Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Forenzní analýza v IT

Bc. Filip Šafanda

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Filip Šafanda

Systémové inženýrství a informatika
Informatika

Název práce

Forenzní analýza v IT

Název anglicky

Computer forensic analysis

Cíle práce

Cílem diplomové práce je analýza možností využití současných prostředků k provádění forenzního výzkumu v IT, provedení zajištění digitálních stop z osobního počítače s operačním systémem Windows a jejich rozbor a klasifikace. Výstupem práce je zpracování forenzních dat pro účely další znalecké činnosti.

Metodika

Pro vypracování teoretické části bude využito studia a analýzy dostupných odborných zdrojů týkajících se problematiky digitální forenzní analýzy. Praktická část se bude zabývat zajištěním digitálních forenzních dat z osobního počítače s operačním systémem Windows. Sběr dat bude inicializován na virtuálních počítačích testovacích subjektů, na kterých bude reálnými uživateli nasimulována činnost v rámci operačního systému. Posléze bude provedena analýza zajištěných dat. Na závěr diplomové práce proběhne zpracování forenzních dat pro účely další znalecké činnosti. Práce bude obsahovat literární rešerši, zajištění digitálních forenzních dat, klasifikaci zajištěných dat, jejich analýzu, a zpracování pro účely další znalecké činnosti.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

IT, forenzní analýza, bezpečnost, digitální stopy, Autopsy

Doporučené zdroje informací

CARRIER, Brian. File system forensic analysis. Upper Saddle River: Addison-Wesley, c2005. ISBN 0-321-26817-2.

HOLT, Thomas J., Adam M. BOSSLER a Kathryn C. SEIGFRIED-SPELLAR. Cybercrime and digital forensics: an introduction. London: Routledge, 2015. ISBN 978-1-138-02130-3.

KÄVRESTAD, Joakim. Fundamentals of digital forensics: theory, methods, and real-life applications. Cham: Springer, [2018]. ISBN 978-3-319-96318-1.

KOLOUCH, J. *CyberCrime.* Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Ing. Václav Lohr, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 17. 8. 2021

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 07. 02. 2022

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „Forenzní analýza v IT“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 28. 3. 2022 ……

Bc. Filip Šafanda

Poděkování

Rád bych touto cestou poděkoval vedoucímu Ing. Václavu Lohrovi, Ph.D. za cenné rady a připomínky při tvorbě diplomové práce a své rodině za podporu při tvoření této práce.

Forenzní analýza v IT

Abstrakt

Tématem této diplomové práce je forenzní analýza v IT, zajišťování digitálních stop a jejich analýza. Teoretická část práce bude obsahovat přehled problematiky forenzní analýzy v informačních a komunikačních technologiích, posléze se blíže zaměří na využití současných prostředků k provádění úkonů spojených s forenzní analýzou v IT. Praktická část práce využívá poznatky dokumentované v rešeršní části práce. Předmětem praktické části práce je zajištění digitálních stop z osobního počítače s operačním systémem Windows a jejich analýza, dále také zpracování dat pro účely další znalecké činnosti. Sběr dat bude inicializován na virtuálních počítačích testovacích subjektů, na kterých bude reálnými uživateli nasimulována činnost v rámci operačního systému.

Klíčová slova: Autopsy, bezpečnost, digitální stopy, forenzní analýza, IT

Computer forensic analysis

Abstract

Theme of thesis is forensic analysis in IT, obtaining evidence of digital traces and its analysis. Theoretical part of thesis will contain otherview of forensic analysis in information and communication technology, afterwards it will take a closer look to utilization of current resources used to performing tasks in conjunction with forensic analysis in IT. Practical part of thesis uses findings documented in theoretical part of thesis. Subject of practical part of thesis is obtaining evidence of digital traces from personal computer with Windows operating system and its analysis, and afterwards processing the data for further purposes of future expertise. Collection of data evidence will be perfromed on virtual computers of test subjects, on these computers will be also simulated user activity by real users within the operating system.

Keywords: Autopsy, security, digital traces, forensic, IT

Obsah

1 Úvod 12
2 Cíl práce a metodika 13
2.1 Cíl práce 13
2.2 Metodika 13
3 Teoretická východiska 14
3.1 Digitální forenzní analýza 14
3.2 Historie vzniku digitální forenzní analýzy 14
3.3 Druhy zajistitelných digitálních důkazů 15
3.3.1 Elektronická pošta 15
3.3.2 Digitální obrazové soubory 17
3.3.3 Aktivita webového prohlížeče 18
3.3.4 Data z komunikačních nástrojů (Instant messaging) 19
3.3.5 SQLite Databáze 20
3.3.6 Odkazové soubory systému Windows 21
3.3.7 Data registrů operačního systému 22
3.3.8 Data síťové komunikace 23
3.3.9 Ostatní podstatná systémová data 23
3.4 Bitová kopie systému a dump operační paměti 23
3.4.1 Bitová kopie systému 24
3.4.2 Dump operační paměti 24
3.5 Postupy při zajišťování forenzních dat 25
3.5.1 Zajišťování dat ze živého systému 26
3.5.2 Zajišťování dat z neživého systému 26
3.5.3 Write blocker 27
3.5.4 Zajišťování dat z virtuálních stanic 27
3.6 Porovnání nástrojů pro účely digitální forenzní analýzy 29
3.6.1 FTK Forensic Toolkit 30
3.6.2 Autopsy 31
3.6.3 DEFT 32
3.6.4 CAINE 33

3.6.5 Cellebrite Inspector 34
3.6.6 Další nástroje 36
4 Vlastní práce 40
4.1 Testovací prostředí a využitý software 40
4.2 První scénář 41
4.3 Druhý scénář 41
4.4 Zajištění forenzních dat 41
4.4.1 Proces zajištění dat ze živého systému 42
4.4.2 Proces zajištění dat z neživého systému 43
4.5 Analýza, klasifikace a zpracování dat prvního scénáře 43
4.5.1 Data živé analýzy (aktivní síťová spojení, uživatelé, procesy, dump) 43
4.5.2 Souborový systém (kořenový strom, user data, smazané soubory) 48
4.5.3 Nativní podstatná systémová data (registry atd.) 51
4.5.4 Aplikace (instalovaný software) 54
4.5.5 Data webového prohlížeče 56
4.5.6 Obrazové soubory 58
4.5.7 E-mail a messaging nástroje 59
4.6 Analýza, klasifikace a zpracování dat druhého scénáře 60
4.6.1 Souborový systém (kořenový strom, user data, smazané soubory) 61
4.6.2 Nativní podstatná systémová data (registry, atd) 62
4.6.3 Aplikace (instalovaný software) 63
4.6.4 Data webového prohlížeče 65
4.6.5 Obrazové soubory 66
4.6.6 E-mail a messaging nástroje 66
5 Výsledky a diskuse 68
5.1 Výsledky a diskuse zajištění a analýzy dat 68
5.2 Využití forenzní analýzy a její opodstatnění 69
5.3 Možné dopady narušení důvěrnosti, dostupnosti nebo integrity dat 69
6 Závěr 71
7 Seznam použitých zdrojů 72
8 Přílohy 75

