom provođenja analize registra ključno je usredotočiti se na ključne košnice. NTUSER.DAT košnica sadrži podatke specifične za korisnika, uključujući nedavne datoteke i
naredbe Run. Košnica SYSTEM pruža detalje o konfiguraciji sustava i povezanim uređajima. SOFTWARE košnica otkriva informacije o instaliranim aplikacijama i postavkama sustava.

6.2.1.1. NTUSER.DAT

Za početak ćemo na računalu osumnjičenog preko alata FTK Imager dobiti zaštićene datoteke tako da ćemo na karticu "File" → "Obtain Protected Files" i te datoteke ćemo spremiti u određenu mapu. Nakon što se operacija izvela u odabranoj datoteci možemo naći zaštićene datoteke, što je prikazano na slici 31..

analiza	× +				_	
$\leftarrow \rightarrow \lor C$	\square > This PC > Local Disk (D:)	> analiza >			Search analiza	
⊕ New ~ 🔏 🖸	[î A] & îi î\ Sort	~ 🔳 View ~				🕕 Details
ivrucina20	Name	Date modified	Туре	Size		
	Contraction of the second seco	18.7.2024. 14:36	File folder			
👻 💻 This PC	🗋 default	5.7.2024. 18:37	File	1.792 KB		
> 陆 Local Disk (C:)	SAM	5.7.2024. 18:37	File	128 KB		
> 📥 Local Disk (D:)	SECURITY	5.7.2024. 18:37	File	32 KB		
> 👝 Local Disk (E:)	📄 software	13.7.2024. 2:08	File	131.840 KB		
> 👝 Removable Disk (F:)	📄 system	5.7.2024. 18:37	File	21.760 KB		
> 📫 ESD-USB (H:)	userdiff	28.8.2023. 0:28	File	8 KB		
> 👝 New Volume (V:)						
> 📫 ESD-USB (H:)						
> Removable Disk (F-) 7 items						

Slika 31: Prikaz dobivenih zaštićenih datoteka (Izvor: Vlastita izrada, 2024.)

Da bismo našli željenu datoteku NTUSER.DAT potrebno je ući u mapu Users i tada odabrati korisnika koji je prijavljen na računalu i tada možemo pronaći željenu datoteku NTUSER.DAT, što je prikazano na slici 32..

🚞 ivanv	× +				_		×
← → ↑ C	☐ → This PC → Local Disk (D:) →	> analiza > Users	> ivanv >		Search ivanv		
⊕ New ~ 🔏 🕡	[ີ @] & Ū N Sort ∽	≡ View ~ ····				📑 De	tails
🚞 ivrucina20	Name	Date modified	Туре	Size			
	🚞 Crypto	18.7.2024. 14:36	File folder				
🗸 💻 This PC	Protect	18.7.2024. 14:36	File folder				
> ៉ Local Disk (C:)	NTUSER.DAT	16.7.2024. 1:33	DAT File	14.592 KB			
> 🗂 Local Disk (D:)	UsrClass.dat	16.7.2024. 1:33	DAT File	11.520 KB			
> 🚍 Local Disk (E:)							
> 👝 Removable Disk (F:)							
> 📫 ESD-USB (H:)							
> 👝 New Volume (V:)							
> 📫 ESD-USB (H:)							
Aitems							

Slika 32: Putanja do datoteke NTUSER.DAT (Izvor: Vlastita izrada, 2024.)

Za pregledavanje datoteke NTUSER.DAT koristiti ćemo alat Registry Viewer. Kada otvorimo datoteku u alatu dobiti ćemo različite mape koji sadrže različite ključeve s

vrijednostima koje zapravo predstavljaju postavke i vremena zadnje uporabe pojedine aplikacije, što je prikazano na slici 33..

AccessData Registry Viewer (Demo Mode) - [NTUSER.DAT]				-	o x
File Edit Report View Window Help					- 8 ×
🛸 🛢 🖻 🖛 🖻 🖻 🖻 🗰 📦 🏅					
□	Name	Туре	Data		
AppEvents	<pre>user_experience_metrics.sta</pre>	REG_DWORD	0x00000000 (0)		
Console					
Environment					
EUDC					
E Carlo Carl					
Microsoft					
Printers					
Software					
👜 🧰 System					
Uninstall					
Last Written Time 16 7 2024 15:20:10 UTC					
Last written nime 10.7.2024, 13:39:10 01C					
					-
NTUSER.DAT	1		Offset: 0		

Slika 33: Prikaz mape koje sadrži NTUSER.DAT (Izvor: Vlastita izrada, 2024.)

U datoteci prvo ćemo pronaći UserAssist mapu koja sadrži vrijednosti koje zapravo govore što je osumnjičeni točno radio, koje programe je koristio, u koje vrijeme i slično. Da bismo došli do mape UserAssist potrebno je otvoriti mapu Software/Microsoft/Windows/CurrenVersion/Explorer/UserAssist, kao što je prikazano na slici 34..



Slika 34: Prikaz mape UserAssist u Registry Viewer (Izvor: Vlastita izrada, 2024.)

Zatim možemo u jednim od mapa pronaći kada je osumnjičeni zadnji puta otvorio određenu aplikaciju, na primjer u našem slučaju možemo vidjeti kada ja osumnjičeni zadnji put otvorio aplikaciju Discord. Na slici 35. možemo vidjeti da je aplikacija Discord bila pokretana dva puta i da je zadnji put otvorena 17.7.2024. u 23:49:09 UTC. Te tako možemo vidjeti za većinu aplikacija.

File Edit Report View Window Help Image:	- Troe Data	Ξ×
2 3 8 m B 2 8 8 0 m 0 ?	Troe Data	
	Type Data	
Image: StuckRects3 Name: StuckRects3 Image: StuckRects3 StuckRects3 I	bitsg.Jvaqbjf.FuryyRk. REG_BINARY 80 00 00 00 00 00 00 00 00 00 00 00 00 0	•
Value Name ROTT3 com.squirrel.Discord.Discord		
Time 177,2024, 23:49:09 01C		
		v

Slika 35: Prikaz ključa koji sadrži vrijednosti zadnjeg otvaranja aplikacije Discord (Izvor: Vlastita izrada, 2024.)

Također možemo u mapi Softver/Valve/Steam pronaći kada se osumnjičeni zadnji puta prijavio u aplikaciju Steam i to s kojim korisničkim imenom, koju igru je kada pokrenuo i slično, prikazano na slici 36.

AccessData Registry Viewer (Demo Mode) - [NTUSER.DAT]			- (×
🖽 File Edit Report View Window Help				- 0	5 ×
🖆 💂 🗈, 📭 🕑 🗉 🖻 🔰 💷 🕪 🏌					
	Name BLanguage BStermFe BStermPath StopprestAut6fun ERanningAptD BBapticuterAforeground BSoureAtIontaliBath BSoureAtIontaliBath BStatesdyStatedOfflineMode BAutesdyStateAdOfflineMode BAutesdyStateAdOfflineMode BAutesdyStateAdOfflineMode BAutesdyStateAdOfflineMode BAutesdyStateAdOfflineMode BAutesdyStateAdOfflineMode BAutesdyStateAdOfflineMode BAutesdyStateAdOfflineMode BAutesdyStateAdOfflineMode BStateAdodeStipp BStateModeStipp BStateModeStipp BStateModeStipp	Type REG_5Z REG_5Z REG_5Z REG_5WORD REG_0WORD REG_0WORD REG_0WORD REG_0VCRD REG_0VCRD REG_0VCRD REG_0VCRD REG_0VCRD REG_0VCRD REG_2Z REG_0VCRD REG_2Z REG_2Z	Data english c/program files (x86)/steam/steam.ore c/program files (x86)/steam/steam.ore h.c0000000 (th) h.c0000000 (th) h.c000000 (th) h.c0000000 (th) h.c0000000 (th) h.c000000 (th) h.c000000 (th) h.c0000000 (th) h.c000000 (th) h.c0000000 (th) h.c000000 (th) h.c000000 (th) h.c0000000 (th) h.c0		
🗄 Key Properties	0 65 00 6E 00 67 00 6C 0	0-69 00 73 00	68 00 00 00 e n g l i s h · · ·		
Last Witten Time 1572004, 22:55:29 UTC					•
NTUSER.DAT\Software\Valve\Steam	Offs	rt: 0			14

Slika 36: Prikaz podataka za prijavu na aplikaciji Steam (Izvor: Vlastita izrada, 2024.)

6.2.1.2. SYSTEM

Na slici 37. možemo vidjeti da postoje i ostale datoteke koje možemo otvoriti u Registry Viewer-u i u nastavku ćemo otvoriti datoteku SYSTEM. Ona se u alatu otvara isto kao i prethodna NTUSER.DAT datoteka. Kada ju otvorimo u njoj možemo pronaći podatke o konfiguraciji sustava. Na slikama 37. i 38. možemo saznati koju verziju Windows-a je osumnjičeni koristio, s kojom email adresom je prijavljen na Microsoft rač i koju verziju BIOSa i model matične ploče računalo koristi.

AccessData Registry Viewer (Demo Mode) - Invstem]			
File Edit Depart View Window Hale			
Carrie Edit Report View Window Help			
💌 🖥 🖻 🖛 🗎 🔍 🕾 🖻 🖬 🖬 👗			
ResourceManager	Name	Туре	Data
Registrars	BaseBuildRe	REG_DWORD	0x00000001 (1)
ResourcePolicyStore	BuildBranch	REG_SZ	vb_release
RNG	ab BuildGUID	REG SZ	fffffff-ffff-ffff-ffff-ffffffffffff
Select	ab BuildLab	REG SZ	19041.vb_release.191206-1406
Setup	BuildLabEx	REG_SZ	19041.1.amd64fre.vb_release.191206-1406
AllowStart	ab Compositio	REG SZ	Enterprise
	ab CurrentBuild	REG SZ	19044
EirrtPaat	ab CurrentBuild	REG SZ	19044
Image Based Setup	CurrentMajo	REG DWORD	0x0000000A (10)
MoSetun	CurrentMin	REG DWORD	0x0000000 (0)
Pid	ab Current Type	REG SZ	Multiprocessor Free
Service Reporting API	ab CurrentVersi	REG SZ	6.3
SetupCl	BigitalProdu	REG_BINARY	A4 00 00 03 00 00 00 30 30 33 33 30 2D 38 30 30 30
- 🔄 Snapshot	B DigitalProdu	REG_BINARY	F8 04 00 00 04 00 00 00 30 00 33 00 36 00 31 00 32 00 2
	(ab) DisplayVersion	REG_SZ	21H2
🗊 🧰 Status	ab EditionID	REG_SZ	Professional
🛊 🧰 Timers	b EditionSub	REG_SZ	(value not set)
👜 🦲 Upgrade	EditionSubst	REG_SZ	(value not set)
Software	EditionSubV	REG_SZ	(value not set)
B- State	b]InstallationT	REG_SZ	Client
Waas	👸 InstallDate	REG_DWORD	0x62F1009F (1659961503)
H-L WPA	👸 InstallTime	REG_QWORD	0x E2CCF662 (16342708048618892065)
	ab) PathName	REG_SZ	C:\Windows
Key Properties	and Productid	REG_SZ	00330-80000-00000-AA221
Last Written Time 27.8.2023. 22:44:02 UTC	DeroductName	REG_SZ	Windows 10 Pro
	BegisteredO	REG_SZ	(value not set)
	RegisteredO	REG_SZ	ivan.vrucina2000@gmail.com
	ab Released	REG_SZ	2009
	(ab) Software Type	REG_SZ	System
	(ab) SystemRoot	REG_SZ	C:\WINDOWS
	UBR UBR	REG_DWORD	0x0000C0E (3086)
	MigrationSc	REG_DWORD	0x00000005 (5)
1			

Slika 37: Prikaz ključeva u mapi SYSTEM (Izvor: Vlastita izrada, 2024.)

🔯 AccessData Registry Viewer (Demo Mode) - [system	1]				-		
File Edit Report View Window Help						- 8	×
🛎 📕 🖻 🖛 🗃 🗑 🗑 🖉 🚳 🖗 👂 🌹							
Boytem Bytem Bytem Bytem Bytem Bytem ControlSet01 DriveDatabase DriveDatabase HardwareConfig HardwareConfig HardwareConfig Bytem Bytem	Name III LatUse SystemBiosV SystemFamu SystemFamu SystemFred BySystemFord BioSVendor	7ppe REG_DWORD REG_BINARY REG_MULT_SC REG_MULT_SC REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ REG_SZ	Data 0x0000000 (0) 40 D6 19 C5 19 B5 D5 A O1 4450A - 1072009 P5.60 American Megatrends - 500 0x00000003 (3) To Be Filled By O.E.M. To Be Filled By O.E.M. To Be Filled By O.E.M. American Megatrends Inc. P5.60 ASRock B459 Pro4 10/20 2022 To Be Filled By O.E.M. 0x0000000 (0)				
B Key Properties Last Written Time 13.7.2024.11642:39 UTC ysterm/HardwareConfig/(0559a.18-de9-0000-0000-000 13.7.2024.11642:39 UTC	00 42 00 34 00 10 34 00 00 00) 35 00 30 00-:)	10 00 50 00 72 00 6F 00 8 4 5 0 · .P.≖.o. 4 · .	Offret: 0			•

Slika 38: Prikaz ključeva o matičnoj ploči (Izvor: Vlastita izrada, 2024.)

Kroz mapu SYSTEM moguće je vidjeti koju vrstu monitora je osumnjičeni koristio, koju svu ostalu periferiju, koju vrstu diskova za pohranu je koristio i koji su sve prijenosni diskovi bili priključeni na računalo i slično. To sve se može vidjeti na slikama 39. i 40..



Slika 39: Vrsta monitora koju je osumnjičeni koristio (Izvor: Vlastita izrada, 2024.)



Slika 40: Svi korišteni diskovi za pohranu (Izvor: Vlastita izrada, 2024.)

Temeljitim analiziranjem mape SYSTEM, možemo otkriti kritične dokaze o stanju sustava i radnjama koje se na njemu izvode, što može značajno pridonositi ukupnoj forenzičkoj istrazi.

6.3. Analiza log-ova događaja

Logovi događaja su ključni izvor informacija u forenzičkim istragama jer oni bilježe sistemske, sigurnosne i aplikacijske događaje tako što daju vremensku traku aktivnosti koje mogu biti ključne za razumijevanje onoga što se dogodilo na sustavu osumnjičenoga.

U nastavku prikazati ću nekoliko primjera koje smo pronašli na sustavu osumnjičenog. Prvi primjer, prikazan na slici 41., vezan je uz sigurnosne događaje koji nam prikazuje kada je osumnjičeni zadnji puta upalio računalo i kada se zadnji puta prijavio na sustav. Na slici 42. moguće je vidjeti da je sustav osumnjičenog bio u stanju mirovanja skoro 16 sati.

rent Viewer							
Action View Help							
* * 📰 🛛 📷							
vent Viewer (Local)	Security Number of even	ate: 33 741					
Custom Views	Security runniber of even	10.00.741					
Windows Logs	Keywords	Date	and Time		Source	Event ID	Task Category
Application	Audit Success	16.7.3	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
Security	Audit Success	16.7.3	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
E Setup	Audit Success	16.7.3	024. 18:05:56		Microsoft Windows security auditing-	5379	User Account Management
System	Audit Success	16.7.3	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
Forwarded Events	Audit Success	16.7.2	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
Applications and Services Lo	Audit Success	16.7.3	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
Saved Logs	Audit Success	16.7.2	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
Subscriptions	Audit Success	16.7.2	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
	Audit Success	16.7.2	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
	Audit Success	16.7.3	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
	Audit Success	16.7.3	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
	Audit Success	16.7.2	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
	Audit Success	16.7.2	024. 18:05:56		Microsoft Windows security auditing.	5379	User Account Management
	Audit Success	16.7.3	024. 18:05:56		Microsoft Windows security auditing.	4672	Special Logon
	Audit Success	16.7.2	024. 18:05:56		Microsoft Windows security auditing.	4624	Logon
	Audit Success	16.7.2	024. 18:02:16		Microsoft Windows security auditing.	5382	User Account Management
	Audit Success	16.7.3	024. 18:02:02		Microsoft Windows security auditing.	5382	User Account Management
	Audit Success	16.7.3	024. 18:00:50		Microsoft Windows security auditing.	4672	Special Logon
	Audit Success	16.7.1	024. 18:00:50		Microsoft Windows security auditing.	4624	Logon
	Audit Success	16.7.2	024. 17:59:11		Microsoft Windows security auditing.	5379	User Account Management
	Audit Success	16.7.3	024.17:59:11		Microsoft Windows security auditing.	5379	User Account Management
	An account was succes Subject: Security ID: Account Nam Account Nam Logon ID: Logon Information:	sfully logged on. e: SYSTEM e: DESKTOP-KI MORKGROL 0x3E7	A4ICFES P				
	Logon Type Restricted Adv Remote Crede Virtual Accour Log Name: Sect Source Mit Event ID: 462- Level: Info User: N/A OaCode: Info	nin Mode - Initial Guard: - Int: No unity rosoft Windows security 4 rrmation	Logged: Task Category: Keywords: Computer:	16.7.2024. 18:00:50 Logon Audit Success DESKTOP-KMAICFE			
	More Information: Eve	nt Log Online Help					
	more information:	un sard Unline melp					

Slika 41: Prikaz događaja za prijavu u sustav (Izvor: Vlastita izrada, 2024.)

Re Everir Alemen										
File Action View Help										
++ 2 📰 🖬 🔟										
Event Viewer (Local)	System Number of events: 38.285 (!) New e	vents available								
> Ustom Views	Level	Date and Time	Source	Event ID Task Category						
Application	A Warning	16.7.2024 17:39:05	DNS Client Events	1014 (1014)						
Security	A Information	16.7.2024.17/39/02	Power-Troubleshoater	1 None						
Setup	(i) Information	16.7.2024, 17:39:02	Kernel-Power	566 (268)						
System	(1) Information	16.7.2024. 17:39:01	Kernel-Power	566 (268)						
Forwarded Events	Error	16.7.2024. 17:39:01	VBoxNetLwf	12 None						
> Applications and Services Lo	(1) Information	16.7.2024. 17:39:01	Kernel-Boot	32 (58)						
> 🏥 Saved Logs	(i) Information	16.7.2024. 17:39:01	Kernel-Boot	18 (57)						
Subscriptions	(i) Information	16.7.2024. 17:39:01	Kernel-Boot	30 (21)						
	(1) Information	16.7.2024. 17:39:00	EventLog	6013 None						
	(1) Information	16.7.2024. 17:39:00	Kernel-General	1 (5)						
	(1) Information	16.7.2024. 1:33:14	Kernel-Power	107 (102)						
	(i) Information	16.7.2024. 1:33:11	Kernel-Power	42 (64)						
	(1) Information	16.7.2024. 1:33:09	Kernel-Power	566 (268)						
	(1) Information	16.7.2024. 1:33:09	Kernel-Power	187 (243)						
	(1) Information	16.7.2024. 1:33:09	Winlegon	7002 (1102)						
	(i) Information	16.7.2024. 1:20:08	Service Control Manager	7040 None						
	A Warning	16.7.2024. 1:20:04	DistributedCOM	10016 None						
	A Warning	16.7.2024. 1:19:56	DistributedCOM	10016 None						
	A Warning	16.7.2024, 1:19:46	DNS Client Events	1014 (1014)						
	(i) Information	16.7.2024. 1:19:43	Service Control Manager	7045 None						
	(i) Information	16.7.2024. 1:19:41	Winlegon	7001 (1101)						
	Event 1, Power-Troubleshooter									
	General Details									
	The sectors has a firmed from a large									
	The system has returned from a low power state.									
	Sleep Time: 2024-07-15T23:33:09.83063110 Wake Time: 2024-07-16T15:39:01.9526640	00Z 00Z								
	THE RELEASE THE CALL AND A DECEMBER OF A DECEMBER									
	Wake Source: Unknown									
	Log reame: System									
1	E Causan Davies Traublacka ata	Logged: 16.7.2024, 17:39:02								
	source: Power-indubieshoote									
	Event ID: 1	Task Category: None								
	Event ID: 1 Level: Information	Task Category: None Keywords:								
	Event ID: 1 Level: Information User: LOCAL SERVICE	Task Category: None Keywords: Computer: DESKTOP-KM4ICFE								
	Event ID: 1 Event ID: 1 Level: Information User: LOCAL SERVICE OpCode: Info	Task Category: None Keywords: Computer: DESKTOP-KM4ICFE								
	Event ID: 1 Level: Information User: LOCAL SERVICE	Task Category: None Keywords: Computer: DESKTOP-KM4ICFE								

Slika 42: Prikaz događaja za mirovanje sustava (Izvor: Vlastita izrada, 2024.)