Seznam obrázků

Obrázek 1: Ukázka obsahu headeru e-mailové zprávy 16
Obrázek 2: Ukázka ExitToolGUI 18
Obrázek 3: Ukázka nástroje pro analýzu dat webového prohlížeče 19
Obrázek 4: Software pro analýzu SQLite DB 21
Obrázek 5: Data LNK souborů 22
Obrázek 6: Zařízení write blocker 27
Obrázek 7: FTK Toolkit GUI 31
Obrázek 8: Autopsy GUI 32
Obrázek 9: Deft 33
Obrázek 10: Caine 34
Obrázek 11: Cellebrite Inspector 35
Obrázek 12: Výpis USBDeview 45
Obrázek 13: Volatility příkaz 48
Obrázek 14: Souborový systém 49
Obrázek 15: Smazané soubory 50
Obrázek 16: Obsah koše 50
Obrázek 17: Informace o systému 51
Obrázek 18: Účty 51
Obrázek 19: Historie USB zařízení 52
Obrázek 20: Obsah NTUSER.DAT 53
Obrázek 21: Systém event log 54
Obrázek 22: Instalované programy 55
Obrázek 23: Spuštěné programy 56
Obrázek 24: Historie webového prohlížeče 56
Obrázek 25: Záložky webového prohlížeče 57
Obrázek 26: Login data 57
Obrázek 27: Cookies 57
Obrázek 28: Cache webového prohlížeče 57
Obrázek 29: Nalezené obrazové soubory 59
Obrázek 30: Internet evidence finder výsledek hledání 60

Obrázek 31: Smazané soubory 61
Obrázek 32: Souborový systém 61
Obrázek 33: Účty 62
Obrázek 34: Informace o systému 62
Obrázek 35: Historie USB zařízení 62
Obrázek 36: Obsah NTUSER.DAT 63
Obrázek 37: Systém event log 63
Obrázek 38: Instalované programy 64
Obrázek 39: Spuštěné programy 64
Obrázek 40: Historie webového prohlížeče 65
Obrázek 41: Cookies 65
Obrázek 42: Cache webového prohlížeče 65
Obrázek 43: Nalezené obrazové soubory 66
Obrázek 44: Internet evidence finder výsledek hledání 67
Obrázek 45: Běžící procesy 76
Obrázek 46: Otevřená síťová spojení 77
Obrázek 47: Načtené DLL knihovny 78
Obrázek 48: Certifikáty 79
Obrázek 49: Registry 80
Obrázek 50: Exportované certifikáty 80
Obrázek 51: Ověření bitové kopie 81
Obrázek 52: Ověření bitové kopie 82

1 Úvod

V návaznosti na vývoj v oblasti informačních a komunikačních technologií za poslední léta vzniklo zevšednění potřeby implementace nejrůznějších výpočetních řešení pro převážnou většinu odvětví. Výpočetní systémy jsou považovány za nedílné součásti provozu podnikatelské činnosti soukromých subjektů i fungování institucí státní sféry. Subjekty využívají komplexní informační systémy například pro uchování, zpracování nebo výměnu dat s dalšími entitami. Data jsou považována za důležité informační aktivum, kdy by v důsledku narušení integrity, důvěrnosti nebo dostupnosti dat mohl subjekt utrpět například nezanedbatelné finanční škody, ztrátu důvěryhodnosti, způsobit porušení obecného nařízení o ochraně osobních údajů nebo by mohlo dojít k omezení řízení provozu celé organizace.

Právě integrita, důvěrnost a dostupnost dat bývá častým terčem útoků jedinců i skupin, které svým počínáním některé z těchto atributů narušují v procesu, při kterém se nejčastěji mají v úmyslu zmocnit informačních systémů prostřednictvím využití známých bezpečnostních zranitelností a hrozeb. Takové chování se se označuje jako kybernetický útok. Kybernetický útok bývá jedním z důvodů pro zahájení sběru forenzních dat z postižených informačních systémů většinou s cílem zajištění potřebných digitálních stop pro potřeby kriminalistických procesů nebo využití jako důkazu v rámci soudního řízení.

V této diplomové práci bude pojednáváno především o využití současných prostředků a přístupů k provádění forenzní analýzy v IT, dále jejich praktická aplikace v rámci demonstrace zajištění forenzních digitálních dat z osobních počítačů s operačním systémem Windows testovacích subjektů.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této diplomové práce je analyzovat možnosti využití současných prostředků k provádění forenzní analýzy v informačních a komunikačních technologiích, následně pak aplikovat teoretické poznatky v praktické části práce k demonstraci zajištění forenzních dat z testovacích subjektů. Budou porovnány různé druhy využití softwaru pro zajišťování různých druhů dat. Dále dojde k porovnání přístupů při zajišťování forenzních dat s důrazem kladeným na dodržení uznávaných pravidel při sběru dat takovým způsobem, aby získaná data mohla být využita a akceptována relevantními státními institucemi a složkami (například při možném soudním řízení). Další cíle práce jsou získaná data analyzovat, klasifikovat a zpracovat pro účely další forenzní znalecké činnosti.

2.2 Metodika

Teoretická část práce se zabývá rozebráním a porovnáním současných softwarových, hardwarových i metodologických prostředků či procedur využívaných pro účely provádění forenzní analýzy v informačních a komunikačních technologiích. Práce se také zabývá postupy, které je nutné zohledňovat při zajišťování forenzních dat převážně z osobních počítačů s operačním systémem Microsoft Windows, aby byla zajištěná data využitelná pro další expertízu. Při zajišťování dat je také nutné dodržet veškeré zákonné povinnosti vyplývající z legislativy, včetně dodatečných požadavků vyplývajících z povahy důvodů, které byly iniciátory procesu sběru dat.

Praktická část diplomové práce se zabývá zajištěním forenzních dat z koncových uživatelských stanic užívaných množinou několika reálných uživatelů. Dojde k zajištění forenzních dat z testovacích stanic, posléze k analýze a klasifikaci zajištěných dat a zpracování výstupu pro účely další znalecké činnosti.