Na drugom primjeru, prikazanom na slici 43. možemo vidjeti da je osumnjičeni zbog nepoznatih razloga uklonio disk 4 i disk 3.

🚺 Event Viewer							
File Action View Help							
🗢 🔿 🙍 📰 📓 📷							
Event Viewer (Local)	System Number of events	: 38.287					
> 🔤 Custom Views	Lauri	Date and Te				Event ID	Tech Catagoon
Vindows Logs	Distantia	10 7 2024 10	13.50		ania Castal Manager	Event ID	Nee-
Application	Disformation	18.7.2024. 15	42:30	3	ervice Control Manager	7040	None
Security	Warning	10.7.2024. 19	40:33	а Г	ervice Control Manager	10015	None
Secup	A Warning	18.7.2024. 15	39:13		Natility and COM	10016	None
E Forwarded Events	warning	10.7.2024.15	44-02		Vindour/Indate/Tient	10	Windows Undate Agent
> Applications and Services Lo	Information	10.7.2024.10	44:00		Vindows0pdateClient	43	Windows Update Agent
> Saved Logs	Information	10.7.2024.10	43:30	· · · · · · · · · · · · · · · · · · ·	VindowsUpdateClient	CP AA	Windows Update Agent
Subscriptions		18.7.2024 16	29-26		enice Control Manager	7040	None
		18.7.2024 16	36.08		enice Control Manager	7040	None
		18 7 2024 17	42:03		ernel-Dower	566	(268)
		18 7 2024 17	30-35		arnal-Power	566	(258)
	A Warning	18 7 2024 17	30-23		INS Client Events	1014	(1014)
	A Warning	18.7.2024 16	45-43		ink chan crans	157	None
	AWaming	18.7.2024 16	38-25	6	lick	157	None
	(i) Information	18.7.2024 1	29-21	S	ervice Control Manager	7040	None
	() Information	18.7.2024, 15	27:01	5	ervice Control Manager	7040	None
	A Warning	18.7.2024. 15	26:04		listributedCOM	10016	None
	Warning	18.7.2024, 15	26:04	-	listributedCOM	10016	None
	(i) Information	18.7.2024, 15	25:40	s	ervice Control Manager	7040	None
	(1) Information	18.7.2024, 15	22:55	s	ervice Control Manager	7040	None
	(i) Information	18.7.2024. 14	56:20	N	Itfs (Microsoft-Windows-Ntfs)	98	None
	Event 157. disk						
	General Details						
	Disk 4 has been surprise	removed.					
	Log Name: Syste	m					
	Source: disk	Logged:	18.7.2024. 16:38:25				
	Event ID: 157	Task Categor	/: None				
	Level: Warn	ing Keywords:	Classic				
	User: N/A	Computer:	DESKTOP-KM4ICFE				
	OpCode: Info						
	More Information: Even	t Log Online Help					
	NUT						

Slika 43: Prikaz događaja za uklanjanje diska (Izvor: Vlastita izrada, 2024.)

I na slici 44. moguće je vidjeti da je osumnjičeni brisao i instalirao nekoliko aplikacija.

🛃 Event Viewer									
File Action View Help									
🗢 🔿 🙍 📰 🖬									
Event Viewer (Local)	Application Number								
> Custom Views	Level		Date and Time		Source		Event ID	Tark Category	
Vindows Logs	Distantian		10 7 2024 16-4	105	Boulet Annual		10000	Mana	1
Application	Deformation		19.7.2024.164	2003	Susteen Portose		9216	Nene	
Security	Deformation		10.7.2024.1004	204	System Nestore		1040	None	
Sustem	Deformation		19.7.2024. 164	1.2.4	Milortaller		1040	None	
Forwarded Events			18.7.2024, 16:4	1.34	Milostaller		11707	None	
> C Applications and Services Lo	Dinformation		18.7.2024, 16:4	1:32	RestartMananer		10001	None	
> 👸 Saved Logs	Deformation		18.7.2024, 16.4	1:32	Msilpstaller		1042	None	
5 Subscriptions	(1) Information		18,7,2024, 16:4	1:31	RestartManaper		10000	None	
	(i) Information		18.7.2024, 16:4	1:31	System Restore		8216	None	
	(i) Information		18.7.2024. 16:4	1:31	Msilnstaller		1040	None	
	(1) Information		18.7.2024, 16:4	1:14	RestartManager		10001	None	
	(1) Information		18.7.2024. 16:4	1:14	Msilnstaller		1042	None	
	(i) Information		18.7.2024. 16:4	1:14	Msilnstaller		1034	None	
	Information		18.7.2024. 16:4	1:14	Msilnstaller		11724	None	
	(i) Information		18.7.2024. 16:4	1:12	RestartManager		10000	None	
	Information		18.7.2024. 16:4	611	System Restore		8216	None	
	Information		18.7.2024. 16:4	611	Msilnstaller		1040	None	
	Information		18.7.2024. 16:33	3:11	RestartManager		10001	None	
	Information		18.7.2024. 16:32	2:59	RestartManager		10000	None	
	Information		18.7.2024. 16:13	3:55	ESENT		330	General	
	Information		18.7.2024. 16:13	3:55	ESENT		326	General	
	Event 11724, Msilnstal	ler							×
	General Details								
	Death at Assess	to FTV Income Removal on	enalsted successf		 				
	Produce Accessua	ta Fikimager kemoval co	mpieted successi	uny.					
	Log Name:	Application							
	Source:	Msilnstaller	Logged:	18.7.2024. 16:41:14					
	Event ID:	11724	Task Category:	None					
	Level	Information	Keywords:	Classic					
	Usec	DESKTOP-KMICEE\ivany	Computer	DESKTOP-KM4ICEE					
	OnCode	Info	a service a						
	More Information:	Event Log Online Ideln							
	more an ormation	aron any solute nep							

Slika 44: Prikaz događaja za brisanje aplikacije (Izvor: Vlastita izrada, 2024.)

Uz prethodne logove događaja, prikazati ću još i par sigurnosnih i sistemskih logova. Na slici 45. prikazan je sigurnosni log koji prikazuje da je 1. 9. 2024. bilo neuspješnog pokušaja prijave na račun.

🐻 Event Viewer				
File Action View Help				
🔶 🏟 🙎 📰 📓 🛅				
🛃 Event Viewer (Local)	Security Number of events: 33.213 () New events available		
> 🚔 Custom Views	Kaunada	Data and Taxa	6	Event ID Test Colorese
🗸 🙀 Windows Logs	Reywords	Date and Time	source	Event ID lask Category
Application	HAUDIT Failure	2.9.2024. 16:09:38	Microsoft Windows security auditing.	5038 System Integrity
e Security	Mudit Failure	1.9.2024. 20:04:12	Microsoft Windows security auditing.	4625 Logon
Setup	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	53/9 User Account Management
System	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	53/9 User Account Management
Applications and Services Lo	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	5379 User Account Management
Seved Loar	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	5379 User Account Management
Subscriptions	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	53/9 User Account Management
aggi Subscriptions	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	53/9 User Account Management
	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	53/9 User Account Management
	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	5379 User Account Management
	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	53/9 User Account Management
	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	5379 User Account Management
	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	5379 User Account Management
	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	5379 User Account Management
	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	5379 User Account Management
	Audit Success	1.9.2024. 13:34:03	Microsoft Windows security auditing.	5379 User Account Management
	Court 4605 Address (CARColor Courts	CARACT STATE		
	Event 4623, Microsoft Windows securi	y auditing.		*
	General Details			
	An account failed to log on.			
	Subject			
	Security ID:	SYSTEM		
	Account Name:	DESKTOP-KM4ICFE\$		
	Account Domain:	WORKGROUP		
	Logon ID:	UX3E7		
	Logon Type:	2		
	Assount For Which Longon Evilade			
	Security ID:	NULL SID		
	Account Name:	-		
	Account Domain:	-		
	Failure Information:			
	Failure Reason:	An Error occured during Logon.		
	Status:	0xC000006D		
	Sub Status:	0xC0000380		
	Log Name: Security			
	Source: Microroft Wing	lows security onged: 1.9.2024 20-04-1	2	
	Event ID: 4625	Tark Category Logo-	•	
	Local Jacks	lask Category: Logon		
	Level: Information	Keywords: Audit Failure		
	User: N/A	Computer: DESKTOP-KM40	.FE	
	OpCode: Info			
	More Information: Event Log Onli	ne Help		

Slika 45: Sigurnosni log koji prikazuje neuspješnu prijavu (Izvor: Vlastita izrada, 2024.)

Zatim je na slici 46. moguće vidjeti da sistemski log koji prikazuje da je nastala greška tijekom kopiranja zbog nedostatka prostora na disku, te je sustav zbog toga prekinuo operaciju.

🛃 Event Viewer						
File Action View Help						
🔶 🄿 🞽 📰 🔢 🖬						
🛃 Event Viewer (Local)	System Number of	events: 39.470				
> 📑 Custom Views			Date and Time		Source	
Vindows Logs	Level		Date and time	42	Source	1
Application	Information		2.9.2024. 17:20:	12	Kernel-General	
Security	Information		2.9.2024. 17:20:	12	Kernel-General	
Setup	Information		2.9.2024. 17:20:	12	Kernel-General	
System	Information		2.9.2024. 17:18:	25	Service Control Manager	
Applications and Services Lo	Information		2.9.2024. 17:16:	15	Service Control Manager	
Saved Logs	Error		2.9.2024. 16:12:	47	Volsnap	
	Warning		2.9.2024. 16:12:	42	Volsnap	
Security	Information		2.9.2024. 16:12:	42	Volsnap	
Security1	Information		2.9.2024. 16:12:	42	Volsnap	
- System	Information		2.9.2024. 16:09:	38	Service Control Manager	
Subscriptions	Error		2.9.2024. 16:09:	38	Service Control Manager	
	Information		2.9.2024. 16:09:	38	Application Popup	
	1 Information		2.9.2024. 16:09:	38	Service Control Manager	
	L					
	Event 35, Volsnap					×
	General Details					
	The shadow copie	s of volume C: were aborted	because the shad	ow copy storage failed to grow.		_
	Log Name:	System				
	Source:	Volsnap	Logged:	2.9.2024. 16:12:47		
	Event ID:	25	Task Category	None		
	Lavah	Error	Kennede	Classic		
	Leven	Ellor	Keywords:			
	User:	N/A	Computer:	DESKTOP-KIM4ICFE		
	OpCode:	Info				
	More Information:	Event Log Online Help				

Slika 46: Sistemski log koji prikazuje grešku kod kopiranja diska (Izvor: Vlastita izrada, 2024.)

Na temelju ovih logova događaja možemo zaključiti da je računalo osumnjičenog 1.9.2024. u 20:04: bilo pokrenuto, te da je bilo neuspješne prijave, zatim možemo vidjeti da je zbog nepoznatih razloga osumnjičeni radio kopiju datoteka, te mu je ponestalo prostora na disku zbog čega se pojavila greška u sistemskom logu.

6.4. Analiza procesa

U ovom dijelu napraviti ćemo analizu procesa i memorije pomoću programa ProcMon i ProcDump. Process Monitor (ProcMon) je moćan alat iz Sysinternals Suite-a koji omogućuje praćenje aktivnosti sistema u realnom vremenu, uključujući pristup datotekama, registre, procese, i mrežne aktivnosti. Kada su omogućene značajke poput Virtualization-Based Security (VBS) i Hypervisor-Enforced Code Integrity (HVCI), ProcMon je ključan za praćenje kako ove sigurnosne mjere utječu na procese i otkrivanje eventualnih pokušaja zaobilaženja tih zaštita. ProcMon također omogućuje da analizirate kada i kako se događaji odvijaju, identificirate anomalije, te procijenite učinkovitost VBS-a i HVCI-a u zaštiti sustava. Na temelju ovih podataka možete dokumentirati prijetnje, preporučiti dodatne sigurnosne mjere i poboljšati sigurnosnu strategiju sustava.

U programu ProcMon proučavat ćemo par procesa koja od iznimnog značaja za siguran rad operativnog sustava. Jedan od tih procesa je "**csrss.exe**". On je ključan sistemski proces u operativnom sustavu Windows koji igra vitalnu ulogu u upravljanju korisničkim sesijama i konzolnim prozorima, kao što je Command Prompt. Ovaj proces se pokreće pri dizanju sustava i odgovoran je za stvaranje i upravljanje osnovnim funkcijama korisničkog sučelja. U starijim verzijama Windowsa, "csrss.exe" je imao i ulogu u grafičkim operacijama, no danas se uglavnom fokusira na konzolne aplikacije i upravljanje procesima. Praćenje csrss.exe procesa pomoću alata kao što je ProcMon može pomoći u otkrivanju neovlaštenih promjena ili zlonamjernih aktivnosti koje bi mogle ugroziti sigurnost sustava. Budući da ovaj proces podržava osnovne funkcije korisničkog sučelja i stabilnost operativnog sustava, njegovo praćenje je ključan korak u osiguravanju integriteta sustava, posebno u kontekstu naprednih sigurnosnih značajki poput VBS i HVCI. [24] Na slici 47. moguće je vidjeti vrijeme operacije, koje sve operacije je proces odradio, da li je operacija bila uspješna, putanja do drugog procesa kojeg je operacija pozvala i slično.

Edit Event Filter Tools Optic				
8 👂 🛛 🖉 🖓 🖉	PQ7 BBSB			
Time of Day Process Name	PID Operation	Path	Result	Detail
20:07:58 9734672	1144 BCosteFile	C\Uken\\vanv\Downloads\SvinterpalsSute\Svanon exe	SUCCESS	Desired Access:
20:07:58 9734737	1144 ESCreate File	C-\Users\vanv\Downloads\SvainterpaisSate\Svanon64.eve	SUCCESS	Desired Access
20:07:58 9735016 Cares eve	1144 Pala ev Basic Information File	C \/ Isen\/vanv/Drwnloads\/SvinterpaisSite\/Svinon exe	SUCCESS	CreationTime: 25
20:07:58 9735116 Cores eve	1144 Ballavervicitriomytion	C.V.Isers/wanz/Downloads/Sosintemals/Sub/Sismon exe	SUCCESS	
20:07:58.9735199 Carss exe	1144 FalQueryBasicInformationFile	C:\Users\vanv\Downloads\SvantemailsSute\Svanon64.exe	SUCCESS	CreationTime: 23
20:07:58 9735218 Cores exe	1144 PDCoseFile	C \/ Users\ivany\/Downloads\/SviintemaisSate\/Sviinon.exe	SUCCESS	
20-07-58 9735339	1144 FD arevidirformation	C-\Users\vanv\Downloads\SvsinternaisSute\Sismonfid.exe	SUCCESS	
20:07:58 9735484 Ceres eve	1144 ECConeFile	C \\ Lisen \\vany \Downloads\SviinterpaisS de\Svimon64 exe	SUCCESS	
20-07-58 9735768	1144 III BeoQueoVakie	HKLM/SOFTWARF/Microsoft/Windows/Current/Version/Side/ReSide/PublisherPolicy/DanceTime	SUCCESS	Type REG OW
20-07-58 9735946 Caras eve	1144 BecQueryVakar	HKLM/SOFTWARE/Memorif/Windows/Current/Version/SideBr/Side/PublisherPolicyChange Time	SUCCESS	Type: REG_OW
20.07.58.9847659	1144 For Create File	C:Windows/Sedem 32/abel 32 dl	SUCCESS	Desired Access
20.07.58 9848045	1144 STD and Ball Information File	C: Windows (System 2) shares as	SUCCESS	Creation Time 1
20-07-58 9548144	1144 Pala any kiloformation	C Windows Statem 22 while 22 4	SUCCESS	
20.07.58 9848246	1144 Polloga Fla	C-Wilsona (Statum 32) and 23 at	SUCCESS	
20.07.59 9949923	1144 H BacQ muliake	HKI M/S/DETWARE/Microsoft/Windows/Create/Version/SideBr/Side/Disbate/Dolory/Diagona Time	SUCCESS	Time REG OW
20.07.58 9850006	1144 PoCreate Rie	CVW/news/Section 22/SEE1/32.41124 Confin	NAME NOT FOUND	Desired Access
20.07.50.0052754	1144 Robert	C Ministra System 2 Sector 2 Sector 2	SUPPERC	Offert C20 794
20.07.50 0055452	1144 RoDendEle	C Mittaderal Caster 21 and 4	CHOCERC	Offeren C2C 200
20.07.50.0000402 Contraction	1144 Population	Conversion apparentate and an	CINCERS	Offerer EQE 010
20.07.50 0001000	1144 III Dee Constitution	Live A	SUCCESS	Owner Handle T
20.07.50,0001000 Colsiss.exe	1144 III Peguaterney	TINLAN LIJO M Schusses Microardh Microardh (Consort Vicentors) CME Mile Son Cottoore	CINCERS	Desired Access
20.07.50,5001304	1144 DesCalida Ver	THE DRIVEN CONTINUES IN CONTINUES CONTINUES AND A DRIVEN AND A DRIVENA	CINCERC	Ker-Cathologyati
20.07.50,0002500	1144 III DesCountier	W/ M SOFTWARE WEDGOL WINDOW CONFIL VERSION OW WIND SET STATE	SUCCESS	Octor Manda T
20.07.50,5052555 Carses eve	1144 The Declaration	HALM SOLET WARE INCOMENDATION AND A MEMORY AND A MEMO A MEMORY AND A MEMORY AND	CINCERS	Designed Accesses
20.07.50.0052730 Coroserve	1144 III Performation	THEM SOFT WARE INCOMENTING AND A COMPLETED AND	CINCERC	Orange Cardward
20.07.50,0002302	1144 III DesCounting	HILM SOFTWARE INCOMENTATIONS CARE INVESTIGATION (WINDOW STRING) and Incomentation of the second strings of an address of the second string of the second	0000000	Index: 0 Name
20.07.50,9053194 Const.exe	1144 Progenumery	HIGH SUP TWARE WERDER WINDOW CLIPTER VERSION SMILLIPER V	SUCCESS	Protex: 0, reame:
20.07.50,5053550	1144 meguueryney	Inclusion of the second s	NO NORE ENTRIES	Guery: Cached,
20.07.50,0003771 CSISS.EXE	1144 TE Past weiter	High NCOFTWARE Introduction (Introduction Control of the Contro	SUCCESS	Ourse Handel
20.07.50,3053390	1144 Progutorymey	mkUni Sort Tiware werden minimum current version Strittwings Setting Landos minimum windows entrings 3 tet 30066304630	SUCCESS .	Guery: Handel
20/07/30,3004140 CSSS.ete	1144 negupenney	microsoft which will be a set of the set of	SUCCESS	Desired Access
20.07.50,3004344	1144 Peguueryvake	HIGH SOFTWARE VIECOSOT WINDOW (Litter Version SMI/WinDox Setting) and 4 microsoft windows settings 3 to 305683/44635	BOFFEROVERFLOW	Lengin: 12
20107.30,3004343	1144 m Reguleryvalue	Inclusion twice without windows current version SMI (windows being windows beings, 3) in 36066 3946 31.	50002555	Type: http://doi.org/
20.07.50,5004740 CSISS.exe	1144 m Regulerykey	HILAN SOFT WARE VIECOSOT WINDOW CUTERT VERSON SIMI VIII DISS Settings and 4, microsoft Windows settings, 3 tot 305 bits 3644 30.	SOUCESS .	Query Handell
20107/58.9864900 Cartas exe	1144 HegOpenKey	HKLM/SOFTWARE/Microsoft/Windows/Current/Version/SMI/WinSidS Settings/amdb4_microsoft windows-settings_31bf/3856ad304e35	SUCCESS	Desired Access
20.07.58,5855088 Carss.exe	1144 HeguberyVabe	HKLM/SOFTWARE/Microsoft/Windows/Current/Version/SMI/Win5x5 Settings/amdb4_microsoft-windows-settings_31bf3856ad364e35.	BUFFER OVERFLOW	Length: 12
20.07 50,9055407 CHSS.808	1144 m HegGueryValue	NALM SUP TWARE WARROUGH WINDOWS CUPER VERSION SIM WINDOWS Settings and U4 microsoft windows settings a field stoked so	300LE33	Type: REG_SZ,
20.07.50,5065763 Cares exe	Ties megCloseNey	MCLM Confirm And declosoft windows Current version SMT wirlsx's Settings and 64_microsoft windows settings_3 tof 3556a3364e35	3000233	
20:07.58,9866155 Csrss.exe	1144 HegCloseKey	HKLM/SUFTWARE Microsoft Windows (Lumert Version SM/WinSxS Settings \amd64_microsoft windows settings_31b/3856ad364a35	500CE55	
20.07.58,9866312 Carss.exe	1144 HegCloseKey	HRLM/SUFTWARE Microsoft Windows (Current Version SMI/WinSxS Settings/amd64_microsoft windows settings_31bf3856ad364e35	SUCCESS	
20.07.58.5866478 Carss.exe	1144 IIIS HedCloseKev	HKLM/SOFTWARE/Microsoft/Windows/Culterit/Version/SMI/WinSxS Settings	SUCCESS	

Slika 47: Praćenje aktivnosti procesa "csrss.exe" u programu ProcMon (Izvor: Vlastita izrada, 2024.)