3 Teoretická východiska

3.1 Digitální forenzní analýza

Počítačové systémy a sítě se v současnosti staly nerozdělitelnou součástí lidské společnosti na úrovni každodenního využití. Při vyšetřování kteréhokoliv právního sporu je velice pravděpodobné, že v průběhu předkládání evidence budou do vyšetřování zapojeny také digitální důkazy. S trestnými činy jako například podvod, distribuce drog, terorismus a domácí násilí často bývají spojeny výpočetní systémy na různých úrovních. Předměty vynálezů informačních a komunikačních technologií se staly natolik běžnými, že státy zakomponovaly pokyny, jak nakládat s digitálními důkazy mezi své vnitrostátní právní předpisy. (CASEY, 2009)

Vyšetřování vniknutí do korporátních nebo státních informačních systémů závisí na kvalitě získaných digitálních stop. Zajišťování forenzních digitálních stop se stává postupem času náročnější, jelikož útočníci na počítačové systémy využívají stále důmyslnější způsoby, jak svých cílů dosáhnout, a to včetně důrazu na důkladné skrývání digitální stop po své záškodné činnosti v prostředí kybernetického světa. (WILLIAMS, 2021)

Počítačová forenzní analýza je praktikum získávání, analyzování a klasifikování digitálních dat eticky přípustně a v souladu se zákonem. Získaná data mohou býti využita při detekci a prevenci zločinu a ve kterémkoliv právním případě, kde jsou důkazní materiály přítomny ve formě digitálních dat. Digitální forenzní analýza využívá podobných procesů a přístupů jako ostatní forenzní vědy, zároveň se potýká s obdobnými problémy. (GOGOLIN, 2021)

3.2 Historie vzniku digitální forenzní analýzy

V sedmdesátých letech 20. století nebyly počítačové systémy dostupné běžnému spektru populace. Počítače se využívaly ve velkých soukromých organizacích nebo ve státním sektoru. Skutečnosti týkající se aplikace metod forenzní analýzy v tomto období nejsou historicky známé. Globálně můžeme hovořit o původu forenzní analýzy až v roce 1984, kdy začaly v laboratořích federálního úřadu pro vyšetřování a v ostatních donucovacích orgánech specializovaných na boj proti různým formám trestné činnosti vznikat první

druhy softwaru pro účely zkoumání digitálních důkazů. Andrew Rosen vyvinul historicky první software, který měl sloužit výhradně pro účely digitální forenzní analýzy. (BODDINGTON, 2016)

V důsledku zvyšování dostupnosti počítačových systémů běžným civilním subjektům začala vznikat záliba objevování a využívání zranitelností této nové technologie. Jako odpověď na zvýšené množství kybernetických útoků na počítače a počítačové sítě začaly soukromé i vládní organizace navrhovat a implementovat bezpečností politiky a protiopatření. (BODDINGTON, 2016)

3.3 Druhy zajistitelných digitálních důkazů

Prostřednictvím nástrojů pro zajišťování forenzních digitálních důkazů lze extrahovat z cíleného počítačového systému prakticky kterýkoliv druh dat. Některé ze souborů lze obnovit i po předešlém smazání systémem či uživatelem. V několika následujících odstavcích budou představeny nejčastěji vyskytující se druhy dat.

3.3.1 Elektronická pošta

Forenzní analýza e-mailů je využívána ke zkoumání zdroje a obsahu e-mailu jako důkazního materiálu. K takovému zkoumání se využívá uložených e-mailových souborů ve formátu „.eml“. Každý takový soubor se skládá ze dvou hlavních částí, ze záhlaví a těla, přičemž záhlaví e-mailu obsahuje vlastní vnořené komponenty, které představují atributy obsahující informace např. o reálném odesílateli, příjemci, času odeslání apod. (BOGHDANOSKI, 2018)

Výčet hlavních komponent záhlaví e-mailu a jejich obsažené informace:

- X-Apparently-To: Pole obsahuje e-mail příjemce a může taktéž sloužit k ověření poskytovatele e-mailové služby;
- Return-Path: Pole obsahuje cestu proběhlé komunikace pro případ, že e-mail nebylo možné doručit;

- Received-SPF: Pole obsahuje informace o e-mailové službě, která byla využita pro zaslání e-mailu. Disponuje také jedinečným identifikátorem, který slouží k identifikaci všech záznamů logů komunikace;
- Message ID: Pole obsahuje jedinečný identifikátor, který odkazuje na reálný čas proběhnuté e-mailové komunikace a poskytuje reálnou verzi zprávy. Jedná se o důležitou položku pro forenzní znalce, protože na jejím základě lze určit, zda došlo k podvržení odesílatele nebo jiných parametrů v e-mailu;
- Content-type: Pole obsahuje typ obsahu e-mailu nebo formát kódování (HTML, XLML, Plain Text);
- X-Mailer: Pole obsahuje informaci o verzi klienta, přes který byla zaslána konkrétní zpráva;
- X-Originating-IP&Received: Pole obsahuje informace o IP adrese, ze které došlo k odeslání e-mailu. (BOGHDANOSKI, 2018)

Obrázek 1: Ukázka obsahu headeru e-mailové zprávy

```
Received: from mailer.abc.uk ([XXX.XXX.XXX.XX2]) by
  mailtr.an.organisati.on with esmtp (Exim 4.80) id 1Y25L6-0002zV-oA
  for joe.monday@an.organisati.on; Sun, 14 Dec 2014 18:30:01 +0000
Received: from [XXX.XXX.XXX.XX1] (helo=[192.168.1.8]) by mailer.abc.uk
  (Postfix) with ESMTPSA (envelope-from <john.smith@abc.uk>) id
  2312312132; Sun, 14 Dec 2014 18:30:00 +0000
Content-Type: multipart/alternative;
  boundary="Apple-Mail-QWNHJDNF-KJDD"
MIME-Version: 1.0 (1.0)
Subject: Information on the purchase order
From: John Smith <john.smith@abc.uk>
X-Mailer: iPad Mail (12B440)
Date: Sun, 14 Dec 2014 18:30:05 +0000
CC: Pat Tuesday <pat.tuesday@an.organisati.on>
Content-Transfer-Encoding: 7bit
Message-ID: <KJDKUJSK-EOI-K2LS-DJFD-KJSD49SEI@abc.uk>
To: Joe Monday <joe.monday@an.organisati.on>
X-Username: jksmith3
Return-Path: john.smith@abc.uk
```

Zdroj: https://www.researchgate.net/figure/A-simple-example-of-the-contents-of-an-email-header-Here-we-can-observe-that-the_fig1_274663733

3.3.2 Digitální obrazové soubory

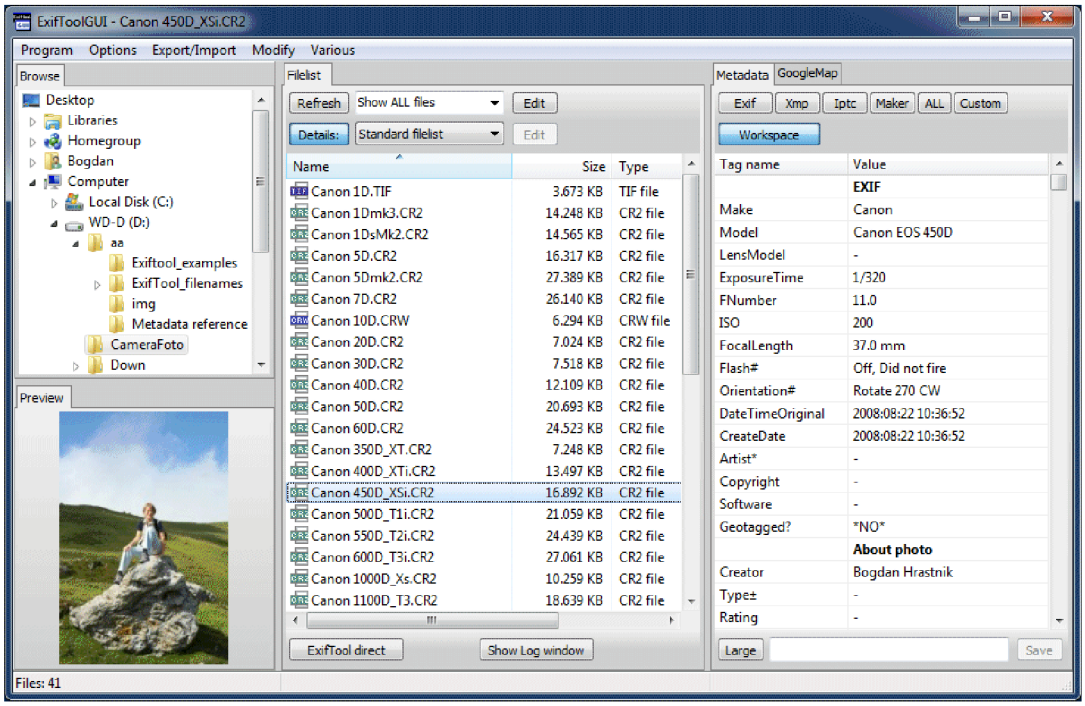
Digitální obrazové soubory se většinou ukládají ve formátu JPEG, tyto soubory obsahují mimo samotný digitální obraz taktéž značné množství metadat. Metadata jsou data, která poskytují dodatečné informace o jiných datech. Při investigaci mohou metadata sehrát významnou roli, jelikož se v nich nachází důležité informace, které běžným pohledem z otevření souboru digitálního obrazu nelze vyčíst. (Fan a kol., 2011)

Způsob, kterým se do grafických souborů ukládají metadata, nese název EXIF. Jedná se o zkrácený výraz pro Exchangeable image file format a jde o specifikaci formátu vkládání metadat do souborů JPEG, TIFF, PNG a jim podobných. Metadata obsahují mnoho podstatných informací, které by mohly být klíčovým důkazem při vyšetřování různých trestních deliktů. (FAN A KOL., 2011)

Možné informace obsažené v EXIF metadatech:

- Značka a model fotoaparátu;
- Datum a přesný čas pořízení snímku;
- Některá z nastavení použitého fotoaparátu (citlivost, clona, ohnisková vzdálenost, použití blesku);
- Náhled snímku;
- Geologická lokace pořízení snímku.

Obrázek 2: Ukázka ExitToolGUI



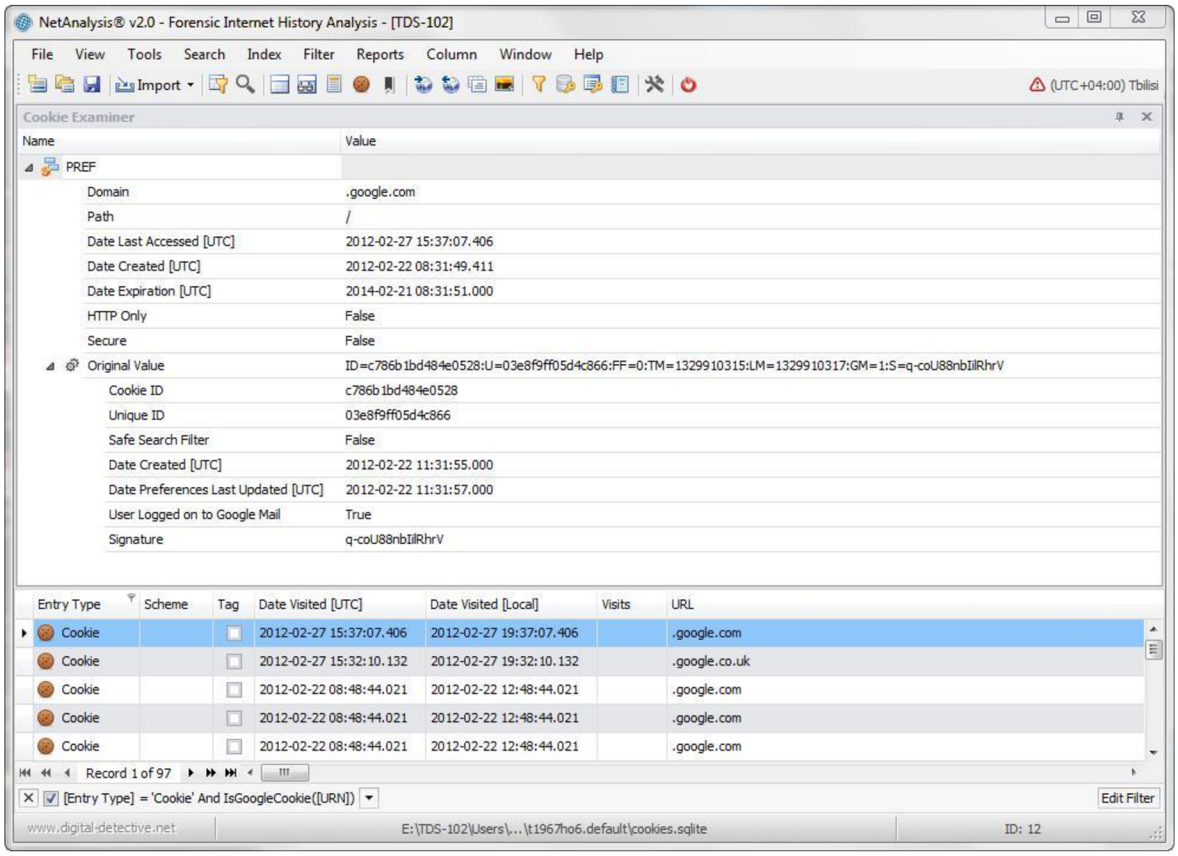
Zdroj: https://exiftool.org/gui/

3.3.3 Aktivita webového prohlížeče

Webový prohlížeč může být použit při páchání trestné činnosti. Hledání důkazů pozůstatků dat, která vznikají při používání webových prohlížečů, bývají velmi častým digitálním důkazním materiálem. Při podrobném zkoumání těchto dat lze zjistit např. výčet navštívených webových stránek včetně frekvence návštěv, řetězce dat, které uživatel zadával do vyhledávačů, dále cookies, seznam stahovaných souborů a dočasně uchovávaná data. (GOGOLIN, 2021)

Většina webových prohlížečů disponuje možností využít funkcionality „private browsing“, pomocí níž dochází k deaktivaci automatického ukládání historie navštívených stránek a dočasně uchovávaných souborů. Takové nastavení umožňuje využívat webové prohlížeče tak, aby nebylo možné jinak lokálně ukládaná data později obnovit a analyzovat. Ovšem funkčnost „private browsing“ bývá narušena využíváním plug-inů prohlížečů, které často toto nastavení ignorují, a přesto ukládají data. (HAYES, 2019)

Obrázek 3: Ukázka nástroje pro analýzu dat webového prohlížeče



Zdroj: https://malware.news/t/netanalysis-v2-10-and-hstex-v4-10-released/31911

3.3.4 Data z komunikačních nástrojů (Instant messaging)

Instant messaging je druh textově založené komunikace převážně mezi dvěma osobami v jedné konverzaci vedené přes jejich osobní počítač, chytrý telefon nebo další druhy zařízení s možností využití instant messaging aplikací.