Sljedeći proces kojeg ćemo promatrati je "**winlogon.exe**". On je ključni proces u Windows operativnom sustavu koji upravlja prijavama korisnika i sigurnosnim funkcijama poput provjere autentičnosti i učitavanja korisničkih profila. Ovaj proces je odgovoran za upravljanje početnim fazama korisničke sesije i osiguranje pravilnog pristupa sistemskim resursima. U forenzičkoj istrazi, winlogon.exe je od velike važnosti jer može pomoći u otkrivanju neovlaštenih prijava i drugih sumnjivih aktivnosti. Ako se sumnja na kompromitaciju sustava, analiza aktivnosti winlogon.exe može otkriti pokušaje manipulacije sigurnosnim postavkama ili pristupom. Napadači često ciljaju ovaj proces kako bi sakrili svoje aktivnosti, pa neuobičajeno ponašanje ili promjene u vezi s winlogon.exe mogu ukazivati na prisutnost zlonamjernog softvera ili druge sigurnosne prijetnje. Praćenjem i analizom ovog procesa, forenzičari mogu prikupiti ključne dokaze za razumijevanje i istraživanje sigurnosnih incidenata. Kao i za prošli proces možemo vidjeti preko programa ProcMon vrijeme operacije, koje sve operacije je proces odradio, da li je operacija bila uspješna, putanja do drugog procesa kojeg je operacija pozvala i detalje o toj aktivnosti i slično i to je prikazano na slici 48. [25]

Process Monitor - Sysinternals: www.sysi	internals.com			– o ×
File Edit Event Filter Tools Option	ns Help			
6 B 🖻 🗟 🖉 🛛 🖉 🕲 🐒	∥ Q ↗ <mark>∰ 🗟 🗟 </mark> 🖪			
Time of Day Process Name	PID Operation	Path	Result	Detail
Ten of Ope Tensors Name 200 062.437440163 Strendogn new 201 062.43747 Strendogn new 201 144.428013 Strendogn new 201 253.4480113 Strendogn new 202 253.148013 Strendogn new 202 253.203570 Strendogn new 203 253.127560 Strendogn new 203 254.1377260 Strendogn new 203 254.1377270 Strendogn new 203 254.1377270 Strendogn new	PD Constant 1502 Chrase Est 1502 Chrase Est 1502 Chrase Est 1502 Chrase Casta 1502 Chrase Casta 1502 Chrase Casta 1503 Chrase Casta 1505 Chrase Chrase 1505 Chrase Chrasta	HKUM HKUM Ophinaen Microsoft Windows NT Currert Version Accessibility/Sersion 1 HKUM Ophinaen Microsoft Windows NT Currert Version Accessibility/Sersion 1 HKUM Ophinaen Microsoft Windows NT Currert Version Accessibility/Sersion 1 HKUM Ophinaen Microsoft Windows NT Currert Version Accessibility/Sersion 1 HKUM Ophinaen Microsoft Windows NT Currert Version Accessibility/Sersion 1 HKUM Ophinaen Microsoft Windows NT Currert Version Accessibility/Sersion 1 HKUM Ophinaen Microsoft Windows NT Currert Version Accessibility Sersion 1 HKUM Ophinaen Microsoft Windows Currert Version Accessibility Sersion 1 HKUM Ophinaen Microsoft Windows Currert Version Sciolerer Scaling HKUM Ophinaen Microsoft Windows Currert Version Toplorer Scaling HKUM Ophinaen Microsoft Windows Currert Version Toplever Scaling HKUM Ophinaen Microsoft Windows Currert Version TopmeManagor HKUM DEF/MLT HKUM DEF/MLT Schareae Microsoft Windows Currert Version TomerManagor HKU DEF/MLT Microsoft Windows Currert Version TomerManagor HKU DEF/MLT Microsoft Windows Currert Version TomerManagor HKU DEF/MLT Microsoft Windows Currert Version Tomeret M	Pand SUCCESS S	Detail Tread (I) 6138. User Time () 0000000 Kernel Time () 000000 Kernel Time () 0000000 Kernel Time () 0000000 Kernel Time () 000000000000 Kernel Time () 0000 Kernel Time () 000000 Kernel Time () 0000000 Kernel Time
20:50:41,3914443 winlogon.exe	1632 III RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Scaling	NAME NOT FOUND	Desired Access: Query Value
20:50:41,3916252 winlogon.exe	1632 III RegQueryKey	HKLM	SUCCESS	Guery: Handle Tags, Handle Tags: 0x0
20.50:41,3919046 winlogon.exe	1632 HegOpenKey	HKLM\SUFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Scaling LIVEM	NAME NOT FOUND	Desired Access: Query Value
20:50:41:3921531 winiogon.exe	1632 III RecOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Exolorer\Scaling	NAME NOT FOUND	Desired Access: Query Value
Showing 67 of 20 622 772 monte (0.0%)	Packed husintual memory			

Slika 48: Praćenje aktivnosti procesa " winlogon.exe" u programu ProcMon (Izvor: Vlastita izrada, 2024.)

Analiziranjem i praćenjem aktivnosti ovih procesa na računalu osumnjičenog forenzičari analiziraju aktivnosti određenih procesa na računalu osumnjičenog kako bi ustanovili da li je računalo bilo hakirano ili podložno nekoj drugoj vrsti zlonamjernih aktivnosti.

6.5. Analiza memorijskog dumpa

Memorijski dump je snimka trenutnog stanja radne memorije (RAM-a) računala u određenom trenutku. Sadrži sve podatke koji su u tom trenutku pohranjeni u RAM-u, uključujući aktivne procese, otvorene datoteke, mrežne konekcije i dijelove programa koji su u upotrebi. Ovakva snimka je ključna za forenzičku analizu jer omogućuje detaljan uvid u radnu okolinu računala u trenutku kada je snimka napravljena. Često se koriste u forenzičkim istragama, posebno u slučajevima istraživanja zlonamjernog softvera, hakiranja ili drugih sumnjivih aktivnosti. Također se koristi u programiranju za otklanjanje grešaka, jer omogućuje programerima da vide gdje je program naišao na problem. Budući da se zlonamjerni softver često pokreće iz memorije, memorijski dump može pomoći u otkrivanju prijetnji koje možda nisu pohranjene na disku. Može sadržavati razne informacije, uključujući popis aktivnih procesa, podatke koji se obrađuju, ali nisu zapisani na disk, šifrirane ključeve, pa čak i osjetljive informacije poput lozinki ili e-mailova. Zbog toga je memorijski dump vrijedan alat za istraživače, analitičare i inženjere koji žele detaljno ispitati stanje sustava u određenom trenutku. [26]Za analizu memorijskog dumpa potrebni su nam alati kao što su FTK Imager, koji koristimo za izradu memorijskog dumpa na računalu osumnjičenog, i Volatility, koji nam omogućuje analizu tog memorijskog dumpa. U FTK Imager-u potrebno je odabrati "Capture Memory" i nakon toga odaberemo lokaciju gdje želimo da se memorijski dump spremi. Nakon

kreiranja memorijskog dumpa, otvaramo Volatility Workbench i u njemu uneseno prethodno kreirani memorijski dump. Nakon toga dobiva se rezultat kao što je prikazano na slici 49..

Image file	D:\mem	n dump\memdump.mem		Brow	vse Image	Command	d Description:	and the b			(alatility)	
Platform	Window	is	~	Refresh	Process List	potentia	ally contain injecte	d code.		ILER	Olacilicy	_
Command	window	s.malfind.Malfind	~	Com	mand Info					E V	vorkpen	С
Command pa	arameters				Run						by Passiviark SU	T CW
Process I	D											
284	1208	svcnost.exe	UX8486612430C0	1	-	0	raise Talse	2024-09-01	18:01:45.000000	N/A	Disabled	
120	2028	MUDicplay Copt	0xa48eeI34C080	21		1	False	2024-09-01	18:01:48.000000	2024-0	Disphled	50
524	1208	auchost ave	0xa48eef3a70c0	17	_	ō	False	2024-09-01	18.01.48.000000	N/A N/A	Disabled	
712	1208	suchost eve	0xa48eef5320c0	12	_	0	False	2024-09-01	18.01.48.000000	N/A	Disabled	
744	1208	sychost.exe	0xa48eef544080	3	-	ő	False	2024-09-01	18:01:48.000000	N/A	Disabled	
968	1208	sychost.exe	0xa48eef732080	12	-	0	False	2024-09-01	18:01:48.000000	N/A	Disabled	
108	1208	sychost.exe	0xa48eef79e080	6	-	ō	False	2024-09-01	18:01:48.000000	N/A	Disabled	
16	1208	svchost.exe	0xa48eef7a6080	4	-	0	False	2024-09-01	18:01:48.000000	N/A	Disabled	
180	1208	svchost.exe	0xa48eef92e080	3	-	0	False	2024-09-01	18:01:48.000000	N/A	Disabled	
188	3712	audiodg.exe	0xa48eef929080	10	-	0	False	2024-09-01	18:01:48.000000	N/A	Disabled	
176	1208	svchost.exe	0xa48eefb09080	5	-	0	False	2024-09-01	18:01:48.000000	N/A	Disabled	
340	1208	spoolsv.exe	0xa48eefb780c0	7	-	0	False	2024-09-01	18:01:48.000000	N/A	Disabled	
116	1208	svchost.exe	0xa48eefc6c0c0	5	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
048	1208	svchost.exe	0xa48eefc8e0c0	8	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
036	1208	svchost.exe	0xa48eefc95080	7	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
108	1208	svchost.exe	0xa48eefc98080	24	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
100	1208	armsvc.exe	0xa48eefc8c080	2	-	0	True	2024-09-01	18:01:49.000000	N/A	Disabled	
088	1208	escsvc64.exe	0xa48eefc96080	2	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
080	1208	svchost.exe	0xa48eefc99080	1	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
980	1208	svchost.exe	0xa48eefc9c080	4	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
396	1208	AnyDesk.exe	0xa48eefc9d080	5	-	0	True	2024-09-01	18:01:49.000000	N/A	Disabled	
832	1208	openvpnserv.ex	0xa48eefca2080	2	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
700	1208	svchost.exe	0xa48eefcb6080	1	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
124	1208	logi_lamparray	0xa48eefcb9080	13	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
152	1208	OfficeClickToR	0xa48eefcbf080	18	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
164	1208	lghub_updater.	0xa48ee85020c0	44	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
176	1208	svchost.exe	0xa48eefb9a0c0	7	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
200	1208	MpDefenderCore	0xa48eeef13080	8	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
224	1208	svchost.exe	0xa48eefc6a080	3	-	0	False	2024-09-01	18:01:49.000000	N/A	Disabled	
C												>

Slika 49: Rezultat unosa memorijskog dumpa u Volatility (Izvor: Vlastita izrada, 2024.)

Image file Platform Command	D:\mem Windows windows	dump\memdump.mem		Brov		C						
Platform	Windows	s			vse Image	Lists pro	Description:	nec that			(alatilit	V
Command	windows		~	Refres	n Process List	potentia	lly contain injecte	d code.		LE:	Olatilit	y
		s.malfind.Malfind	~	Com	mand Info						VOLKDE	encn
Command p	arameters:				Run						Dy Fassivia	IK SOTCWATE
Process 1	ID											
7902	11120	ataawabbalaan	0x010005202000	26		1	Falso	2021-05-0	1 10.01.02.000000	LULI (Diabled	
9492	1208	steamservice.e	0xa48ee9262080	4	_	0	True	2024-09-0)1 18:04:33.000000	N/A N/A	Disabled	^
12532	7892	steamwebhelper	0xa48eee6e80c0	6	-	1	False	2024-09-0	1 18:04:33.000000	N/A	Disabled	
12776	7892	steamwebhelper	0xa48eeb229180	95	-	1	False	2024-09-0	1 18:04:33.000000	N/A	Disabled	
12476	7892	steamwebhelper	0xa48ee6e8e080	8	-	1	False	2024-09-0	1 18:04:34.000000	N/A	Disabled	
13328	7892	steamwebhelper	0xa48ee769f0c0	5	-	1	False	2024-09-0	1 18:04:36.000000	N/A	Disabled	
13384	7892	steamwebhelper	0xa48ee6e8d080	19	-	1	False	2024-09-0	1 18:04:36.000000	N/A	Disabled	
14136	7532	lghub_system_t	0xa48ee6e06100	52	-	1	False	2024-09-0	1 18:04:38.000000	N/A	Disabled	
12584	14136	lghub_agent.ex	0xa48eeda5c0c0	109	-	1	False	2024-09-0	1 18:04:38.000000	N/A	Disabled	
15608	1376	unsecapp.exe	0xa48ede9670c0	3	-	1	False	2024-09-0	1 18:04:41.000000	N/A	Disabled	
16192	1208	EABackgroundSe	0xa48ede959080	33	-	0	False	2024-09-0	1 18:04:41.000000	N/A	Disabled	
17268	7892	steamwebhelper	0xa48eee0db0c0	20	-	1	False	2024-09-0	01 18:04:43.000000	N/A	Disabled	
18636	17844	chrome.exe	0xa48ee0c470c0	50	-	1	False	2024-09-0	01 18:04:46.000000	N/A	Disabled	
18680	18636	chrome.exe	0xa48ee0c580c0	8	-	1	False	2024-09-0	01 18:04:46.000000	N/A	Disabled	
18844	18636	chrome.exe	0xa48ee0f300c0	32	-	1	False	2024-09-0	01 18:04:47.000000	N/A	Disabled	
18856	18636	chrome.exe	0xa48ee0f320c0	20	-	1	False	2024-09-0	01 18:04:47.000000	N/A	Disabled	
18984	18636	chrome.exe	0xa48ee0f3b0c0	10	-	1	False	2024-09-0	01 18:04:47.000000	N/A	Disabled	
19096	18636	chrome.exe	0xa48ee106e0c0	23	-	1	False	2024-09-0	01 18:04:47.000000	N/A	Disabled	
19104	18636	chrome.exe	0xa48ee10700c0	28	-	1	False	2024-09-0	01 18:04:47.000000	N/A	Disabled	
19432	18636	chrome.exe	0xa48ee116a0c0	28	-	1	False	2024-09-0	01 18:04:47.000000	N/A	Disabled	
5344	9320	Discord.exe	0xa48ee057e080	50	-	1	False	2024-09-0	1 18:04:50.000000	N/A	Disabled	
18332	5344	Discord.exe	0xa48ee6462100	70	-	1	False	2024-09-0	1 18:04:51.000000	N/A	Disabled	
16524	5344	Discord.exe	0xa48eee2950C0	10	-	1	Faise	2024-09-0	1 18:04:51.000000	N/A	Disabled	
17900	0122	Discord.exe	0xa45ederie080	13	-	1	False	2024-09-0	1 10:04:51.000000	N/A N/A	Disabled	
17694	1376	ApprenobileDev	0xa49aa06cd0c0	3	_	1	False	2024-09-0	1 18.04.52 000000	N/A	Disabled	
19532	4144	NGenuitu2Helpo	0xx48aa0a44000	25	_	1	Falso	2024-09-0	1 18.04.54 000000	N/A N/A	Disabled	
19764	5344	Discord.exe	0xa48ee057f080	51	_	1	False	2024-09-0	1 18:04:54.000000	N/A	Disabled	
19908	4144	CrossDeviceSer	0xa48ee09bd0c0	12	-	1	False	2024-09-0	1 18:04:54.000000	N/A	Disabled	\sim
						-						>
												/
								C	lear Log Save to file	Copy to clip	board About	Exit

Slika 50: Rezultat unosa memorijskog dumpa u Volatility (Izvor: Vlastita izrada, 2024.)

Na temelju slike 49. i 50. možemo vidjeti da je osumnjičeni koristio aplikacije poput Anydesk-a, aplikacije Logitech G Hub, da koristi drivere za grafičku karticu Nvidia, da za web preglednik koristi Google Chrome za koji ćemo napraviti analizu povijesti, također da koristi Discord aplikaciju za komunikaciju i slično. Zatim ćemo umjesto Volatility Workbench-a koristiti Volatility preko cmd-a. Da bismo to napravili potrebno je memorijski dump preseliti u mapu gdje se nalazi Volatility i u cmd-u otvoriti mapu gdje se nalazi Volatility. Nakon što smo to napravili koristiti ćemo naredbu "**windows.netstat**" plugin koji simulira funkcionalnost komande netstat iz Windows operativnog sustava i koristi se za analizu mrežnih veza koje su bile aktivne u trenutku snimanja memorijskog dumpa. Kada se pokrene ovaj plugin u Volatilityju, pruža informacije o mrežnim konekcijama i slušačima na računalu. To uključuje popis svih aktivnih TCP i UDP veza, zajedno s IP adresama i portovima koji su trenutno otvoreni. Također, dobiva se popis svih portova na kojima sustav čeka dolazne mrežne konekcije, tj. slušače. Uz to, plugin prikazuje trenutni status svake mrežne veze, poput povezano, zatvoreno ili u stanju čekanja. Kada izvršimo taj plugin, dobiva se rezultat koji je prikazan na slici 51..