V první řadě je nutné identifikovat umístění hledaných dat. V závislosti na druhu konkrétní aplikace může být umístění různé. Stejně tak se bude lišit druh dat, který je ukládán na lokální úložiště zařízení, formát, ve kterém jsou data uchovávána, způsoby, jakými mohou být data získána, zpřístupněna a analyzována. Na lokální úložiště je ukládáno pouze určité množství specifických dat. Značná část dat vzniklých na základě instant messaging komunikace není ukládána na lokální úložiště uživatelů. (SGARAS A KOL., 2014)

Základní taxonomie dat z komunikačních nástrojů:

- Instalační soubory: Data týkající se instalace instant messaging klienta na konkrétní zařízení;
- Provozní data: Provozní data jsou taková data, která jsou zpracovávána pro účely přenosu po komunikačních a telekomunikačních sítích. Taková data se mohou vzorek od vzorku lišit, často obsahují údaje o času a geologické lokaci;
- Obsahová data: Obsahují konkrétní obsah komunikace, můžou být ve formátu textu, audio souborů, video souborů apod.;
- Data profilu uživatele: Týkají se profilu uživatele aplikace, typicky obsahují jméno uživatele, příjmení, datum narození, pohlaví, profilový obrázek, adresu, telefonní číslo a e-mail;
- Přenesené přílohy: Soubory, které byly přeneseny pomocí funkcionality přenosu souborů prostřednictvím aplikace. (SGARAS A KOL., 2014)

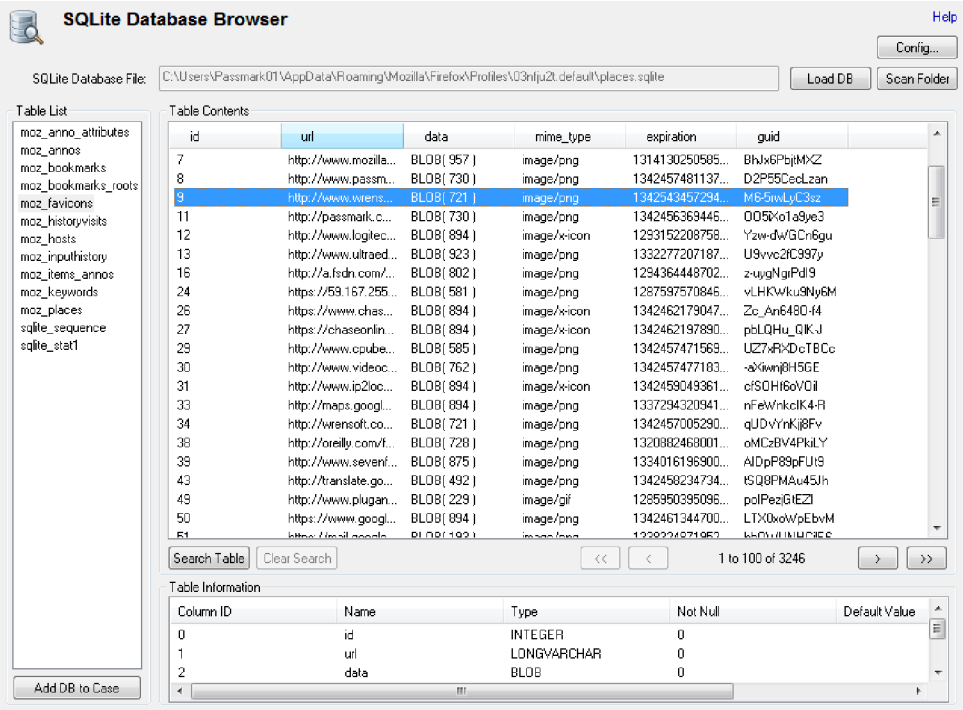
3.3.5 SQLite Databáze

Soubory SQLite databází jsou velmi často využívány nejrůznějšími aplikacemi pro účely uchovávání dat ve spořádané a strukturální formě. SQLite je knihovna jazyka C, která implementuje engine SQL databáze nevyžadující zvláštní systémový proces. Jedná se o relační databázi složenou z tabulek obsahující jednotlivé záznamy dat. Z důvodu možnosti vyvíjet databáze odlišnými a specifickými přístupy je znalecká činnost při zkoumání SQLite databází netriviální proces. Tento druh databází se nejčastěji využívá v aplikacích, jako jsou webové prohlížeče a klientský software instant messaging aplikací. (KÄVRESTAD, 2020)

Při zkoumání databází je zásadní znalost způsobu, jak jsou data zapisována do databáze a mazána. Při zápisu dat do databáze SQLite využívá „write-ahead log“ nebo také „rollback-journal“. Oba zmíněné způsoby jsou velice obdobné. Jestliže data v databázi musí být modifikována, informace o změně je zapsána do „write-ahead log“ nebo „rollback-journal“ nebo přímo do databáze. Vždy, když je aplikace připravena pro commit změn v „write-ahead log“ nebo „rollback-journal“ nebo při zaplnění, tak se změny zapíší do databáze. Z tohoto vyplývá, že při forenzním zkoumání databáze je možné, že neobsahuje všechna data, protože může obsahovat změny, při kterých neproběhl

commit, a tudíž jsou obsažené pouze v „write-ahead log“ nebo „rollback-journal“. Tyto logovací soubory jsou umístěny ve stejné složce jako samotná databáze. (HASSAN, 2020)

Obrázek 4: Software pro analýzu SQLite DB



Zdroj: https://www.osforensics.com/sqlite-database-browser.html

3.3.6 Odkazové soubory systému Windows

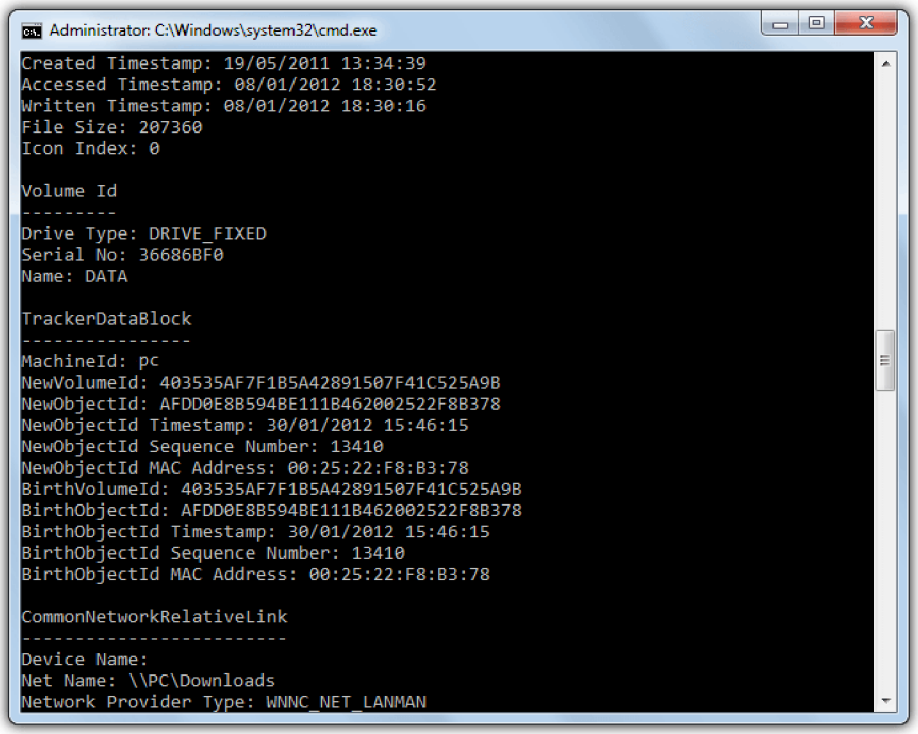
Soubory s koncovkou LNK jsou popisovány jako druh metadat, který odkazuje na aplikaci nebo soubor v operačním systému Windows. Takovéto soubory jsou často objevovány například na pracovní ploše uživatele, můžou ale existovat i v jiných částech file systému počítače. LNK soubory jsou automaticky vytvářeny operačním systémem samotným nebo také uživatelem. Odkazové soubory LNK obsahují množství užitečných informací. (WILLIAMS, 2021)