Command Promp	t	× + ~								٥	×
D:\mem dump\Vol Volatility 3 Fr	atilityW amework	orkbench>vol.exe 2.7.0	e -f memd	ump.mem windows.	netstat						
Progress: 100.	00	PDB sca	nning fi	nished							
Offset Proto	LocalAd	dr LocalPo	ort	ForeignAddr	Foreign	Port State	PID	Owner	Created		
0xa48efb239ad0	TCPv4	192.168.1.5	53735	88.221.92.144	443	CLOSE_WAIT			N/A		
0xa48ee828b010	TCPv4	192.168.1.5	52111	172.67.167.47	443	ESTABLISHED			N/A		
0xa48ee804a5e0	TCPv4	192.168.1.5	63451	51.195.5.160	443	ESTABLISHED			N/A		
0xa48eebdd94f0	TCPv4	192.168.1.5	52381	192.99.44.206	443	ESTABLISHED			N/A		
0xa48edeceb320	TCPv4	192.168.1.5	52376	192.99.44.206	443	ESTABLISHED			N/A		
0xa48efd2e7ae0	TCPv4	192.168.1.5	52117	104.19.194.29	443	ESTABLISHED			N/A		
0xa48edeaf8660	TCPv4	192.168.1.5	52868	31.13.84.9	443	ESTABLISHED			N/A		
0xa48eede48010	TCPv4	192.168.1.5	53705	192.99.44.206	443	ESTABLISHED			N/A		
0xa48ee6e0b790	TCPv4	127.0.0.1	49778	127.0.0.1	49785	ESTABLISHED			N/A		
0xa48ee73f4010	TCPv4	192.168.1.5	52326	192.99.44.206	443	ESTABLISHED			N/A		
0xa48ee7540010	TCPv4	192.168.1.5	53736	95.101.75.164	443	CLOSE_WAIT			N/A		
0xa48eea7cc5e0	TCPv4	192.168.1.5	52092	104.96.144.90	443	ESTABLISHED			N/A		
0xa48eea76d050	TCPv4	192.168.1.5	52873	31.13.84.53	443	ESTABLISHED			N/A		
0xa48ee938c5e0	TCPv4	192.168.1.5	52537	35.210.110.89	443	ESTABLISHED			N/A		
0xa48efb0c0ae0	TCPv4	192.168.1.5	64385	192.99.44.206	443	ESTABLISHED			N/A		
0xa48ee86db530	TCPv4	192.168.1.5	63452	35.186.224.45	443	ESTABLISHED			N/A		
0xa48ee034f010	TCPv4	192.168.1.5	52142	52.111.231.17	443	ESTABLISHED			N/A		
0xa48ee7b89ac0	TCPv4	192.168.1.5	52316	192.99.44.206	443	ESTABLISHED			N/A		
0xa48efacdba70	TCPv4	192.168.1.5	64027	192.99.44.193	443	ESTABLISHED			N/A		
0xa48eeac86010	TCPv4	127.0.0.1	50142	127.0.0.1	27060	ESTABLISHED			N/A		
0xa48ee11a3090	TCPv4	192.168.1.5	53761	192.99.44.206	443	ESTABLISHED			N/A		
0xa48ee6bb3760	TCPv4	127.0.0.1	49777	127.0.0.1	49786	ESTABLISHED			N/A		
0xa48ee6622a30	TCPv4	127.0.0.1	49803	127.0.0.1	9100	ESTABLISHED			N/A		
0xa48ef9802620	TCPv4	192.168.1.5	53083	142.250.201.197	443	ESTABLISHED			N/A		
0xa48ef14a89a0	TCPv4	192.168.1.5	54271	52.58.152.24	443	CLOSED -		N/A			

Slika 51: Rezultat plugin-a u cmd-u (Izvor: Vlastita izrada, 2024.)

Proučavanjem IP adresa na slici 51. možemo otkriti koja od njih je sumnjiva. To bismo napravili tako da bi one sumnjive unijeli na web stranicu "What's my IP address" i na temelju toga bismo ih eliminirali. Na primjer, uzmemo jednu od IP adresa dobivenih u cmd-u i zalijepimo ju u gore navedenu web stranicu i dobivamo rezultat kao na slici 52.

MY IP	IP LOOKUP	HIDE MY IP	VPNS *	TOOLS *	LEARN *
IP Details For	52.58.152.24				
Decimal:	876255256		Hamburg województwo zac		
Hostname:	ec2-52-58-152-24.eu-central-	+ Freie Hansesto Nieders	adt Bremen Brandenburg woj		
1.compute.ar	nazonaws.com	- Nederland	Berlin Województw		
ASN:	16509	CA Nordrhein-Westfa	nen wojewod		
ISP:	A100 ROW GmbH	België - Belgique He	ssen/Thuringen		
Services:	Datacenter	is de France Luxembourg	in tes		
Country:	Germany	de-France Lorraine Baden-Wo	Bayern		
State/Region:	Hessen	Alsoce	irgau B		
- City:	Frankfurt am Main	Bourgogne Svizzera	isse, Österreich Kärnten		
Latitude:	50.1109 (50° 6′ 39.18″ N)	Leave	c) o openstreetwap renns		
Longitude:	8.6820 (8° 40′ 55.19″ E)	CLICK TO CHECK BLACKLIST S	TATUS		

Slika 52: Rezultat unosa dobivene IP adrese (Izvor: Vlastita izrada, 2024.)

Ovakvom provjerom možemo otkriti s kojim računalima ili serverima je računalo osumnjičenog komuniciralo u trenutku kreiranja memorijskog dumpa. Ovaj plugin značajno doprinosi forenzičkim analizama i omogućava identifikaciju potencijalno sumnjivih mrežnih aktivnosti koje mogu ukazivati na prisutnost zlonamjernog softvera, neovlaštenih pristupa ili drugih sigurnosnih prijetnji.

6.6. Analiza povijesti web preglednika

Analiza povijesti web preglednika igra ključnu ulogu u digitalnoj forenzici. Web preglednici poput Chromea, Firefox-a i Edge-a pohranjuju podatke o korisničkim aktivnostima, uključujući posjećene web stranice, preuzete datoteke, kolačiće i spremljene lozinke. Ovi podaci pomažu istražiteljima u rekonstrukciji korisničkog ponašanja na internetu, što može biti presudno u istrazi zločina, cyber-kriminala ili povreda korporativnih politika. Iako korisnici mogu brisati povijest pregledavanja ili koristiti privatne modove, napredni forenzički alati često mogu povratiti te podatke. Sve ovo čini analizu povijesti web preglednika nezamjenjivom u mnogim digitalnim istragama.

Tijekom ove analize pomoću alata BrowsingHistoryView i WebBrowserPassView moći ćemo pregledati povijest web preglednika osumnjičenog i također moguće sve email adrese, korisnička imena i lozinke korištene u web pregledniku. Za početak ćemo koristiti gore navedeni alat BrowsingHistoryView. BrowsingHistoryView je jedan od alata razvijen od strane NirSoft-a, koji je dizajniran za pregled i analizu povijesti pregledavanja iz različitih web preglednika. Ovaj alat omogućuje korisnicima da jednostavno pregledaju, filtriraju i izvezu povijest pregledavanja sa svojih uređaja.

Kada pokrenemo ovaj alat otvaraju nam se dva prozori. Da bismo mogli pretraživati osumnjičenikovu povijest potrebno je odabrati datume između kojih želimo da se povijest učita s računala, što je prikazano na slici 53.

Filter by visit date/time:	Load histor	y items from th	e last xx days	~ 10	
From: 26. 8.2024.	~ 19:44:26	5 🌲 To:	2. 9.202	4. ~ 19:4	4:26 🌲
Load only URLs contain	one of the sp	pecified strings	(comma-delimited	list):	
Don't load URLs that co	ontain one of	the specified str	ings (comma-delir	nited list):	
Web Browsers					
Internet Explorer		Chrome	F	irefox	
Internet Explorer 10)/11 + Edge	Chrome Ca	nary 🔽 S	SeaMonkey	
🖂 Safari		🔽 Opera	🖂 Y	(andex	
🗹 Edge (Chromium-ba	sed)	🔽 Pale Moon	<u>_</u> \	/ivaldi	
🖂 Waterfox		🖂 Brave			
Load history from					
Load history from the c	urrent runnin	g system (All us	ers)	~	
				~	
History:					
History: App Data:					
History: App Data:					
History: App Data: Local App Data:					
History: App Data: Local App Data: Computer Name:					
History: App Data: Local App Data: Computer Name:	cache task of	IE 10/IE 11/Edg	e for unlocking th	e database f	ile.
History: App Data: Local App Data: Computer Name: Automatically stop the Load Internet Explorer	cache task of	IE 10/IE 11/Edg	e for unlocking th	e database f	ile.
History: App Data: Local App Data: Computer Name: Automatically stop the Load Internet Explorer Skip duplicate URLs tha	cache task of history by us t their time di	IE 10/IE 11/Edg ng API. fference is less	e for unlocking th	e database f	ile. seconds

Slika 53: Opcije za učitavanje povijest web preglednika (Izvor: Vlastita izrada, 2024.)

Budući da smo na slici 53. odabrali da se povijest web preglednika učita od 26.8.2024. do 2.9.2024. te na slici 54. je moguće vidjeti da je osumnjičeni pretraživao po web stranicama github, Youtube, po tražili Google i slično. Uz te web stranice moguće je vidjeti u koje vrijeme je on pristupao tim web stranicama, na koji način je pristupao (link ili preko neke forme, kao što je submit), koliko dugo se zadržao na kojoj web stranici i preko kojeg web preglednika je pristupano.

🗱 BrowsingHistoryView								- 0
File Edit View Options Help								
🗐 🖬 🗡 🗈 🤮 🖉 🧱 約 🕶 🚀								
URL	Title	Visit Time 🗸	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser	User Profile
#https://www.tiktok.com/@imgnivn	This account is private. F	1.9.2024. 20:14:41	379	https://www.tiktok.com		00:00:03.936	Edge (Chromium-based)	ivanv
#https://www.tiktok.com/@imgnivn	This account is private. F	1.9.2024. 20:14:40	379	https://www.tiktok.com		00:00:01.326	Edge (Chromium-based)	ivanv
#https://www.tiktok.com/@imgnivn	This account is private. F	1.9.2024. 20:14:32	379	https://www.tiktok.com		00:00:07.500	Edge (Chromium-based)	ivanv
#https://www.tiktok.com/foryou	(1)	1.9.2024. 20:14:30	245	https://www.tiktok.com		00:00:02.237	Edge (Chromium-based)	ivanv
🔗 https://www.tiktok.com/foryou	(1)	1.9.2024. 20:14:20	245			00:00:09.947	Edge (Chromium-based)	ivanv
https://github.com/volatilityfoundation/volatility3/releases/tag/v2.7.0	Release Volatility 3 2.7.0 ·	1.9.2024. 20:11:43	4	https://github.com/vola	Link		Chrome	ivanv
https://github.com/volatilityfoundation/volatility3/releases/tag/v2.7.0	Release Volatility 3 2.7.0 ·	1.9.2024. 20:11:42	4	https://github.com/vola	Link	00:00:00.290	Chrome	ivanv
https://github.com/volatilityfoundation/volatility3/releases/tag/v2.7.0	Release Volatility 3 2.7.0 ·	1.9.2024. 20:11:42	4	https://github.com/vola	Link	00:00:00.333	Chrome	ivanv
https://github.com/volatilityfoundation/volatility3/releases/tag/v2.7.0	Release Volatility 3 2.7.0 ·	1.9.2024. 20:11:41	4	https://volatilityfoundat	Link	00:00:00.630	Chrome	ivanv
https://volatilityfoundation.org/the-volatility-framework/	The Volatility Framework	1.9.2024. 20:11:36	1	https://www.google.hr/	Link		Chrome	ivanv
https://www.google.hr/search?q=volatility+download&sca_esv=a781b331acaf4086	volatility download - Go	1.9.2024. 20:11:33	3		Form Submit	00:00:02.862	Chrome	ivanv
Nttps://volatilityfoundation.org/	Home of The Volatility Fo	1.9.2024. 20:11:28	2	https://www.google.hr/	Link	00:00:05.044	Chrome	ivanv
https://www.google.hr/search?q=volatility+download&sca_esv=a781b331acaf4086	volatility download - Go	1.9.2024. 20:11:26	3	https://www.google.hr/	Link	00:00:02.396	Chrome	ivanv
Mttps://www.google.hr/search?q=volatility+download&sca_esv=a781b331acaf4086	volatility download - Go	1.9.2024. 20:11:25	3	https://www.google.hr/	Form Submit	00:00:00.307	Chrome	ivanv
📀 https://www.google.hr/search?source=hp&ei=kKN5WrEfgciyAfqcs7AH&btnG=Tra	Volatility - Google Search	1.9.2024. 20:11:20	4	https://www.google.hr/	Link	00:00:05.021	Chrome	ivanv
https://www.google.hr/search?source=hp&ei=kKN5WrEfgciyAfqcs7AH&btnG=Tra	Volatility - Google Search	1.9.2024. 20:11:20	4	https://mail.google.co	Link	00:00:00.616	Chrome	ivanv
https://www.youtube.com/watch?v=G-8-iZSdAbs	Microsoft SysInternals Pr	1.9.2024. 20:10:53	1	https://www.youtube.c	Link	19:41:56.206	Chrome	ivanv
https://www.youtube.com/watch?v=G-8-iZSdAbs&pp=ygURUHJvY01vbiBmb3Jlbn	Microsoft SysInternals Pr	1.9.2024. 20:10:53	1	https://www.youtube.c	Link		Chrome	ivanv
https://www.youtube.com/results?search_query=ProcMon+forensics	ProcMon forensics - You	1.9.2024. 20:10:47	2	https://www.youtube.c	Link	01:53:48.974	Chrome	ivanv
https://www.youtube.com/watch?v=7eAOZuJQvc&t=196s&pp=ygULUHJvY01vbiB	Malware Analysis - Word	1.9.2024. 20:10:41	1	https://www.youtube.c	Link		Chrome	ivanv
https://www.youtube.com/watch?v=7eAOZuJJQvc&t=196s	Malware Analysis - Word	1.9.2024. 20:10:41	1	https://www.youtube.c	Link	00:00:01.472	Chrome	ivanv
https://www.youtube.com/watch?v=00U3am0aBss&pp=ygULUHJvY01vbiB2YnM%3D	Using PerfMon to deter	1.9.2024. 20:10:34	1	https://www.youtube.c	Link		Chrome	ivanv
https://www.youtube.com/watch?v=00U3am0aBss	Using PerfMon to deter	1.9.2024. 20:10:34	1	https://www.youtube.c	Link	00:00:02.210	Chrome	ivanv
https://www.youtube.com/watch?v=ojUFjE00prA&pp=ygULUHJvY01vbiB2YnM%3D	Process Monitor 101 - Yo	1.9.2024. 20:09:33	1	https://www.youtube.c	Link		Chrome	ivanv
https://www.youtube.com/watch?v=ojUFjE00prA	Process Monitor 101 - Yo	1.9.2024. 20:09:33	1	https://www.youtube.c	Link	00:00:57.714	Chrome	ivanv

Slika 54: Prikaz povijesti web preglednika (Izvor: Vlastita izrada, 2024.)

Nakon pregleda povijest web preglednika, koristeći alat WebBrowserPassView. WebBrowserPassView je forenzički alat koji omogućuje brzo i jednostavno dohvaćanje lozinki pohranjenih u različitim web preglednicima. Razvijen od strane NirSoft-a, ovaj alat može izvući lozinke koje su korisnici spremili za automatsku prijavu na web stranice. Pokretanjem alata, on automatski dohvaća lozinke iz različitih web preglednika, te na kraju dobivamo rezultat kao što je na slici 55..

WebBrowserPassView									– 🗆 X
File Edit View Options Help									
🔜 🕑 🖻 🖆 🖏 📲									
URL /	Web Browser	User Name	Password	Password Stre	User Name Field	Password Field	Created Time	Modified Time	Filename
https://talent.testgorilla.com/create-acc	Chrome			Very Strong	mat-input-0	mat-input-1	11.12.2023. 13:18:15		C:\Users\ivanv\AppData\Loc
https://tankionline.com/play/	Chrome			Strong	username	password	8.6.2021. 1:33:55		C:\Users\ivanv\AppData\Loc
https://truckersmp.com/auth/login	Chrome			Strong	email	password	16.8.2017. 16:54:21		C:\Users\ivanv\AppData\Loc
https://trucksbook.eu/	Chrome			Strong	email	pass	16.8.2017. 12:22:13		C:\Users\ivanv\AppData\Loc
https://twitter.com/	Chrome			Strong	session[username	session[password]	12.8.2015. 15:03:15		C:\Users\ivanv\AppData\Loc
Phttps://twitter.com/account/reset_passw	Chrome			Strong		auth_password	12.8.2015. 15:04:35		C:\Users\ivanv\AppData\Loc
https://ucp.fiverp.net/login	Chrome			Strong	login	password	30.10.2017. 20:24:48		C:\Users\ivanv\AppData\Loc
https://vi.aliexpress.com/item/10050023	Chrome			Strong			30.1.2024. 22:04:14		C:\Users\ivanv\AppData\Loc
https://voyo.rtl.hr/registracija	Chrome			Strong	reg_email	reg_password	19.11.2023. 14:49:03		C:\Users\ivanv\AppData\Loc
https://web.facebook.com/	Chrome			Very Strong	email	pass	25.3.2016. 11:33:20		C:\Users\ivanv\AppData\Loc
https://webauth.vip.hr/vasmpauth/Proc	Chrome			Strong	UserID	Password	28.2.2015. 15:41:14		C:\Users\ivanv\AppData\Loc
https://webmail2.foi.hr/	Chrome			Strong	username	password	17.8.2020. 14:20:41		C:\Users\ivanv\AppData\Loc
https://webshop.tokic.hr/	Chrome			Strong	email	password	1.9.2023. 16:17:41		C:\Users\ivanv\AppData\Loc
https://windscribe.com/signup	Chrome			Strong	username	password	6.1.2019. 18:37:57		C:\Users\ivanv\ksppData\Loc
https://worldoftrucks.com/en/sign_in.php	Chrome			Strong	id	password	1.2.2017. 22:57:46		C:\Users\ivanv\AppData\Loc
https://www.adm.hr/account-create.asp	Chrome			Strong	email	passlog	29.8.2018. 22:17:11		C:\Users\ivanv\AppData\Loc
Shttps://www.aliexpress.com/item/32868	Chrome			Strong			24.9.2019. 16:23:33		C:\Users\ivanv\AppData\Loc
https://www.amazon.co.uk/ap/signin	Chrome			Strong	email	password	3.3.2018. 13:43:28		C:\Users\ivanv\AppData\Loc
https://www.amazon.com/ap/register	Chrome			Strong	email		1.3.2018. 20:44:33		C:\Users\ivanv\AppData\Loc
😢 https://www.amazon.com/ap/signin	Chrome			Strong	email	password	28.2.2018. 18:51:13		C:\Users\ivanv\AppData\Loc
😢 https://www.amazon.it/ap/signin	Chrome			Strong	email	password	17.7.2018. 16:19:28		C:\Users\ivanv\AppData\Loc
https://www.back4blood.com/en-us	Chrome			Strong	email	password	8.8.2021. 13:52:46		C:\Users\ivanv\AppData\Loc
https://www.balkanpesbox.com/	Chrome			Very Strong			17.12.2022. 18:54:52		C:\Users\ivanv\AppData\Loc
https://www.bornprettystore.com/	Chrome			Very Strong			23.4.2018. 15:36:43		C:\Users\ivanv\AppData\Loc
https://www.buzzsneakers.com/HRK_hr/	Chrome			Strong	reg_email	reg_password	5.5.2022. 16:16:23		C:\Users\ivanv\AppData\Loc
https://www.challengeme.gg/register/	Chrome			Strong	fos_user_registrati	fos_user_registrati	2.11.2016. 20:17:41		C:\Users\ivanv\AppData\Loc
https://www.coinbase.com/signup	Chrome			Strong	email	password	17.3.2021. 17:02:02		C:\Users\ivanv\AppData\Loc
https://www.coinoto.com/login	Chrome			Strong	email	passwd	25.12.2017. 13:31:57		C:\Users\ivanv\AppData\Loc
😢 https://www.cordis.hr/registracija/	Chrome			Strong	mjesto	pass	19.8.2021. 17:34:51		C:\Users\ivanv\AppData\Loc
https://www.createdebate.com/debate/s	Chrome			Strong	username	password	8.6.2022. 2:16:39		C:\Users\ivanv\AppData\Loc
https://www.deezer.com/en/login	Chrome			Strong	login_mail	login_password	20.1.2020. 11:56:30		C:\Users\ivanv\AppData\Loc
A	~·····			V			10.2.2024 0.64.20		CATH-112
250 Passwords, 1 Selected	Nir Soft Fre	eware. https://www.nirsoft	.net						

Slika 55: Podaci o računu korisnika iz različitih web preglednika (Izvor: Vlastita izrada, 2024.)