LNK soubory obsahují následující užitečné informace pro forenzní analýzu:

- MAC atributy (čas tvorby, modifikace a přístupu);

- Předešlé uživatelské aktivity (například jestliže uživatel smaže soubor, tak jemu asociovaný LNK odkaz zůstane zachován v počítači s informacemi, že se v minulosti v daném systému soubor vyskytoval);
- Velikost souboru, na který odkaz odkazuje;
- Původní cesta odkazovaného souboru;
- Identifikační číslo a název svazku, kde se nachází linkovaný soubor. (HASSAN, 2020)

Obrázek 5: Data LNK souborů



Zdroj: https://www.raymond.cc/blog/parse-and-analyze-windows-lnk-shortcut-files/

3.3.7 Data registrů operačního systému

Registry operačního systému Windows jsou dobrým zdrojem informací o nastavení a využití zkoumaného počítače. Registry jsou získávány z bitové kopie hard disku na systémovém oddílu ve složce „C:\Windows\System32\config\“. Dalším zdrojem je NTUSER.dat, který se zpravidla nachází v root adresáři každého uživatele systému. Je důležité zmínit, že některé klíče registrů se automaticky neaktualizují, ale aktualizují

se až s vypnutím počítače. Tudíž zachycená data registrů nemusí být aktuální v případě, že provádíme zajištění dat registrů na živém systému. Dobrý nápad může být provést kopii registrů při živém systému, posléze také z bitové kopie, která byla zajištěna z vyjmutého datového média z vypnutého počítače. (KÄVRESTAD, 2020)

3.3.8 Data síťové komunikace

Jedná se o data, která mohou být důležitá při kriminálním vyšetřování trestních činů. Ze získaných dat sítě a informací ze síťových prvků lze zjistit, co se opravdu aktuálně v síti dělo. V reakci na incident je typické, že mohl být malware, kterým se infikoval počítač v síti, využit k rozesílání závadných e-mailů dalším organizacím. V tomto případě by bylo na prvním místě nutné identifikovat závadného hosta, a to se nejlépe podaří pomocí monitoringu síťového toku a identifikace původce těchto závadných e-mailů. Monitorování a získávání dat síťové komunikace lze provádět mnoha nástroji. Tato data obsahují například informaci, kdo s kým komunikoval, přes jakou službu, port a jiné. (HASSAN, 2019)

3.3.9 Ostatní podstatná systémová data

Mezi ostatní data generovaná činností operačního systému se řadí např. event viewer logy, aktivní procesy, uživatelé systému či historie připojených USB zařízeních. Tato data mohou hrát důležitou roli při forenzní analýze, jelikož je možné, že obsahují zásadní informace o chování systému. (ZBROG, 2021)

3.4 Bitová kopie systému a dump operační paměti

Forenzní bitová kopie je přesná kopie datového média, která probíhá kopírováním každého jednoho bitu. Soubory, složky, logické svazky a další mohou být zajištěny. Forenzní bitová kopie zachytí veškeré struktury na pevném disku. Použití pouhého systémového kopírování není totožné s bitovou kopií. (BOGHDANOSKI, 2018)

Dump operační paměti je snapshot operační paměti, který se zajišťuje pro potřeby analýzy obsahu paměti RAM. RAM dump obsahuje veškerá data týkající se všech běžících procesů v čase, kdy je dump zajištěn. (SGARAS A KOL., 2014)

3.4.1 Bitová kopie systému

Proces zajištění bitové kopie se zabývá vytvořením takové kopie hard disku nebo jiného datového média, která by byla využitelná pro účely dalšího forenzního zkoumání. Důležitým aspektem forenzního zkoumání je ujistit se, že data na datovém médiu nebyla kompromitována. Z tohoto důvodu je běžná praxe provést bitovou kopii systému, a posléze ji analyzovat, nikoliv analyzovat živý systém. Práce s bitovou zálohou přináší také i jiné výhody, a to primárně zvýšení rychlosti práce s daty. Jako nejbezpečnější způsob, jak extrahovat z cíleného datového média bitovou kopii, se udává postup, kdy forenzní technik pověřený zajištěním dat fyzicky vyjme datové médium z počítače, následně ho připojí ke svému počítači pomocí write blockeru. Write blocker je hardwarové zařízení, které zamezí počítači zapisovat data na zkoumaný disk. Alternativou k write blockeru je připojit disk k počítači v režimu read only. Taková kopie systému vzniká kopírováním dat od prvního do posledního bitu, čímž vznikne identická kopie hard disku. Pokud se jedná o disk, který je encryptován, bude encryptována i vzniklá kopie. Z toho důvodu se v případě takového disku provádí logická kopie disku, která následně obsahuje data disku viděná počítačem. Výrazně se tak redukuje šance na obnovení smazaných souborů. (KÄVRESTAD, 2020)

3.4.2 Dump operační paměti

Operační paměť může obsahovat značné množství zajímavých informací včetně hashovacích klíčů, encryptovaná data v decryptovaném formátu a další. Zajištění operační paměti lze provést pouze za běhu operačního systému. Data, která operační paměť obsahuje, jsou volatilní tím způsobem, že se při vypnutí počítače ztratí. Každopádně by se dump operační paměti měl v rámci digitální forenzní analýzy provádět vždy, kdy je to možné. Důležité je zmínit, že výstupem nástrojů zachycující dump operační paměti je soubor, který může přesahovat velikost 4 GB. Z této skutečnosti vyplývá,

že je nutné při dumpu operační paměti disponovat médiem, které není nakonfigurováno na file system FAT32, nýbrž na NTFS, HFS+ nebo například EXT4. (BODDINGTON, 2016)

3.5 Postupy při zajišťování forenzních dat

Počáteční reakce na incident je zásadně důležitý krok v procesu při zajišťování forenzních důkazů. Správné načasování prvotní reakce je kritické jak pro omezení škod a zamezení případnému laterálnímu pohybu škodlivého kódu mezi ostatní zařízení na síti, tak pro včasné zajištění forenzních digitálních dat před nežádoucím narušení jejich integrity, či dokonce ztráty (například v případě ztráty obsahu paměti RAM po vypnutí počítače). Klasický postup vyjmutí hard disku z počítače a posléze analyzovat jeho kopii není praktický a v některých případech z reálné praxe je i nemožný. (HASSAN, 2019)