Na slici 55. moguće je vidjeti da je korisnik kreirao račune na web stranicama kao što su Twitter, Facebook, Amazon, Ali Express, Voyo i slično. Uz svaku stranicu, ponuđeni su korisnička imena i lozinka za svaku web stranicu i uz to je moguće vidjeti da li je umjesto korisničkog imena korišten email, uz sve to moguće je još vidjeti kada je račun kreiran i kada je zadnji put promijenjeno.

Ovi podaci omogućuju forenzičarima da precizno rekonstruiraju aktivnosti osumnjičenog na računalu, identificiraju račune koje je koristio tijekom određenog vremenskog razdoblja, te otkriju moguće obrasce ponašanja i namjere koje su ključne za istragu.

6.7. Pisanje forenzičkog izvještaja

Forenzički izvještaj je dokument koji priprema stručnjak s posebnim znanjem ili obukom za istragu zločina, bilo da se radi o kibernetičkom kriminalu ili fizičkom zločinu. Postoje različite vrste forenzičkih izvješća: računalno, medicinsko, istražno i evaluacijsko forenzičko izvješće. Računalno forenzičko izvješće koristi se za istraživanje zločina počinjenih putem elektroničkih uređaja kao što su mobilni telefoni, računala i tableti. Takvo izvješće pruža informacije o tome kada se zločin dogodio i koji su njegovi uzroci. Korištenje forenzičkih izvješća je važno jer omogućava detaljnu analizu i razumijevanje zločina, što može pomoći u njihovom rješavanju i prevenciji budućih incidenata.[27]

U nastavku je prikazan simulirani forenzički izvještaj koji se sastojati od sažetka slučaja, analiziranih dokaza, prikupljenih dokaza, koraka istrage i zaključka.

6.7.1.Forenzički izvještaj

Identifikacija slučaja i relevantnih strana

Dana 25. svibnja 2024. godine, tvrtka Micro pokrenula je istragu s brojem slučaja **#2024-0515-MICRO** zbog ozbiljne sumnje da je zaposlenik Ivo Ivić odavao povjerljive informacije konkurentskoj tvrtki. Zaposlenikovo računalo, koje koristi operativni sustav Windows 11, zaplijenjeno je kako bi se istražile te sumnje i kako bi se provela opsežna digitalna forenzička analiza.

Istragu je vodila digitalna forenzička ekipa tvrtke Micro, čiji članovi su:

- Marko Horvat, glavni forenzičar s dugogodišnjim iskustvom u analizi digitalnih dokaza
- Ana Petrović, specijalist za analizu digitalnih artefakata i rekonstrukciju korisničkih aktivnosti
- Luka Kovačić, stručnjak za prikupljanje, očuvanje i analizu digitalnih dokaza, s posebnim naglaskom na forenzičku obradu diskova

Tijekom ove forenzičke analize tim je pristupio prikupljanju i očuvanju svih relevantnih podataka s diska računala. Analiza je obuhvatila detaljno ispitivanje povijesti web preglednika kako bi se utvrdile eventualne posjete sumnjivim web stranicama ili komunikacijske aktivnosti s konkurencijom. Osim ispitivanja povijesti web preglednika, analizirani su digitalni artefakti, uključujući datoteke, logove i privremene podatke kako bi se rekonstruirale aktivnosti na računalu.

Forenzička ekipa je istražila sve zabilježene događaje i procese na računalu, uključujući pokretanje aplikacija, promjene datoteka i sistemske događaje. Cilj ove opsežne analize bio je utvrditi prisutnost bilo kakvih dokaza koji bi potvrdili ili opovrgli sumnje o odavanju povjerljivih informacija konkurenciji, te omogućiti precizne zaključke i daljnje pravne korake. Kronologija događaja

Kronologija događaja

Istraga u vezi sa slučajem #2024-0515-MICRO započela je 25. svibnja 2024. godine, kada je tvrtka Micro pokrenula postupak zbog sumnje da zaposlenik Ivo Ivić odaje povjerljive informacije konkurenciji.

Detaljna kronologija dokumentira svaki korak poduzet tijekom istrage, pružajući jasan vremenski okvir i objašnjenje postupaka koji su provedeni kako bi se prikupili relevantni dokazi i donijeli zaključci o mogućem odavanju povjerljivih informacija.

25. svibnja 2024.

- 09:00 Interna istraga započinje nakon što su prijavljene sumnje o mogućem odavanju povjerljivih informacija. Forenzički tim tvrtke Micro sastavljen je i dobio zadatak istražiti ovaj slučaj.
- 10:30 Donosi se odluka o zapljeni računala zaposlenika lve lvića, koje koristi operativni sustav Windows 11zato što je računalo identificirano kao ključni izvor potencijalnih dokaza.
- 11:30 Računalo je formalno zaplijenjeno i premješteno u forenzički laboratorij tvrtke Micro radi provođenja digitalne analize. U ovom trenutku, računalni sustav je zaštićen kako bi se očuvala cjelovitost podataka.

26. svibnja 2024.

 08:00 - Forenzički tim započinje s procesom stvaranja forenzičke kopije cijelog diska računala. Forenzička kopija uključuje sve aktivne datoteke, izbrisane datoteke i nedodijeljeni prostor koji može sadržavati ostatke izbrisanih podataka. Proces je vođen strogim procedurama kako bi se osiguralo da svi podaci ostanu netaknuti.

14:00 - Forenzička kopija diska je dovršena, a njezina cjelovitost je provjerena koristeći odgovarajuće alate za verifikaciju. Kopija je pohranjena na sigurne medije, a originalno računalo je izolirano kako bi se spriječio bilo kakav daljnji pristup.

27. svibnja 2024.

- 09:00 Tim započinje s detaljnom analizom povijesti web preglednika, tražeći bilo kakve znakove posjeta sumnjivim web stranicama ili korištenje internetskih komunikacijskih kanala koji bi mogli ukazivati na odavanje povjerljivih informacija. Posebna pažnja posvećena je nedavno posjećenim stranicama i pretraživačkim pojmovima.
- 13:00 Slijedi analiza digitalnih artefakata, uključujući pregled privremenih datoteka, sistemskih logova, i drugih zapisa koji mogu pomoći u rekonstrukciji aktivnosti korisnika. Ova analiza pruža uvid u korisnikove radnje, kao što su pristupi određenim datotekama, korištenje aplikacija, te vrijeme i način korištenja računala.
- 16:00 Tim provodi dodatnu analizu zabilježenih događaja na sustavu, uključujući promjene u datotekama, instalacije softvera, i druge ključne događaje koji mogu biti relevantni za istragu.

28. svibnja 2024.

- 10:00 Forenzički stručnjaci istražuju pokrenute procese na računalu, uključujući aplikacije koje su mogle biti korištene za komunikaciju s konkurencijom ili prijenos povjerljivih podataka. Tim analizira i procese koji su bili aktivni u vrijeme sumnjivih radnji kako bi se identificirali potencijalni kanali curenja informacija.
- 13:30 Na temelju provedenih analiza, tim pregledava i organizira prikupljene dokaze.
 Povezuju se različiti dijelovi informacija kako bi se stvorila cjelovita slika događaja i mogućih radnji zaposlenika.
- 16:00 Istraga se privodi kraju, a forenzički tim započinje izradu detaljnog izvještaja koji uključuje sve ključne nalaze, prikupljene dokaze i zaključke. Izvještaj će poslužiti kao temelj za daljnje korake, uključujući eventualne pravne postupke protiv osumnjičenog.

Tehnički detalji

U ovoj istrazi korišten je niz forenzičkih alata, od kojih je svaki imao specifičnu ulogu u različitim fazama analize. FTK Imager, na primjer, bio je ključan u početnoj fazi za stvaranje forenzičkih slika tvrdih diskova i drugih uređaja za pohranu podataka, osiguravajući pritom integritet dokaza pomoću generiranih hash vrijednosti. Volatility i Volatility Workbench omogućili su dubinsku analizu memorije sustava, otkrivajući informacije poput aktivnih procesa i mrežnih veza koje nisu bile sačuvane na disku. Registry Viewer poslužio je za detaljan pregled Windows Registry-ja, gdje su identificirane ključne promjene i artefakti vezani za sigurnosne postavke sustava. Event Viewer omogućio je analizu Windows event logova, pružajući uvid u važne događaje poput sigurnosnih incidenata i promjena u konfiguraciji sustava. Process Monitor (ProcMon) pružio je mogućnost praćenja aktivnosti u stvarnom vremenu, čime su identificirani sumnjivi procesi i njihove interakcije s datotekama i registryjem. Za analizu povijesti pregledavanja, korišten je BrowsingHistoryView, koji je omogućio identifikaciju posjećenih web stranica relevantnih za istragu. WebBrowserPassView je bio koristan za pronalazak sačuvanih lozinki u web preglednicima, čime su otkriveni potencijalno kompromitirani korisnički računi. Konačno, BitLocker je korišten za dešifriranje podataka zaštićenih enkripcijom, omogućujući pristup i analizu sadržaja koji bi inače bio nedostupan.

Tijekom forenzičke istrage, izrađena je slika osumnjičenog diska pomoću alata FTK Imager s ciljem očuvanja svih podataka u njihovom izvornom stanju i omogućavanja detaljne analize. Analizirane su različite vrste datoteka, uključujući dokumente, slike, videozapise, arhivske datoteke, izvršne datoteke i sistemske datoteke relevantne za slučaj. Izbrisane datoteke identificirane su nakon što je slika diska montirana u FTK Imageru, gdje su se vidjeli tragovi tih datoteka u slobodnom prostoru na disku i u područjima diska koja nisu dodijeljena nijednoj datoteci (unallocated space). Skrivene datoteke otkrivene su analizom sistemskih atributa, kao i pregledom metapodataka i anomalija u strukturi datotečnog sustava.

Za analizu artefakata s računala osumnjičenog korišten je alat Registry Viewer radi detaljnog pregleda Windows registra. Poseban fokus bio je na datoteci NTUSER.DAT, koja sadrži korisnički specifične podatke. Analizirane su aplikacije poput Discorda i Steama zbog njihove mogućnosti za komunikaciju u stvarnom vremenu, što je relevantno za istragu. Pregledani su podaci o korištenju ovih aplikacija, uključujući vrijeme posljednjeg pristupa, učestale kontakte i druge relevantne aktivnosti. Također je analizirana sistemska datoteka system, koja pruža informacije o hardveru računala. Proučeni su ključevi koji otkrivaju detalje o matičnoj ploči, vrsti monitora koji je korišten, kao i diskovima upotrijebljenim za pohranu podataka. Ovi podaci omogućili su rekonstrukciju hardverske konfiguracije računala, što je

ključno za razumijevanje načina korištenja računala i povezivanje specifičnih komponenti s analiziranim artefaktima. Ova analiza registra pružila je važne uvide u aktivnosti korisnika i tehničke aspekte sustava, osiguravajući temelj za daljnju forenzičku analizu i potencijalne dokaze u istrazi.

Za analizu logova događaja korišten je alat Event Viewer, koji je omogućio pregled sigurnosnih, aplikacijskih i sistemskih logova. Analizom ovih logova prikupljeni su ključni podaci o aktivnostima na računalu osumnjičenog, uključujući trenutke prijave u sustav, vrijeme paljenja računala, trajanje perioda mirovanja sustava, te informacije o uklanjanju diskova i brisanju aplikacija. Proučeni su logovi kako bi se utvrdilo kada je osumnjičeni pristupio sustavu, koliko je vremena računalo provelo u stanju mirovanja, te kada je i koji disk bio uklonjen. Također su identificirani trenuci kada su aplikacije bile obrisane, kao i zapisi o neuspješnim prijavama. Ova analiza omogućila je rekonstrukciju ključnih aktivnosti i događaja koji su se odvijali na računalu, pružajući važne uvide za daljnju istragu.

Analizom csrss.exe u alatu ProcMon moguće je otkriti različite aktivnosti koje taj proces obavlja. Kroz ProcMon se prate datoteke koje proces otvara, čita, piše ili mijenja, promjene u registru, kao i procese koje stvara ili uklanja. Također se mogu pratiti putanje koje proces koristi, te zabilježiti greške i izuzetci koji se javljaju. Ove informacije pomažu u prepoznavanju sumnjivih aktivnosti i problema sa sustavom, pružajući uvid u način na koji csrss.exe funkcionira i identificirajući potencijalne anomalije ili sigurnosne prijetnje. Analiza omogućuje detaljno razumijevanje ponašanja procesa i može otkriti aktivnosti koje nisu u skladu s normalnim operacijama sustava.

Za analizu memorijskog dumpa korišteni su alati Volatility Workbench i Volatility. Ovi alati omogućili su detaljno ispitivanje sadržaja memorije i identifikaciju aktivnosti korisnika. Analizom memorijskog dumpa otkriveno je da je korisnik koristio aplikaciju AnyDesk, koja omogućuje udaljeni pristup i može se koristiti za prenošenje podataka konkurenciji. Također su identificirani podaci o grafičkoj kartici koju je korisnik koristio, web pregledniku koji je bio aktivan, te IP adresama s kojima je računalo imalo vezu. Ove informacije pružaju uvid u tehničke aspekte rada računala i mrežne aktivnosti, što je ključno za daljnje razumijevanje korisnikovih radnji i potencijalnih sigurnosnih prijetnji.

Za analizu povijesti web preglednika korišteni su alati BrowsingHistoryView i WebBrowserPassView. Ovi alati omogućili su dubinsko istraživanje aktivnosti osumnjičenog na internetu. BrowsingHistoryView omogućava pregled detaljne povijesti pregledavanja, uključujući web stranice kao što su GitHub, YouTube i Google tražilica. Alat prikazuje podatke o vremenskim oznakama kada je osumnjičeni posjećivao ove stranice, trajanje sesija na svakoj stranici te koji web preglednik je korišten. Ova analiza pružila je uvid u obrasce pretraživanja i aktivnosti korisnika na internetu. WebBrowserPassView je korišten za otkrivanje pohranjenih vjerodajnica u web pregledniku. Alat je omogućio pristup svim email adresama, korisničkim imenima i lozinkama koje su bile pohranjene u pregledniku. Na taj način, prikupljeni su podaci o računima koje je osumnjičeni koristio, uključujući web stranice na kojima su ti računi bili aktivni. Zajedno, ovi alati omogućili su sveobuhvatan pregled internetskih aktivnosti osumnjičenog, otkrivajući koje su stranice posjećene, koliko je vremena provedeno na njima i kakve su informacije bile pohranjene. Ovi podaci su ključni za razumijevanje obrazaca ponašanja korisnika i mogu pružiti važne uvide u moguće sumnjive aktivnosti ili sigurnosne prijetnje.

Tijekom forenzičke istrage prikupljeni dokazi su popraćeni odgovarajućim hash vrijednostima kako bi se osigurao njihov integritet. Za svaku forenzičku kopiju diska izračunate su hash vrijednosti koristeći standardne algoritme, poput MD5 i SHA-1. Ove hash vrijednosti prikazane su u izvještaju kako bi se dokazalo da podaci nisu mijenjani od trenutka njihovog prikupljanja do trenutka analize. Prikazane hash vrijednosti za sve forenzičke kopije potvrđuju da su dokazi autentični i nepromijenjeni, što je ključno za održavanje vjerodostojnosti cjelokupnog forenzičkog postupka. Time se osigurava da rezultati analize temelje na originalnim, nepromijenjenim podacima, što je od suštinske važnosti za integritet i valjanost istrage. Prikupljene hash vrijednosti prikazane su na slici 56.

Opis metodologije

Tijekom analize slike diska pregledane su sve datoteke, uključujući sistemske datoteke, korisničke dokumente, aplikacijske datoteke, privremene datoteke, logove, datoteke vezane uz mrežni promet, datoteke preglednika i izbrisane datoteke, pri čemu nije pronađena nijedna koja bi bila povezana s firmom. Zatim, tijekom analize datoteke NTUSER.DAT proučavane su aplikacije koje su bile otvarane, s posebnim fokusom na aplikacije Discord i Steam zbog njihove upotrebe u komunikaciji, pri čemu Discord omogućava čak i prijenos uživo. Nadalje, analizirana je datoteka SYSTEM u kojoj su pregledani podaci o računalu osumnjičenog, uključujući informacije o matičnoj ploči, vrsti monitora, diskovima korištenim za pohranu podataka i verziji BIOS-a koju je osumnjičeni koristio. Zatim su analizirani logovi događaja, koji su pokazali da se osumnjičeni prijavio u sustav 16.7.2024. u 18:00, da je računalo 16.7.2024. u 17:39 bilo u stanju mirovanja, da je osumnjičeni 18.7.2024. u 16:38 uklonio disk 4, da je 18.7.2024. u 16:41 obrisao aplikaciju FTK Imager, te da je 1.9.2024. bilo neuspjelih prijava na sustav, kao i da je 2.9.2024. u 16:12 došlo do greške prilikom kopiranja diska. Kod analize

procesa proučavani su procesi CSRSS.EXE i WINLOGON.EXE. Analizom kreiranog memorijskog dumpa utvrđeno je da je osumnjičeni koristio aplikaciju Anydesk, aplikaciju Logitech G Hub, drivere za grafičku karticu Nvidia te web preglednik Google Chrome. Također, pomoću plugin-a Windows.NETSTAT analizirane su IP adrese s kojima je računalo imalo vezu. Daljnjom analizom je otkriveno da je korisnik preko Google Chrome web preglednika pretraživao web stranice poput YouTube, TikTok, GitHub, te koliko je puta i koliko dugo je posjećivao svaku od tih stranica. Na kraju, analizom računa utvrđeno je da je korisnik imao aktivne račune na web stranicama kao što su Twitter, Facebook, AliExpress i Voyo, koje je redovito koristio.

Nakon stvaranja slike diska, provedena je detaljna analiza svih vrsta datoteka. Istražene su sistemske datoteke ključne za operativni sustav, korisnički dokumenti, aplikacijske datoteke, privremene datoteke, logovi, datoteke preglednika te izbrisane datoteke koje bi mogle sadržavati preostale informacije. Unatoč iscrpnoj analizi svih mogućih izvora podataka, relevantni dokazi nisu pronađeni

S obzirom na to da je Discord platforma za komunikaciju, a Steam za kupnju i igranje igara, oba sustava su podvrgnuta detaljnoj analizi u cilju identifikacije potencijalnih dokaza. Koristili smo forenzičke alate za pristup svim razgovorima i aktivnostima na Discordu i Steamu, uključujući mogućnost prijenosa uživo na Discordu. Također su analizirane aplikacije otvorene putem datoteke NTUSER.DAT, kao i podaci iz datoteke SYSTEM, koji sadrže informacije o računalu osumnjičenog, poput matične ploče i verzije BIOS-a. Svi pronađeni dokazi dokumentirani su s detaljnim informacijama o korisnicima, vremenskim oznakama i sadržaju poruka.

Analizom logova događaja utvrđeno je da osumnjičeni je pristupio sustavu 16. srpnja 2024. u 18:00 sati, neposredno nakon što je računalo izašlo iz stanja mirovanja u 17:39 sati. Dana 18. srpnja 2024. u 16:38 sati, osumnjičeni je fizički uklonio disk 4 iz računala, a samo tri minute kasnije, u 16:41 sati, obrisao je aplikaciju FTK Imager, koja je korištena za forenzičko ispitivanje i analizu podataka. Ove radnje ukazuju na moguće namjerno uklanjanje dokaza. Nadalje, 1. rujna 2024. zabilježene su neuspješne prijave na sustav, što može sugerirati pokušaje neovlaštenog pristupa ili prikrivanja aktivnosti. Konačno, 2. rujna 2024. u 16:12 sati, došlo je do greške prilikom kopiranja diska, što može biti povezano s prethodnim radnjama uklanjanja diska ili brisanja aplikacija, te može ukazivati na moguću manipulaciju podacima ili fizičke smetnje u sustavu.

Tijekom analize procesa, posebno su proučavani procesi CSRSS.EXE i WINLOGON.EXE. Nakon detaljne istrage, nije pronađen nijedan dokaz koji bi upućivao na to da je osumnjičeni obavljao aktivnosti kojima bi odavao informacije konkurenciji. Analizom ovih procesa nisu identificirane nikakve neobične aktivnosti ili manipulacije koje bi sugerirale da je osumnjičeni bio uključen u neovlašteno prikupljanje ili prijenos informacija.

Analizom memorijskog dumpa utvrđeno je da je osumnjičeni koristio aplikaciju AnyDesk za daljinsko upravljanje računalom, Logitech G Hub za upravljanje perifernim uređajima, te grafičke drivere Nvidia za optimizaciju grafičkih performansi. Također je identificiran web preglednik Google Chrome, što ukazuje na aktivnosti pregledavanja interneta. Dodatno, pomoću plugin-a Windows.NETSTAT analizirane su IP adrese s kojima je računalo imalo aktivne veze, pružajući uvid u mrežne aktivnosti i potencijalne komunikacije s vanjskim poslužiteljima.

Daljnjom analizom utvrđeno je da je korisnik putem web preglednika Google Chrome pretraživao različite web stranice, uključujući YouTube, TikTok i GitHub. Precizirane su informacije o učestalosti posjeta i vremenskom trajanju svakog posjeta tim stranicama, što omogućuje razumijevanje obrazaca korištenja. Osim toga, analizom korisničkih računa ustanovljeno je da je korisnik imao aktivne račune na nekoliko značajnih web stranica, uključujući Twitter, Facebook, AliExpress i Voyo. Ovi računi su korišteni redovito, što sugerira aktivno sudjelovanje na tim platformama.

Zaključci s analizom

Na temelju temeljite forenzičke analize svih dostupnih podataka, uključujući slike diska, logove događaja, memorijske dumpove te aktivnosti na različitim platformama i aplikacijama, utvrđeni su sljedeći rezultati. Analizom slike diska obuhvaćene su sistemske datoteke, korisnički dokumenti, aplikacijske i privremene datoteke, logovi, datoteke preglednika i izbrisane datoteke. Unatoč temeljitoj pretrazi, nijedna od ovih datoteka nije sadržavala relevantne dokaze koji bi upućivali na curenje podataka ili druge neovlaštene radnje. Detaljna analiza platformi Discord i Steam pokazala je da su svi razgovori i aktivnosti, uključujući mogućnost prijenosa uživo na Discordu, pregledani bez pronalaska sumnjivih radnji. Također su analizirane aplikacije otvorene putem datoteke NTUSER.DAT i podaci iz datoteke SYSTEM, no nisu otkriveni dokazi koji bi sugerirali prijenos informacija konkurenciji ili druge neovlaštene aktivnosti. Istraživanjem logova događaja ustanovljeno je da je osumnjičeni pristupio sustavu 16. srpnja 2024., neposredno nakon izlaska računala iz stanja mirovanja. Dana 18. srpnja 2024. uklonio je disk 4 i obrisao aplikaciju FTK Imager. Iako su zabilježene neuspješne prijave na sustav i greška prilikom kopiranja diska 2. rujna 2024., ove radnje nisu

direktno povezane s curenjem podataka, ali mogu sugerirati pokušaje prikrivanja aktivnosti. Analizom procesa CSRSS.EXE i WINLOGON.EXE, nije pronađen nijedan dokaz koji bi upućivao na aktivnosti koje bi sugerirale odavanje informacija konkurenciji. Detaljna istraga ovih procesa nije otkrila nikakve nepravilnosti ili manipulacije. Memorijski dump je pokazao korištenje aplikacija AnyDesk, Logitech G Hub, grafičkih drivera Nvidia i web preglednika Google Chrome. Analizom IP adresa pomoću plugin-a Windows.NETSTAT, nije identificirana sumnjiva mrežna aktivnost koja bi upućivala na curenje podataka. Daljnjom analizom web aktivnosti otkriveno je da je korisnik redovito posjećivao stranice poput YouTubea, TikToka, GitHub-a, Twittera, Facebooka, AliExpressa i Voya. Ove aktivnosti nisu pokazale znakove neovlaštenog pristupa ili prijenosa informacija.

Istraživanjem svih dostupnih podataka, uključujući fizičko uklanjanje diska i brisanje aplikacija, forenzička analiza nije otkrila nikakve dokaze o curenju podataka ili odavanju informacija. Analizirani dokazi, uključujući aktivnosti na Discordu i Steamu, logove događaja, procese i memorijske dumpove, nisu pokazali konkretne znakove neovlaštenog prijenosa informacija ili sumnjivih radnji koje bi ukazivale na kršenje sigurnosti. Unatoč detaljnoj analizi svih relevantnih izvora, nije pronađena poveznica koja bi sugerirala da je osumnjičeni bio angažiran u aktivnostima koje bi mogle uključivati odavanje informacija konkurenciji.

Prilozi

Na slici 56 prikazana je slika diska osumnjičenog, koja je bila podvrgnuta detaljnoj forenzičkoj analizi. Tijekom ovog procesa pažljivo su proučavane različite vrste datoteka, uključujući sistemske i korisničke datoteke, kao i one aplikacijske i privremene naravi. Posebna pozornost posvećena je datotekama koje su bile izbrisane jer su one mogle sadržavati ključne informacije ili tragove aktivnosti osumnjičenog.

🚞 [root]	× +			- • ×	📫 ESD	-USB (H:)	× +			-	o x
← → ↑ C	This PC > Removable D	isk (F:) > [root] >					□ > This PC	> ESD-USB (H:) >			
	10 @ @ 14 s	ort 🗧 🗮 View 🗸		📑 Details	🕀 Nev	∾~ % ©		🕆 🗊 🕅 🕅 🕅	≡ View - ····		🕕 Details
🚞 analiza	Name	Date modified	Туре	Size		Name		Date modified	Type S	ize	
🚞 desktop	🚞 boot	26.7.2023. 19:24	File folder			🔁 boot		26.7.2023. 17:24	File folder		
	🧰 efi	26.7.2023. 19:24	File folder			🧰 efi		26.7.2023. 17:24	File folder		
🗸 💻 This PC	🚞 Primjer 1	27.2.2024. 16:03	File folder		• 1	🛅 Primjer 1		27.2.2024. 14:03	File folder		
> ៉ Local Disk (C:)	🚞 sources	26.7.2023. 19:25	File folder			sources		26.7.2023. 17:25	File folder		
> 📾 Local Disk (D:)	🚞 support	26.7.2023. 19:40	File folder			support		26.7.2023. 17:40	File folder		
> 👝 Local Disk (E:)	System Volume Information	26.7.2023. 19:24	File folder			👼 autorun		5.5.2023. 19:24	Informacije o post		
> 🚍 Removable Disk (F	autorun 📄	5.5.2023. 21:24	Informacije o post		~	📄 bootmgr		5.5.2023. 19:24		405 KB	
> 👝 Removable Disk (C	bootmgr	5.5.2023. 21:24		405 KB		📄 bootmgr.efi		5.5.2023. 19:24		1.536 KB	
> 📫 ESD-USB (H:)	bootmgr.efi	5.5.2023. 21:24		1.536 KB		OsnovnaSredstvaPop	is Imovine	22.2.2024. 14:24	Chrome HTML Do	744 KB	
New Volume (Vr)	💿 OsnovnaSredstvaPopis Imovine	22.2.2024. 16:24	Chrome HTML Do	744 KB		💀 Posel		27.2.2024. 14:03	OpenDocument T	722 KB	

Slika 56: Analiza slike diska (Izvor: Vlastita izrada, 2024.)

Na slici 57 prikazane su hash vrijednosti koje su dobivene nakon izrade forenzičke slike diska osumnjičenog pomoću alata FTK Imager. Ove hash vrijednosti ključne su za verifikaciju integriteta podataka tijekom cijelog procesa analize. One omogućuju stručnjacima da potvrde da podaci na slici diska nisu bili promijenjeni ili manipulirani nakon što je slika napravljena. U slučaju bilo kakve promjene u sadržaju diska, hash vrijednosti bi se promijenile što bi odmah ukazalo na potencijalnu neovlaštenu intervenciju. Time hash vrijednosti služe kao osnovni alat u održavanju vjerodostojnosti i pouzdanosti forenzičke analize.

Name Analiza.E01 Sector count 30720000 MD5 Hash 665a3862ba3ff090459d9f61ad88afcb Ford verification hash 665a3862ba3ff090459d9f61ad88afcb Report Hash 665a3862ba3ff090459d9f61ad88afcb Verify result Match Stored verification hash 665a3862ba3ff090459d9f61ad88afcb Verify result Match Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Report Hash f595e53320b55bba3fc96eabfb2b00b4d10c Verify result Match Bad Blocks List Bad block(s) in image	Ξ					
Sector count 30720000 MD5 Hash Computed hash Computed hash 665a3862ba3ff090459d9f61ad88afcb Stored verification hash 665a3862ba3ff090459d9f61ad88afcb Report Hash 665a3862ba3ff090459d9f61ad88afcb Verify result Match Stored verification hash 665a3862ba3ff090459d9f61ad88afcb Verify result Match Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Report Hash f595e53320b55bba3fc96eabfb2b00b4d10c Verify result Match Bad Blocks List Bad blocks found in image		Name	Analiza.E01			
MD5 Hash Computed hash 665a3862ba3ff090459d9f61ad88afcb Stored verification hash 665a3862ba3ff090459d9f61ad88afcb Report Hash 665a3862ba3ff090459d9f61ad88afcb Verify result Match Stored verification hash 665a3862ba3ff090459d9f61ad88afcb Verify result Match Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Report Hash f595e53320b55bba3fc96eabfb2b00b4d10c Verify result Match Bad Blocks List Bad blocks (s) in image		Sector count	30720000			
Computed hash 665a3862ba3ff090459d9f61ad88afcb Stored verification hash 665a3862ba3ff090459d9f61ad88afcb Report Hash 665a3862ba3ff090459d9f61ad88afcb Verify result Match Stored verification hash 655a3862ba3ff090459d9f61ad88afcb Verify result Match Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Report Hash f595e53320b55bba3fc96eabfb2b00b4d10c Verify result Match Bad Blocks List Bad Blocks (s) in image	Ξ	MD5 Hash				
Stored verification hash 665a3862ba3ff090459d9f61ad88afcb Report Hash 665a3862ba3ff090459d9f61ad88afcb Verify result Match SHA1 Hash F595e53320b55bba3fc96eabfb2b00b4d10c Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Verify result Match Bad Blocks List Bad block(s) in image		Computed hash	665a3862ba3ff09	0459d9f61ad	188afcb	
Report Hash 665a3862ba3ff090459d9f61ad88afcb Verify result Match SHA1 Hash F595e53320b55bba3fc96eabfb2b00b4d10c Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Report Hash f595e53320b55bba3fc96eabfb2b00b4d10c Verify result Match Bad Blocks List Bad block(s) in image		Stored verification hash	665a3862ba3ff09	0459d9f61ad	188afcb	
Verify result Match SHA1 Hash Computed hash Computed hash f595e53320b55bba3fc96eabfb2b00b4d10c Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Report Hash f595e53320b55bba3fc96eabfb2b00b4d10c Verify result Match Bad Blocks List Bad blocks found in image		Report Hash	665a3862ba3ff09	0459d9f61ad	188afcb	
SHA1 Hash Computed hash f595e53320b55bba3fc96eabfb2b00b4d10c Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Report Hash f595e53320b55bba3fc96eabfb2b00b4d10c Verify result Match Bad Blocks List Bad block(s) in image		Verify result	Match			
Computed hash f595e53320b55bba3fc96eabfb2b00b4d10c Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Report Hash f595e53320b55bba3fc96eabfb2b00b4d10c Verify result Match Bad Blocks List Bad block(s) in image	Ξ	SHA1 Hash				
Stored verification hash f595e53320b55bba3fc96eabfb2b00b4d10c Report Hash f595e53320b55bba3fc96eabfb2b00b4d10c Verify result Match Image: Bad Blocks List Bad block(s) in image		Computed hash	f595e53320b55b	ba3fc96eabf	b2b00b4	d10c3
Report Hash f595e53320b55bba3fc96eabfb2b00b4d10c Verify result Match Bad Blocks List Bad block(s) in image		Stored verification hash	f595e53320b55b	ba3fc96eabf	b2b00b4	d10c3
Verify result Match Bad Blocks List Bad block(s) in image No bad blocks found in image		Report Hash	f595e53320b55b	ba3fc96eabf	b2b00b4	d10c3
Bad Blocks List Bad block(s) in image No bad blocks found in image		Verify result	Match			
Bad block(s) in image No bad blocks found in image	Ξ	Bad Blocks List				
		Bad block(s) in image	No bad blocks for	ound in imag	ge	

Slika 57: Hash vrijednosti slike diska (Izvor: Vlastita izrada, 2024.)

Na slici 58. prikazane su informacije iz Registry Viewera koje detaljno prikazuju posljednje vrijeme pristupa aplikaciji Discord na računalu osumnjičenog. U ovom slučaju, podaci iz registra pokazuju točan datum i vrijeme kada je aplikacija Discord zadnji put pokrenuta ili korištena. Ovi podaci su ključni za razumijevanje vremenskog okvira aktivnosti korisnika, posebno u kontekstu analize potencijalnih sumnjivih radnji. Analizom ovih informacija, može se povezati aktivnosti na Discordu s drugim događajima na sustavu, kao što su promjene u datotekama ili mrežnim vezama, što može pomoći u stvaranju cjelovite slike o korisnikovom ponašanju u kritičnim trenucima.

😭 AccessData Registry Viewer (Demo Mode) -	[NTUSER.DAT]			-		;
File Edit Report View Window He	lp					- 0
🖆 🚊 🗈, 🖛 🖶 🗑 🗑 🖉 🖬	8					
Studeets3 Takkhand Type#Path User Shell Folders User Shell Folders <		Hanne Brandbill sup Anadyl Furyy NL. Brandbill Sup Anadyl Chaldbill Brandbill Sup Anadyl Sup Anadyl Sup Anadyl Brandbill Sup Anadyl Sup	Type REG_BINARY			
Key Properties		00 80 00 00 00 02 00 00 0	00-0B 00 00 0	0 51 C1 02 00QÁ	_	
Last Written Time	18.7.2024. 12:00:45 UTC	10 2F 3F 3C 3E C4 DF 80 20 D0 B1 1B 3E 68 6B BB	3E-B7 E8 6F 31 3D-36 14 CC 31	E UB 85 FF 3D //?<>AB->-éo>9= D B7 90 04 3E 02±->hkw=6-1=>		
□ Value Properties		30 7F F9 5A 3E 3F 12 3F 3	BE-07 00 00 0	0 10 4E C7 EA -ùZ>?·?>····NÇê		
Value Name ROT13	com.squirrel.Discord.Discord	40 A3 D8 DA 01 00 00 00 0	00-	£00 · · · ·		
Time	17.7.2024. 23:49:09 UTC					
Times Executed	2					
TUSER DAT\Software\Microsoft\Windows\Curr	entVersion\Evplorer\UserAssist\/CEREESCD-ACE2-4E4E-9178-9926E41749E4	\Count Offse	t: 0			

Slika 58. Informacije o zadnjem otvaranju aplikacije Discord (Izvor: Vlastita izrada, 2024.)

Na slici 59 prikazani su logovi događaja koji bilježe točan trenutak kada se osumnjičeni zadnji put prijavio na svoj račun. Analizom ovih logova omogućeno je praćenje aktivnosti osumnjičenog te procjena vremena kada su se odvijale potencijalno sumnjive radnje. Ovi podaci ključni su za rekonstrukciju događaja i utvrđivanje prisutnosti osumnjičenog tijekom ključnih trenutaka istrage.

Event Viewer				
le Action View Help				
🔿 🖄 💼 🖬 💼				
Event Viewer (Local)	Security Number of events: 3	.741		
Custom Views Windows Loas	Keywords	Date and Time	Source	Event ID Task Category
windows Logs	Q Audit Success	16.7.2024 18:05:56	Microsoft Windows security auditing	5379 User Account Management
Security	Q Audit Success	16.7.2024. 18:05:56	Microsoft Windows security auditing.	5379 User Account Management
Setup	Audit Success	16.7.2024. 18:05:56	Microsoft Windows security auditing.	5379 User Account Management
System	Audit Success	16.7.2024. 18:05:56	Microsoft Windows security auditing.	5379 User Account Management
Forwarded Events	Audit Success	16.7.2024, 18:05:56	Microsoft Windows security auditing.	5379 User Account Management
Applications and Services Lo	Audit Success	16.7.2024, 18:05:56	Microsoft Windows security auditing.	5379 User Account Management
Saved Logs	Audit Success	16.7.2024, 18:05:56	Microsoft Windows security auditing.	5379 User Account Management
Subscriptions	Audit Success	16.7.2024. 18:05:56	Microsoft Windows security auditing.	5379 User Account Management
	Audit Success	16.7.2024. 18:05:56	Microsoft Windows security auditing-	5379 User Account Management
	Audit Success	16.7.2024. 18:05:56	Microsoft Windows security auditing.	5379 User Account Management
	Audit Success	16.7.2024, 18:05:56	Microsoft Windows security auditing.	5379 User Account Management
	Audit Success	16.7.2024. 18:05:56	Microsoft Windows security auditing.	5379 User Account Management
	Audit Success	16.7.2024. 18:05:56	Microsoft Windows security auditing.	5379 User Account Management
	Audit Success	16.7.2024. 18:05:56	Microsoft Windows security auditing.	4672 Special Logon
	Audit Success	16.7.2024. 18:05:56	Microsoft Windows security auditing.	4624 Logon
	Audit Success	16.7.2024. 18:02:16	Microsoft Windows security auditing.	5382 User Account Management
	Audit Success	16.7.2024. 18:02:02	Microsoft Windows security auditing.	5382 User Account Management
	Audit Success	16.7.2024, 18:00:50	Microsoft Windows security auditing.	4672 Special Logon
	Audit Success	16.7.2024. 18:00:50	Microsoft Windows security auditing.	4624 Logon
	Audit Success	16.7.2024. 17:59:11	Microsoft Windows security auditing.	5379 User Account Management
	Audit Success	16.7.2024. 17:59:11	Microsoft Windows security auditing.	5379 User Account Management
	General Details An account was successfully Subject: Security ID: Account Name Account Domain: Logon ID: Logon Information: Logon Type:	logged on. SYSTEM DESICIO-HOMELCES WORKGROUP DUEZ S		
	Remote Credential Virtual Account Log Name: Security Source: Microsol Event ID: 4624 Level: Informat User: IV/A OpCode: Info More Information: <u>Event Le</u>	Sume - No t Windows security Logged: 16.7.2034.1800.5 Tesk Category: Logon on Keywordte Audrif Success Computen: DESKTOP-IOMRICF g Online Help	0 FE	

Slika 59: Prikazi logova događaja za prijave na sustav (Izvor: Vlastita izrada, 2024.)

Na slici 60 prikazani su logovi događaja koji jasno dokumentiraju pokušaj osumnjičenog da napravi kopiju diska C:. Ovi logovi pružaju detaljan prikaz aktivnosti sustava tijekom

pokušaja kopiranja, uključujući točno vrijeme početka operacije, korištene alate i ciljnu lokaciju na koju je disk trebao biti kopiran. Prema zapisima, operacija je prekinuta zbog nedostatka prostora na odredišnom disku, što je spriječilo uspješno dovršavanje kopiranja.