V dnešní době vývoj informačních a komunikačních technologií dovedl mnoho společností k distribuci sítí mezi odlišná města, státy a kontinenty. Výše zmíněné způsobuje, že mohou nastat případy, kdy nelze z geografických důvodů provést vyjmutí fyzického disku. V těchto případech by mělo dojít k zajištění nezbytných důkazů vzdálenou formou připojení. Další překážkou mohou být nadměrně velká disková pole, která mohou obsahovat tisíce uživatelů a nadměrné množství uživatelských dat, což by vedlo ke zvýšení obtíži identifikovat hledaná data a také k navýšení potřebného času k analýze. Typicky se takto rozměrná datová média užívají v serverech, kde může být dalším problémem nemožnost odstavení systémů z důvodů způsobení újmy společnosti, která tato zařízení provozuje. (KÄVRESTAD, 2020)

V případech, kdy z jakýchkoliv důvodů nelze provést fyzické vyjmutí hard disku z počítače k účelu vytvoření bitové kopie, je nutné využít technik analýzy živého systému. Důležité je podotknout, že v případě živé analýzy systému nikdy nelze zamezit vzniknutí nežádoucích změn. Připojíme-li USB zařízení nebo dojde-li k síťové komunikaci, přihlášení uživatele nebo ke spuštění spustitelného souboru, dojde vždy k modifikaci logů, hodnot registrů nebo dalších událostí. Z toho důvodu je nutné evidovat změny způsobené zásahem forenzního technika. (ZBROG, 2021)

3.5.1 Zajišťování dat ze živého systému

V případě sběru forenzních stop ze živého systému již nelze zamezit pozměnění forenzních dat, jelikož při práci se softwarovým vybavením zařízení dochází k zápisu a čtení na disku, toto riziko nelze eliminovat. Lze ale postupovat takovým způsobem, aby byla zajištěna veškerá potřebná forenzní data. Mimo provedení bitové kopie systému, dumpu operační paměti a sběru obsahu registru je nutné zaměřit se také na nastavení data a času, aktivní uživatele, zařízení připojená pomocí USB nebo také síťová data a aktivní procesy. (HAYES, 2019)

Autor Joakim Kävrestad uvádí, že vhodný způsob, kterým lze postupovat při zajištění dat ze živého systému, spočívá v posloupnosti činností forenzního technika. Vhodné je začít zajišťovat takové důkazy, jejichž sběrem nedojde k ohrožení běhu operačního systému zkoumaného zařízení ve smyslu zredukování šancí na neočekáváné vypnutí nebo navození stavu hibernace počítače. Zároveň by forenzní technik měl upřednostnit sběr takových dat, která jsou nejvíce relevantní konkrétnímu aktuálnímu případu. (KÄVRESTAD, 2020)

Posloupnost kroků dle autora Joakima Kävrestada:

1) Zajistit síťová připojení a odpojit počítač z internetové sítě;
2) Vypnout automatické hibernování systému;
3) Zdokumentovat běžící programy a procesy;
4) Zjistit historii připojených zařízení pomocí USB;
5) Zjistit na zařízení aktivaci encrypce dat;
6) Provést dump operační paměti a obsahu registrů;
7) Provést bitovou kopii disku.

3.5.2 Zajišťování dat z neživého systému

Dostane-li se forenzní technik k zařízení, které je ve vypnutém stavu, tak se dramaticky redukují možnosti zajišťování forenzních dat. V tomto případě se jediná data nachází na statické paměti, např. na pevném disku zařízení, ze kterého je nutné vytvořit bitovou kopii. Při vyjmutí disku a připojení k zařízení, na kterém je prováděna bitová kopie, je nutné zamezit jakémukoliv zápisu na zkoumané paměťové médium, aby nedošlo

ke znehodnocení důkazního materiálu nebo stop. K tomuto účelu slouží hardwarová zařízení tzv. „write blockery“. (SGARAS A KOL., 2014)

3.5.3 Write blocker

Write blocker je hardwarové zařízení, které umožňuje číst data z hard disků se znemožněním datového zápisu na použité zkoumané médium. Bývá prodáván v balíčcích, které obsahují více druhů blockerů, napájecí adaptér a kabely, které jsou zakončeny konektory jako např. eSATA, SATA, IDE, SCSI, USB apod. Podobně se používají write blocking čtečky karet. Zamezení zápisu dat na datové médium zamezí vzniku změn, a tudíž narušení integrity dat při zajišťování bitové kopie disku. (HAYES, 2019)

Obrázek 6: Zařízení write blocker

Zdroj: https://security.opentext.com/tableau/hardware/details/t35u-rw

3.5.4 Zajišťování dat z virtuálních stanic

V současné době vzrůstá v komerčních prostředích potřeba velkých diskových polí a pokročilých výpočetních zdrojů. Z těchto důvodů začaly společnosti využívat data centra, cloudové služby a různá virtuální prostředí, a proto je forenzní analýza virtuálních

desktopů již běžným standardem. Virtualizace se poprvé objevila v 60. letech 20. století, kdy společnost IBM začala experimentovat s virtuálními počítači. Virtuální počítač funguje ideálně v prostředí fyzického počítače. Virtuální zařízení se opírá o software, který se chová jako procesor, operační paměť a podobně. Na jedné fyzické stanici může být zároveň spuštěno několik virtuálních stanic, každá z nich je izolovaná od ostatních. (KHANGAR, 2012)

Virtuální stanice jsou velice vhodné pro potřeby forenzních techniků. Získané bitové kopie při forenzní analýze lze spustit prostřednictvím virtuálních desktopů. Tímto způsobem lze prošetřit přesný stav počítače, kdy byla bitová kopie zpracována, včetně hardwarových zdrojů nasimulovaných virtuálním prostředí. Ačkoliv virtualizace stále disponuje určitými limity, přidává alespoň možnost vizuálního prozkoumání operačního systému zkoumaného případu investigace. (ZBROG, 2021)

V případě potřeby sběru forenzních dat z virtuálních zařízení se může proces značně lišit v závislosti na konkrétním typu virtualizace. Většinou je třeba zajistit specifická data vytvořená na discích fyzického zařízení, které simuluje jím hostované virtuální desktopy. (KHANGAR, 2012)

Druhy dat, která mohou být vygenerována při hostování virtuálního zařízení typu VMware:

1) VMX: primární konfigurační soubor, který obsahuje informace o zvolené konfiguraci při tvorbě nového virtuálního desktopu;
2) VMXF: sekundární konfigurační soubor, který obsahuje konfiguraci zvolenou v konkrétním virtuálním stroji;
3) VMSD: obsahuje metadata o všech snapshotech virtuálního desktopu;
4) VMDK: popisuje strukturu disku a jeho nastavení, reprezentuje využitou část disku fyzického zařízení;
5) LOG: obsahuje logy virtuálního zařízení;
6) NVRAM: BIOS virtuálního zařízení;
7) VSWP: virtuální paměť, která se využije v případě, že zařízení potřebuje více paměti;
8) VMSS: reprezentuje stav pozastavené nebo suspendované virtuální stanice;
9) VHD: obsahuje bitovou kopii disku a MBR tabulku, tento typ souboru lze examinovat např. pomocí FTK Imager. (KHANGAR, 2012)