🛃 Event Viewer						
File Action View Help						
🗢 🄿 🖄 📰 📓 🖬						
Event Viewer (Local)	System Number of	events: 39.470				
> 📑 Custom Views	Level		Date and Time		Source	
Vindows Logs	Cevel				Source	1
Application	Information		2.9.2024. 17:20:	12	Kernel-General	
Security	Information		2.9.2024. 17:20:	12	Kernel-General	
Setup	Information		2.9.2024. 17:20:	12	Kernel-General	
E Securited Events	Information		2.9.2024. 17:18:	25	Service Control Manager	
Applications and Senices Lo	Information		2.9.2024. 17:10:		Service Control Manager	
Saved Logs	Error		2.9.2024. 16:12:	47	voisnap	
Application	Warning		2.9.2024. 16:12:	42	Volsnap	
Security	Information		2.9.2024. 16:12:	42	voisnap	
Security1	Information		2.9.2024. 16:12:	42	Volsnap	
System	Information		2.9.2024. 16:09:	38	Service Control Manager	
📑 Subscriptions	Error		2.9.2024. 16:09:	38	Service Control Manager	
· ·	1 Information		2.9.2024. 16:09:	38	Application Popup	
	(1) Information		2.9.2024. 16:09:	38	Service Control Manager	
	L					
	Event 35, Volsnap					×
	General Details					
	o clans					
	The shadow copie	s of volume C: were aborted	because the shad	ow copy storage failed to grow.		_
	1					
	Log Name:	System				
	Source:	Volsnap	Logged:	2.9.2024. 16:12:47		
	Event ID:	35	Task Category:	None		
	Level:	Error	Keywords:	Classic		
	User:	N/A	Computer:	DESKTOP-KM4ICFE		
	OnCode	Info				
	Manalafarmatian	Front Lon Online Unio				
	wore information:	Event Log Unline Help				

Slika 60: Analiza logova događaja za prekinutu operaciju kopiranja (Izvor: Vlastita izrada, 2024.)

Na slici 61. prikazan je memorijski dump analiziran pomoću alata Volatility Workbench, koji omogućuje pregled svih aplikacija aktivnih u trenutku kreiranja dumpa na računalu osumnjičenog. Ovaj memorijski dump sadrži podatke o procesima, pokrenutim aplikacijama, te informacijama o mrežnim konekcijama i korisničkim sesijama.

Image file:	D:\mem	dump\memdump.mem		Brow	se Image	Command	Description:			Low Market					
Platform:	Windows	Windows			Lists process memory ranges that Refresh Process List potentially contain injected code.							Volatility			
Command:	windows.malfind.Malfind			ws.ms/find Mulfind							Workbench				
				_						- paner	by PassMar	k Soft			
Command pa	arameters:				Run										
U Process I	b														
7892	11120	steamwebhelper	0xa48ee927e100	26	-	1	False	2024-09-01	18:04:33.000000	N/A	Disabled				
9492	1208	steamservice.e	0xa48ee9262080	4	-	0	True	2024-09-01	18:04:33.000000	N/A	Disabled				
12532	7892	steamwebhelper	0xa48eee6e80c0	6	-	1	False	2024-09-01	18:04:33.000000	N/A	Disabled				
12776	7892	steamwebhelper	0xa48eeb229180	95	-	1	False	2024-09-01	18:04:33.000000	N/A	Disabled				
12476	7892	steamwebhelper	0xa48ee6e8e080	8	-	1	False	2024-09-01	18:04:34.000000	N/A	Disabled				
13328	7892	steamwebhelper	0xa48ee769f0c0	5	-	1	False	2024-09-01	18:04:36.000000	N/A	Disabled				
13384	7892	steamwebhelper	0xa48ee6e8d080	19	-	1	False	2024-09-01	18:04:36.000000	N/A	Disabled				
14136	7532	lghub system t	0xa48ee6e06100	52	-	1	False	2024-09-01	18:04:38.000000	N/A	Disabled				
12584	14136	lghub agent.ex	0xa48eeda5c0c0	109	-	1	False	2024-09-01	18:04:38.000000	N/A	Disabled				
15608	1376	unsecapp.exe	0xa48ede9670c0	3	-	1	False	2024-09-01	18:04:41.000000	N/A	Disabled				
16192	1208	EABackgroundSe	0xa48ede959080	33	-	0	False	2024-09-01	18:04:41.000000	N/A	Disabled				
17268	7892	steamwebhelper	0xa48eee0db0c0	20	-	1	False	2024-09-01	18:04:43.000000	N/A	Disabled				
18636	17844	chrome.exe	0xa48ee0c470c0	50	-	1	False	2024-09-01	18:04:46.000000	N/A	Disabled				
18680	18636	chrome.exe	0xa48ee0c580c0	8	-	1	False	2024-09-01	18:04:46.000000	N/A	Disabled				
18844	18636	chrome.exe	0xa48ee0f300c0	32	-	1	False	2024-09-01	18:04:47.000000	N/A	Disabled				
18856	18636	chrome.exe	0xa48ee0f320c0	20	-	1	False	2024-09-01	18:04:47.000000	N/A	Disabled				
18984	18636	chrome.exe	0xa48ee0f3b0c0	10	-	1	False	2024-09-01	18:04:47.000000	N/A	Disabled				
19096	18636	chrome.exe	0xa48ee106e0c0	23	-	1	False	2024-09-01	18:04:47.000000	N/A	Disabled				
19104	18636	chrome.exe	0xa48ee10700c0	28	-	1	False	2024-09-01	18:04:47.000000	N/A	Disabled				
19432	18636	chrome.exe	0xa48ee116a0c0	28	-	1	False	2024-09-01	18:04:47.000000	N/A	Disabled				
5344	9320	Discord.exe	0xa48ee057e080	50	-	1	False	2024-09-01	18:04:50.000000	N/A	Disabled				
18332	5344	Discord.exe	0xa48ee6462100	7	-	1	False	2024-09-01	18:04:51.000000	N/A	Disabled				
16524	5344	Discord.exe	0xa48eee2950c0	70	-	1	False	2024-09-01	18:04:51.000000	N/A	Disabled				
17900	5344	Discord.exe	0xa48edef1e080	13	-	1	False	2024-09-01	18:04:51.000000	N/A	Disabled				
17840	8132	AppleMobileDev	0xa48eeece1080	8	-	1	False	2024-09-01	18:04:51.000000	N/A	Disabled				
17684	1376	ApplicationFra	0xa48ee06cd0c0	3	-	1	False	2024-09-01	18:04:52.000000	N/A	Disabled				
19532	4144	NGenuity2Helpe	0xa48ee0e44080	25	-	1	False	2024-09-01	18:04:54.000000	N/A	Disabled				
19764	5344	Discord.exe	0xa48ee057f080	51	-	1	False	2024-09-01	18:04:54.000000	N/A	Disabled				
19908	4144	CrossDeviceSer	0xa48ee09bd0c0	12	-	1	False	2024-09-01	18:04:54.000000	N/A	Disabled				
/												1			

Slika 61: Analiza memorijskog dumpa pomocu alata Volatility Workbench (Izvor: Vlastita izrada, 2024.)

Na slici 62. prikazan je rezultat dobiven korištenjem alata Volatility nakon pokretanja plugin-a windows.netstat. Ovaj alat omogućuje detaljan prikaz svih aktivnih mrežnih veza na računalu osumnjičenog u trenutku izrade memorijskog dumpa. Prikazane su sve IP adrese s kojima je računalo uspostavilo vezu, uključujući lokalne i udaljene IP adrese, kao i odgovarajuće portove koji su korišteni za komunikaciju. Svaka od ovih IP adresa detaljno je analizirana kako bi se utvrdilo jesu li povezane s legitimnim ili sumnjivim mrežnim aktivnostima.

Command Promp	t											
D:\mem dump\Vol	atilityW	vorkbench:	>vol.exe	-f memd	ump.mem windows.u	netstat						
Volatility 3 Fr	amework	2.7.0										
Progress: 100.	00		PDB sca	nning fi	nished							
Offset Proto	LocalAc	idr	LocalPo	rt	ForeignAddr	Foreign	Port	State	PID	Owner	Created	
0xa48efb239ad0	TCPv4	192.168	.1.5	53735	88.221.92.144	443	CLOSE_I	WAIT			N/A	
0xa48ee828b010	TCPv4	192.168	.1.5	52111	172.67.167.47	443	ESTABL:	ISHED			N/A	
0xa48ee804a5e0	TCPv4	192.168	.1.5	63451	51.195.5.160	443	ESTABL:	ISHED			N/A	
0xa48eebdd94f0	TCPv4	192.168	.1.5	52381	192.99.44.206	443	ESTABL:	ISHED			N/A	
0xa48edeceb320	TCPv4	192.168	.1.5	52376	192.99.44.206	443	ESTABL:	ISHED			N/A	
0xa48efd2e7ae0	TCPv4	192.168	.1.5	52117	104.19.194.29	443	ESTABL:	ISHED			N/A	
0xa48edeaf8660	TCPv4	192.168	.1.5	52868	31.13.84.9	443	ESTABL:	ISHED			N/A	
0xa48eede48010	TCPv4	192.168	.1.5	53705	192.99.44.206	443	ESTABL:	ISHED			N/A	
0xa48ee6e0b790	TCPv4	127.0.0	.1	49778	127.0.0.1	49785	ESTABL:	ISHED			N/A	
0xa48ee73f4010	TCPv4	192.168	.1.5	52326	192.99.44.206	443	ESTABL:	ISHED			N/A	
0xa48ee7540010	TCPv4	192.168	.1.5	53736	95.101.75.164	443	CLOSE_	WAIT			N/A	
0xa48eea7cc5e0	TCPv4	192.168	.1.5	52092	104.96.144.90	443	ESTABL:	ISHED			N/A	
0xa48eea76d050	TCPv4	192.168	.1.5	52873	31.13.84.53	443	ESTABL:	ISHED			N/A	
0xa48ee938c5e0	TCPv4	192.168	.1.5	52537	35.210.110.89	443	ESTABL:	ISHED			N/A	
0xa48efb0c0ae0	TCPv4	192.168	.1.5	64385	192.99.44.206	443	ESTABL:	ISHED			N/A	
0xa48ee86db530	TCPv4	192.168	.1.5	63452	35.186.224.45	443	ESTABL:	ISHED			N/A	
0xa48ee034f010	TCPv4	192.168	.1.5	52142	52.111.231.17	443	ESTABL:	ISHED			N/A	
0xa48ee7b89ac0	TCPv4	192.168	.1.5	52316	192.99.44.206	443	ESTABL:	ISHED			N/A	
0xa48efacdba70	TCPv4	192.168	.1.5	64027	192.99.44.193	443	ESTABL:	ISHED			N/A	
0xa48eeac86010	TCPv4	127.0.0	.1	50142	127.0.0.1	27060	ESTABL:	ISHED			N/A	
0xa48ee11a3090	TCPv4	192.168	.1.5	53761	192.99.44.206	443	ESTABL:	ISHED			N/A	
0xa48ee6bb3760	TCPv4	127.0.0	.1	49777	127.0.0.1	49786	ESTABL:	ISHED			N/A	
0xa48ee6622a30	TCPv4	127.0.0	.1	49803	127.0.0.1	9100	ESTABL:	ISHED			N/A	
0xa48ef9802620	TCPv4	192.168	.1.5	53083	142.250.201.197	443	ESTABL:	ISHED			N/A	
0xa48ef14a89a0	TCPv4	192.168	.1.5	54271	52.58.152.24	443	CLOSED			N/A		

Slika 62: Prikaz rezulata nakon pokretanja plugin-a windows.netstat (Izvor: Vlastita izrada, 2024.)

Na slikama 63. i 64. prikazani su rezultati dobiveni korištenjem dva ključna forenzička alata BrowsingHistoryView i WebBrowserPassView. BrowsingHistoryView omogućio je detaljan pregled povijesti pregledavanja web stranica na računalu osumnjičenog. Analizom ovih podataka zna se je koje je web stranice osumnjičeni posjetio, u koje vrijeme, koliko puta je posjećivao određene stranice, koliko se dugo zadržavao na njima, te koji je web preglednik koristio za pristup tim stranicama. WebBrowserPassView alat omogućio je pristup svim računima koji su bili korišteni na računalu osumnjičenog. Prikazane su lozinke, korisnička imena, datumi kada su računi kreirani i kada su posljednji put izmijenjeni. Ovi podaci su izuzetno važni jer mogu otkriti je li osumnjičeni koristio više korisničkih računa, potencijalno s različitim identitetima, te jesu li računi korišteni za pristup osjetljivim ili sumnjivim resursima

22 BrowsingHistoryView								- 0	3				
File Edit View Options Help													
□ Ⅰ × Ⅰ Ⅰ Ⅰ Ⅰ Ⅰ Ⅲ 赵+ ⋪													
URL	Title	Visit Time 🗸	Visit Count	Visited From	Visit Type	Visit Duration	Web Browser	User Profile					
€https://www.tiktok.com/@imgnivn	This account is private. F	1.9.2024. 20:14:41	379	https://www.tiktok.com		00:00:03.936	Edge (Chromium-based)	ivanv					
Chttps://www.tiktok.com/@imgnivn	This account is private. F	1.9.2024. 20:14:40	379	https://www.tiktok.com		00:00:01.326	Edge (Chromium-based)	ivany					
(e) https://www.tiktok.com/@imgnivn	This account is private. F	1.9.2024. 20:14:32	379	https://www.tiktok.com		00:00:07.500	Edge (Chromium-based)	ivany					
//www.tiktok.com/foryou	(1)	1.9.2024. 20:14:30	245	https://www.tiktok.com		00:00:02.237	Edge (Chromium-based)	ivanv					
Chttps://www.tiktok.com/foryou	(1)	1.9.2024. 20:14:20	245			00:00:09.947	Edge (Chromium-based)	ivanv					
Phttps://github.com/volatilityfoundation/volatility3/releases/tag/v2.7.0	Release Volatility 3 2.7.0	1.9.2024. 20:11:43	4	https://github.com/vola	Link		Chrome	ivany					
https://github.com/volatilityfoundation/volatility3/releases/tag/v2.7.0	Release Volatility 3 2.7.0	1.9.2024. 20:11:42	4	https://github.com/vola	Link	00:00:00.290	Chrome	ivanv					
https://github.com/volatilityfoundation/volatility3/releases/tag/v2.7.0	Release Volatility 3 2.7.0	1.9.2024. 20:11:42	4	https://github.com/vola	Link	00:00:00.333	Chrome	ivany					
Phttps://github.com/volatilityfoundation/volatility3/releases/tag/v2.7.0	Release Volatility 3 2.7.0	1.9.2024. 20:11:41	4	https://volatilityfoundat	Link	00:00:00.630	Chrome	ivanv					
Phttps://volatilityfoundation.org/the-volatility-framework/	The Volatility Framework	1.9.2024. 20:11:36	1	https://www.google.hr/	Link		Chrome	ivany					
https://www.google.hr/search?q=volatility+download&sca_esv=a781b331acaf4086	volatility download - Go	1.9.2024. 20:11:33	3		Form Submit	00:00:02.862	Chrome	ivany					
https://volatilityfoundation.org/	Home of The Volatility Fo	1.9.2024. 20:11:28	2	https://www.google.hr/	Link	00:00:05.044	Chrome	ivany					
Phttps://www.google.hr/search?q=volatility+download&sca_esv=a781b331acaf4086	volatility download - Go	1.9.2024. 20:11:26	3	https://www.google.hr/	Link	00:00:02.396	Chrome	ivanv					
Phttps://www.google.hr/search?q=volatility+download&sca_esv=a781b331acaf4086	volatility download - Go	1.9.2024. 20:11:25	3	https://www.google.hr/	Form Submit	00:00:00.307	Chrome	ivany					
Phttps://www.google.hr/search?source=hp&ei=kKN5WrEfgciyAfqcs7AH&btnG=Tra	Volatility - Google Search	1.9.2024. 20:11:20	4	https://www.google.hr/	Link	00:00:05.021	Chrome	ivanv					
Phttps://www.google.hr/search?source=hp&ei=kKN5WrEfgciyAfqcs7AH&btnG=Tra	Volatility - Google Search	1.9.2024. 20:11:20	4	https://mail.google.co	Link	00:00:00.616	Chrome	ivany					
Phttps://www.youtube.com/watch?v=G-8-iZSdAbs	Microsoft SysInternals Pr	1.9.2024. 20:10:53	1	https://www.youtube.c	Link	19:41:56.206	Chrome	ivanv					
Phttps://www.youtube.com/watch?v=G-8-iZSdAbs&pp=ygURUHJvY01vbiBmb3Jlbn	Microsoft SysInternals Pr	1.9.2024. 20:10:53	1	https://www.youtube.c	Link		Chrome	ivany					
https://www.youtube.com/results?search_query=ProcMon+forensics	ProcMon forensics - You	1.9.2024. 20:10:47	2	https://www.youtube.c	Link	01:53:48.974	Chrome	ivanv					
Phttps://www.youtube.com/watch?v=7eAOZuJJQvc&t=196s&pp=ygULUHJvY01vbiB	Malware Analysis - Word	1.9.2024. 20:10:41	1	https://www.youtube.c	Link		Chrome	ivanv					
https://www.youtube.com/watch?v=7eAOZuUQvc&t=196s	Mahware Analysis - Word	1.9.2024. 20:10:41	1	https://www.youtube.c	Link	00:00:01.472	Chrome	ivany					
Phttps://www.youtube.com/watch?v=00U3am0aBss&pp=ygULUHJvY01vbiB2YnM%3D	Using PerfMon to deter	1.9.2024. 20:10:34	1	https://www.youtube.c	Link		Chrome	ivanv					
https://www.youtube.com/watch?v=00U3am0aBss	Using PerfMon to deter	1.9.2024. 20:10:34	1	https://www.youtube.c	Link	00:00:02.210	Chrome	ivanv					
Optimize the set of	Process Monitor 101 - Yo	1.9.2024. 20:09:33	1	https://www.youtube.c	Link		Chrome	ivany					
Phttps://www.youtube.com/watch?v=ojUFjE00prA	Process Monitor 101 - Yo	1.9.2024. 20:09:33	1	https://www.youtube.c	Link	00:00:57.714	Chrome	ivanv					

Slika 63: Prikaz povijesti web preglednika (Izvor: Vlastita izrada, 2024.)

😽 WebBrowserPassView									-	0 ×
File Edit View Options Help										
🔜 🖻 🖻 🖆 🕼 📲										
URL /	Web Browser	User Name	Password	Password Stre	User Name Field	Password Field	Created Time	Modified Time	Filename	
https://talent.testgorilla.com/create-acc	Chrome			Very Strong	mat-input-0	mat-input-1	11.12.2023. 13:18:15		C:\Users\ivanv\	AppData\Loc
https://tankionline.com/play/	Chrome			Strong	username	password	8.6.2021. 1:33:55		C:\Users\ivanv\	AppData\Loc
https://truckersmp.com/auth/login	Chrome			Strong	email	password	16.8.2017. 16:54:21		C:\Users\ivanv\	AppData\Loc
https://trucksbook.eu/	Chrome			Strong	email	pass	16.8.2017. 12:22:13		C:\Users\ivanv\	AppData\Loc
https://twitter.com/	Chrome			Strong	session[username	session[password]	12.8.2015. 15:03:15		C:\Users\ivanv\	AppData\Loc
https://twitter.com/account/reset_passw	Chrome			Strong		auth_password	12.8.2015. 15:04:35		C:\Users\ivanv\	AppData\Loc
https://ucp.fiverp.net/login	Chrome			Strong	login	password	30.10.2017. 20:24:48		C:\Users\ivanv\	AppData\Loc
https://vi.aliexpress.com/item/10050023	Chrome			Strong			30.1.2024. 22:04:14		C:\Users\ivanv\	AppData\Loc
https://voyo.rtl.hr/registracija	Chrome			Strong	reg_email	reg_password	19.11.2023. 14:49:03		C:\Users\ivanv\	AppData\Loc
https://web.facebook.com/	Chrome			Very Strong	email	pass	25.3.2016. 11:33:20		C:\Users\ivanv\	AppData\Loc
https://webauth.vip.hr/vasmpauth/Proc	Chrome			Strong	UserID	Password	28.2.2015. 15:41:14		C:\Users\ivanv\	AppData\Loc
https://webmail2.foi.hr/	Chrome			Strong	username	password	17.8.2020. 14:20:41		C:\Users\ivanv\	AppData\Loc
https://webshop.tokic.hr/	Chrome			Strong	email	password	1.9.2023. 16:17:41		C:\Users\ivanv\	AppData\Loc
https://windscribe.com/signup	Chrome			Strong	username	password	6.1.2019. 18:37:57		C:\Users\ivanv	HoppData\Loc
https://worldoftrucks.com/en/sign_in.php	Chrome			Strong	id	password	1.2.2017. 22:57:46		C:\Users\ivanv\	AppData\Loc
https://www.adm.hr/account-create.asp	Chrome			Strong	email	passlog	29.8.2018. 22:17:11		C:\Users\ivanv\	AppData\Loc
https://www.aliexpress.com/item/32868	Chrome			Strong			24.9.2019. 16:23:33		C:\Users\ivanv\	AppData\Loc
https://www.amazon.co.uk/ap/signin	Chrome			Strong	email	password	3.3.2018. 13:43:28		C:\Users\ivanv\	AppData\Loc
https://www.amazon.com/ap/register	Chrome			Strong	email		1.3.2018. 20:44:33		C:\Users\ivanv\	AppData\Loc
https://www.amazon.com/ap/signin	Chrome			Strong	email	password	28.2.2018. 18:51:13		C:\Users\ivanv\	AppData\Loc
https://www.amazon.it/ap/signin	Chrome			Strong	email	password	17.7.2018. 16:19:28		C:\Users\ivanv\	AppData\Loc
https://www.back4blood.com/en-us	Chrome			Strong	email	password	8.8.2021. 13:52:46		C:\Users\ivanv\	AppData\Loc
https://www.balkanpesbox.com/	Chrome			. Very Strong			17.12.2022. 18:54:52		C:\Users\ivanv\	AppData\Loc
https://www.bornprettystore.com/	Chrome			. Very Strong			23.4.2018. 15:36:43		C:\Users\ivanv\	AppData\Loc
https://www.buzzsneakers.com/HRK_hr/	Chrome			Strong	reg_email	reg_password	5.5.2022. 16:16:23		C:\Users\ivanv\	AppData\Loc
https://www.challengeme.gg/register/	Chrome			Strong	fos_user_registrati	fos_user_registrati	2.11.2016. 20:17:41		C:\Users\ivanv\	AppData\Loc
https://www.coinbase.com/signup	Chrome			Strong	email	password	17.3.2021. 17:02:02		C:\Users\ivanv\	AppData\Loc
https://www.coinoto.com/login	Chrome			Strong	email	passwd	25.12.2017. 13:31:57		C:\Users\ivanv\	AppData\Loc
https://www.cordis.hr/registracija/	Chrome			Strong	mjesto	pass	19.8.2021. 17:34:51		C:\Users\ivanv\	AppData\Loc
Phttps://www.createdebate.com/debate/s	Chrome			Strong	username	password	8.6.2022. 2:16:39		C:\Users\ivanv\	AppData\Loc
https://www.deezer.com/en/login	Chrome			Strong	login_mail	login_password	20.1.2020. 11:56:30		C:\Users\ivanv\	AppData\Loc
A	~·····			v			10.2.2024 0.54.20		CAU	A
250 D	Marcate	For success to the section of the se								
200 Passwords, 1 belected	NIFSOIL	rreeware. https://www.nirso	unet							

Slika 64: Podaci o računu korisnika korištene na web preglednicima (Izvor: Vlastita izrada, 2024.)

7. Zaključak

U ovom završnom radu bavio sam se forenzičkom analizom operacijskog sustava Windows 11. U radu sam koristio različite izvore informacija, Google Scholar i Google, dok sam za prikazivanje i upravljanje izvorima u radu koristio alat Zotero. Forenzička analiza provedena je uz pomoć programa FTK Imager, Registry Viewer, Event Viewer, Volatility Workbench, Volatility, WebBrowserPassView, BrowsingHistoryView, ProcMon i BitLocker. Na početku rada, objasnio sam temeljne pojmove vezane uz digitalnu forenziku te sam se osvrnuo na povijest operacijskog sustava Windows. Detaljno sam objasnio ključne značajke Windowsa 11, kao što su TPM (Trusted Platform Module), UEFI Secure Boot i VBS (Virtualization-Based Security).

Kroz praktični dio rada, pružio sam kratki vodič kroz ključne komponente Windows operacijskog sustava koje su relevantne za forenzičku analizu, uključujući Windows Registry, logove događaja, povijest preglednika i BitLocker-a. Nakon teoretskog uvoda i vodiča, prikazao sam forenzičku analizu na simuliranom slučaju što je obuhvatio prikupljanje podataka s diska, analizu artefakata, pregled logova događaja, analizu procesa, analizu memorijskog dumpa i analizu povijesti web preglednika, te izradu izvještaja slučaja.

Ovaj završni rad daje sveobuhvatan pregled forenzičke analize Windowsa 11, pružajući korisne alate i metode za prikupljanje i analizu digitalnih dokaza. Ovaj rad može poslužiti kao vodič za buduće forenzičke analize i istraživanja u području digitalne forenzike, posebno u kontekstu najnovijih operacijskih sustava.

Popis literature

- [1] "What Is Digital Forensics? | Simplilearn," Simplilearn.com. Accessed: May 16, 2024. [Online]. Available: https://www.simplilearn.com/what-is-digital-forensics-article
- [2] "What Is Digital Forensics? A Closer Examination of the Field." Accessed: May 20, 2024. [Online]. Available: https://www.apu.apus.edu/area-of-study/informationtechnology/resources/what-is-digital-forensics/
- [3] V. dizajn, "Virtus dizajn." Accessed: Jul. 23, 2024. [Online]. Available: https://detektivmreza.hr/hr/usluga/digitalna-forenzika-27
- [4] tprestianni, "What is Computer Forensics?," National University. Accessed: May 16, 2024. [Online]. Available: https://www.nu.edu/blog/what-is-computer-forensics/
- [5] "Microsoft Windows | History, Versions, & Facts | Britannica." Accessed: May 20, 2024. [Online]. Available: https://www.britannica.com/technology/Microsoft-Windows
- [6] O. H.-L. P. A. Malware, sophisticated cyberattacks T. technology can be embedded into modern CPUs, and "securely storeartifacts used to authenticate the platform "2 The artifacts TPMs protect range from passwords to certificates to fingerprints-any important information users want securely stored, "What Is a Trusted Platform Module (TPM) Intel," Intel. Accessed: May 23, 2024. [Online]. Available: https://www.intel.com/content/www/us/en/business/enterprisecomputers/resources/trusted-platform-module.html
- [7] W. I. Blog and T. W. Team, "Update on Windows 11 minimum system requirements and the PC Health Check app," Windows Insider Blog. Accessed: May 23, 2024. [Online]. Available: https://blogs.windows.com/windows-insider/2021/08/27/update-on-windows-11-minimum-system-requirements-and-the-pc-health-check-app/
- [8] "Security Comparison Windows 11 and Windows 10." Accessed: May 21, 2024. [Online]. Available: https://answers.microsoft.com/en-us/windows/forum/all/security-comparisonwindows-11-and-windows-10/b702855b-a299-4f92-9136-37659107fe8e
- [9] "What is virtualization-based security (VBS)? | Definition from TechTarget," Enterprise Desktop. Accessed: May 15, 2024. [Online]. Available: https://www.techtarget.com/searchenterprisedesktop/definition/virtualization-basedsecurity-VBS
- [10] "Computer Forensics: Forensic Issues with Virtual Systems | Infosec." Accessed: May 21, 2024. [Online]. Available: https://www.infosecinstitute.com/resources/digitalforensics/computer-forensics-forensic-issues-virtual-systems/
- [11] "What is a Hypervisor? Hypervisor Explained AWS," Amazon Web Services, Inc. Accessed: May 21, 2024. [Online]. Available: https://aws.amazon.com/whatis/hypervisor/
- [12] J. Boone, "Windows Defender Credential Guard and PEAP MS-CHAPv2," SecureW2. Accessed: May 21, 2024. [Online]. Available: https://www.securew2.com/blog/windowsdefender-credential-guard-and-peap-ms-chapv2
- [13]barrygolden, "Hypervisor-Protected Code Integrity (HVCI) Windows drivers." Accessed: May 21, 2024. [Online]. Available: https://learn.microsoft.com/en-us/windowshardware/drivers/bringup/device-guard-and-credential-guard
- [14] "What Is the Windows Registry and How Does It Work?," What Is the Windows Registry and How Does It Work? Accessed: May 24, 2024. [Online]. Available: https://www.avast.com/c-windows-registry
- [15] "What Is a Hive in the Windows Registry?," Lifewire. Accessed: May 25, 2024. [Online]. Available: https://www.lifewire.com/what-is-a-registry-hive-2625986
- [16] "UserAssist," The 4N6 Post. Accessed: May 25, 2024. [Online]. Available: https://www.4n6post.com/2023/02/userassist.html
- [17]J. Hendrickson, "What Is the NTUSER.DAT File in Windows?," How-To Geek. Accessed: May 25, 2024. [Online]. Available: https://www.howtogeek.com/401365/what-is-thentuser-file/

- [18] "What Is a Windows Event Log? IT Glossary | SolarWinds." Accessed: May 25, 2024. [Online]. Available: https://www.solarwinds.com/resources/it-glossary/windows-event-log
- [19] "Understanding Windows Event Log," Motadata. Accessed: Sep. 03, 2024. [Online]. Available: https://www.motadata.com/it-glossary/windows-event-log/
- [20] "Browser forensics: Google chrome | Infosec." Accessed: May 26, 2024. [Online]. Available: https://www.infosecinstitute.com/resources/digital-forensics/browser-forensicsgoogle-chrome/
- [21]Wisemonkeys, "Web Browser Forensics:Tools,Evidence Collection And Analysis," Medium. Accessed: May 27, 2024. [Online]. Available: https://medium.com/@wisemonkeysoffpage/web-browser-forensics-tools-evidencecollection-and-analysis-162a175fda87
- [22] "What is BitLocker javatpoint," www.javatpoint.com. Accessed: Aug. 31, 2024. [Online]. Available: https://www.javatpoint.com/what-is-bitlocker
- [23]P. Froklage, "Forensic Images for DVR Analysis (E01 or DD) in Magnet Witness," Magnet Forensics. Accessed: Jul. 17, 2024. [Online]. Available: https://www.magnetforensics.com/blog/dvr-examiner-forensic-images-for-dvr-analysise01-or-dd/
- [24] "What Is Csrss.exe?," Lifewire. Accessed: Sep. 01, 2024. [Online]. Available: https://www.lifewire.com/what-is-csrss-exe-4584354
- [25]C. Hoffman, "What Is Windows Logon Application (winlogon.exe), and Why Is It Running on My PC?," How-To Geek. Accessed: Sep. 01, 2024. [Online]. Available: https://www.howtogeek.com/322411/what-is-windows-logon-application-winlogon.exeand-why-is-it-running-on-my-pc/
- [26] "Memory dump definition Glossary | NordVPN." Accessed: Sep. 02, 2024. [Online]. Available: https://nordvpn.com/cybersecurity/glossary/memory-dump/
- [27]xadmin, "Forensic Report Example → Free Report Examples." Accessed: Jul. 20, 2024. [Online]. Available: https://www.reportexamples.org/forensic-report-example/

Popis slika

Slika 1: Korisničko sučelje Windows-a 95 (Izvor: David Grossman, 2017)	5
Slika 2: Korisničko sučelje Windows-a XP (Izvor: Jo Best, 2014.)	6
Slika 3: Korisničko sučelje Windows-a 7 (Izvor: GFC Global, bez dat.)	6
Slika 4: Korisničko sučelje Windows-a 10 (Izvor: Michael Muchmore, 2022.)	7
Slika 5: Korisničko sučelje Windows-a 11 (Izvor: Vlastita izrada, 2024.)	8
Slika 6: Zahtjevi za nadogradnju na Windows 11 (Izvor: Rohan Pal, 2022.)	8
Slika 7: Pojednostavljeni prikaz Hypervisora (Izvor: Jordan Macpherson, 2022.)	11
Slika 8: Sučelje Registry Editora (Izvor: Vlastita izrada, 2024.)	13
Slika 9: Putanja do UserAssist u Windows Registry (Izvor: Vlastita izrada, 2024.)	14
Slika 10: Pretraživanje File Explorera do datoteke (Izvor: Vlastita izrada, 2024.)	15
Slika 11: Pronalazak datoteke "NTUSER.DAT" (Izvor: Vlastita izrada, 2024.)	16
Slika 12: Uključivanje postavke za prikazivanje skrivenih datoteka (Izvor: Vlastita izrada,	
2024.)	16
Slika 13: Prikaz mape Logs (Izvor: Vlastita izrada, 2024.)	17
Slika 14: Prikaz log-ova u Event Viewer-u (Izvor: Vlastita izrada, 2024.)	18
Slika 15: Prikaz log-ova za sustav (Izvor: Vlastita izrada, 2024.)	18
Slika 16: Prikaz log-ova za aplikacije (Izvor: Vlastita izrada, 2024.)	19
Slika 17: Putanja do datoteke History (Izvor: Vlastita izrada, 2024.)	21
Slika 18: Putanja do datoteke Bookmarks (Izvor: Vlastita izrada, 2024.)	22
Slika 19: Putanja do datoteke Login Data (Izvor: Vlastita izrada, 2024.)	22
Slika 20: Sučelje Bitlocker-a (Izvor: Vlastita izrada, 2024.)	23
Slika 21: Odabir otvaranja diska (Izvor: Vlastita izrada, 2024.)	24
Slika 22: Odabir spremanja ključa za oporavak (Izvor: Vlastita izrada, 2024.)	24
Slika 23: Datoteka s ključem za oporavak (Izvor: Vlastita izrada, 2024.)	25
Slika 24: Obavijest o nemogućnosti pristupa disku (Izvor: Vlastita izrada, 2024.)	25
Slika 25: Prozor za unos lozinke (Izvor: Vlastita izrada, 2024.)	25
Slika 26: Kreiranje slike diska (Izvor: Vlastita izrada, 2024.)	27
Slika 27: Odabir vrstu izvora dokaza (Izvor: Vlastita izrada, 2024.)	28
Slika 28: Pokretanje stvaranje slike diska (Izvor: Vlastita izrada, 2024.)	29
Slika 29: Montiranje novo kreirane slike (Izvor: Vlastita izrada, 2024.)	29
Slika 30: Prikaz podataka kod montirane slike i originalnog diska (Izvor: Vlastita izrada,	
2024.)	30
Slika 31: Prikaz dobivenih zaštićenih datoteka (Izvor: Vlastita izrada, 2024.)	31
Slika 32: Putanja do datoteke NTUSER.DAT (Izvor: Vlastita izrada, 2024.)	31

Sina 35. Frikaz mape koje sauzi NTOSEN. DAT (izvor. viastita izrada, 2024 .)
Slika 34: Prikaz mape UserAssist u Registry Viewer (Izvor: Vlastita izrada, 2024.)32
Slika 35: Prikaz ključa koji sadrži vrijednosti zadnjeg otvaranja aplikacije Discord (Izvor:
Vlastita izrada, 2024.)
Slika 36: Prikaz podataka za prijavu na aplikaciji Steam (Izvor: Vlastita izrada, 2024.)33
Slika 37: Prikaz ključeva u mapi SYSTEM (Izvor: Vlastita izrada, 2024.)
Slika 38: Prikaz ključeva o matičnoj ploči (Izvor: Vlastita izrada, 2024.)
Slika 39: Vrsta monitora koju je osumnjičeni koristio (Izvor: Vlastita izrada, 2024.)35
Slika 40: Svi korišteni diskovi za pohranu (Izvor: Vlastita izrada, 2024.)
Slika 41: Prikaz događaja za prijavu u sustav (Izvor: Vlastita izrada, 2024.)
Slika 42: Prikaz događaja za mirovanje sustava (Izvor: Vlastita izrada, 2024.)
Slika 43: Prikaz događaja za uklanjanje diska (Izvor: Vlastita izrada, 2024.)
Slika 44: Prikaz događaja za brisanje aplikacije (Izvor: Vlastita izrada, 2024.)
Slika 45: Sigurnosni log koji prikazuje neuspješnu prijavu (Izvor: Vlastita izrada, 2024.)38
Slika 46: Sistemski log koji prikazuje grešku kod kopiranja diska (Izvor: Vlastita izrada, 2024.)
Slika 47: Praćenje aktivnosti procesa "csrss.exe" u programu ProcMon (Izvor: Vlastita izrada,
2024.)
Slika 48 [.] Praćenje aktivnosti procesa " winlogon exe" u programu ProcMon (Izvor: Vlastita
izrada, 2024.)
izrada, 2024.)
izrada, 2024.)41 Slika 49: Rezultat unosa memorijskog dumpa u Volatility (Izvor: Vlastita izrada, 2024.)42 Slika 50: Rezultat unosa memorijskog dumpa u Volatility (Izvor: Vlastita izrada, 2024.)42
izrada, 2024.)41 Slika 49: Rezultat unosa memorijskog dumpa u Volatility (Izvor: Vlastita izrada, 2024.)42 Slika 50: Rezultat unosa memorijskog dumpa u Volatility (Izvor: Vlastita izrada, 2024.)42 Slika 51: Rezultat plugin-a u cmd-u (Izvor: Vlastita izrada, 2024.)43
izrada, 2024.)
izrada, 2024.)
izrada, 2024.)
izrada, 2024.)
 izrada, 2024.) Slika 49: Rezultat unosa memorijskog dumpa u Volatility (Izvor: Vlastita izrada, 2024.) Slika 50: Rezultat unosa memorijskog dumpa u Volatility (Izvor: Vlastita izrada, 2024.) Slika 51: Rezultat plugin-a u cmd-u (Izvor: Vlastita izrada, 2024.) Slika 52: Rezultat unosa dobivene IP adrese (Izvor: Vlastita izrada, 2024.) Slika 53: Opcije za učitavanje povijest web preglednika (Izvor: Vlastita izrada, 2024.) Slika 54: Prikaz povijesti web preglednika (Izvor: Vlastita izrada, 2024.) 46
izrada, 2024.)
izrada, 2024.)
izrada, 2024.)
izrada, 2024.)
 izrada, 2024.) Slika 49: Rezultat unosa memorijskog dumpa u Volatility (Izvor: Vlastita izrada, 2024.) Slika 50: Rezultat unosa memorijskog dumpa u Volatility (Izvor: Vlastita izrada, 2024.) Slika 51: Rezultat plugin-a u cmd-u (Izvor: Vlastita izrada, 2024.) Slika 52: Rezultat unosa dobivene IP adrese (Izvor: Vlastita izrada, 2024.) Slika 53: Opcije za učitavanje povijest web preglednika (Izvor: Vlastita izrada, 2024.) Slika 54: Prikaz povijesti web preglednika (Izvor: Vlastita izrada, 2024.) Slika 55: Podaci o računu korisnika iz različitih web preglednika (Izvor: Vlastita izrada, 2024.) 46 Slika 56: Analiza slike diska (Izvor: Vlastita izrada, 2024.) 46 Slika 57: Hash vrijednosti slike diska (Izvor: Vlastita izrada, 2024.) 55 Slika 58. Informacije o zadnjem otvaranju aplikacije Discord (Izvor: Vlastita izrada, 2024.) 57 Slika 60: Analiza logova događaja za prekinutu operaciju kopiranja (Izvor: Vlastita izrada, 2024.)
izrada, 2024.)
izrada, 2024.)

Slika 62: Prikaz rezulata nakon pokretanja plugin-a windows.netstat (Izvor: Vlastita izrada,	
2024.)	59
Slika 63: Prikaz povijesti web preglednika (Izvor: Vlastita izrada, 2024.)	59
Slika 64: Podaci o računu korisnika korištene na web preglednicima (Izvor: Vlastita izrada,	
2024.)	60