3.6 Porovnání nástrojů pro účely digitální forenzní analýzy

Nástroje pro digitální forenzní analýzu mohou být kategorizovány do několika odlišných skupin. Lze hovořit například o nástrojích zaměřených na analýzu databází, diskových polí, zaznamenávání dat, elektronické pošty, souborového systému, síťového toku, mobilních zařízení nebo také registrů operačních systémů. Značná část jednotlivých nástrojů softwarových balíčků avšak poskytuje více druhů kategorií najednou. Tyto nástroje bývají označovány jako „wrappers“. Bývá zvykem, že jeden balíček nástrojů obsahuje stovky specifických technologií s různými funkcionalitami. (ZBROG, 2021)

Nové nástroje jsou vyvíjeny každým dnem, ať se jedná o profesionální nástroje, na jejichž vývoj jsou vynaloženy nemalé finanční prostředky, nebo o nástroje vznikající v garážích a dílnách hackerských skupin. Každý z těchto druhů nástrojů se zpravidla zaměřuje na jiný styl užití. (ZBROG, 2021)

Výběr forenzních nástrojů pro profesionální užití by měl splňovat vlastní kritéria subjektů, které nástroj budou využívat. Těmito kritérií může být například cena, druh licence, přístupnost, spolehlivost. Primárně by ale měl výstup softwaru splňovat podmínky pro následnou využitelnost získaných dat pro orgány činné v trestním řízení. (BOGHDANOSKI, 2018)

Digitální forenzní zkoumání nebo odpověď na bezpečností incident pravděpodobně ve většině případech začne sběrem dat. Cílem je zajistit co největší množství dat z různých zdrojů, například data z pevných disků, registrů systému, obsah operační paměti a dočasné soubory. Často se také zajišťují data síťového toku ze zařízení, jako jsou router a switche. (SGARAS A KOL., 2014)

Mezi jednotlivými forenzními nástroji mohou existovat zásadní odlišnosti. Nástroje se mohou lišit například druhem licence, zda je produkt volně dostupný (open-source), placený jednorázovým poplatkem (buy-to-use) nebo na principu předplatného pro určité časové období (subscription-based). Některé nástroje mohou být dostupné pouze pro výhradní druh operačního systému nebo nemusí splňovat veškeré předpoklady, které by měl konkrétní nástroj splňovat. Nástroje pro digitální forenzní analýzu mohou plnit mnoho funkcí. (HASSAN, 2020)

Forenzní nástroje mohou plnit funkcionalitu prezervace, identifikace, extrakce a dokumentace. Při prezervaci provádí nástroj kopii datového média pro účely další forenzní analýzy. Nejběžněji se v literatuře popisují dva druhy kopií; bitová a logická kopie datového média. Při provedení bitové kopie provede nástroj kopii od prvního do poslední bitu, čímž vznikne přesná kopie celého zvoleného datového média. V případě využití logické kopie se provede kopie pouze zvoleného oddílu na disku. (WILLIAMS, 2021)

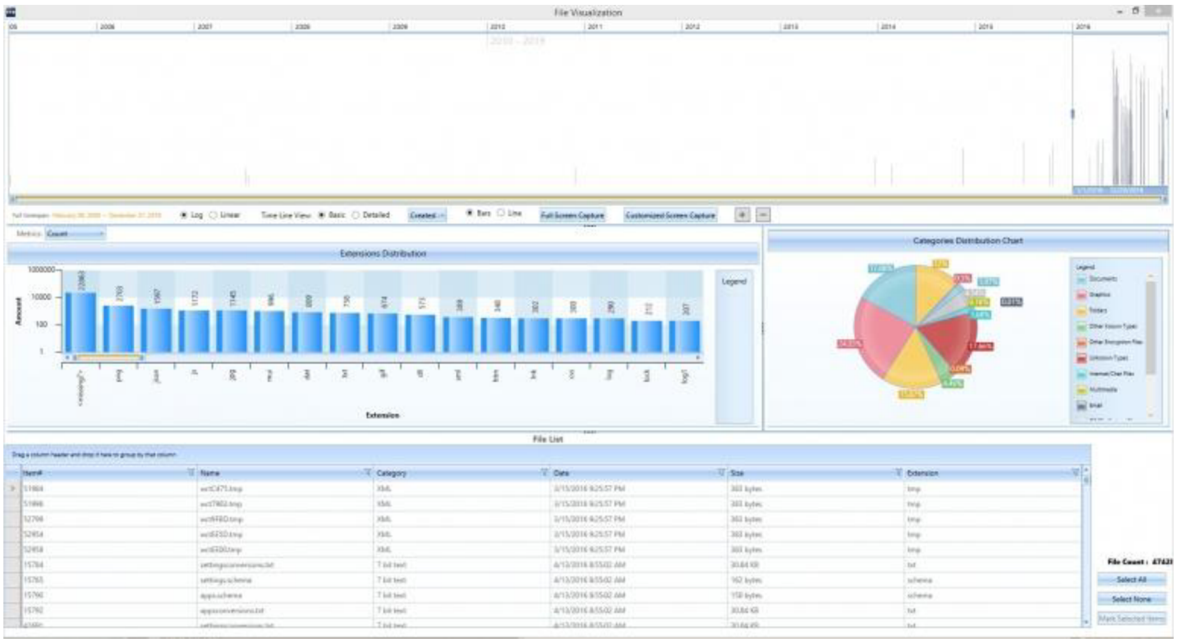
Funkce identifikace je potřebná k jednoznačné identifikaci a taktéž k zabezpečení integrity dat pomocí jednosměrných hashovacích funkcí. Většina nástrojů umožňuje uživateli volbu rovnou z několika druhů funkcí. Extrakce slouží například k funkcionalitě vyhledávaní důkazních dat na základě řetězců slov nebo indexů. Závěrem poslouží metoda dokumentace k tvorbě dalších ověřených kopií dat pro účely následného vyšetřování. (WILLIAMS, 2021)

3.6.1 FTK Forensic Toolkit

Nástroj FTK Forensic Toolkit od společnosti Accessdata slouží k softwarovému vytváření bitových nebo logických kopií datových médií bez způsobení změn původních forenzních důkazů, a k jejich analýze. Lze využít taktéž i v případě živé analýzy systému pro účely získání dumpu operační paměti. Veškerá data vygenerována pomocí nástroje FTK jsou posléze ověřována použitím hashovacích funkcí. Mezi jeho další funkcionality patří například: (www.accessdata.com, online)

- Dešifrování souborů a prolomení hesel;
- Analýza souborů registru operačního systému;
- Obnovení již smazaných souborů;
- Možnost rychlé lokalizace a izolace dat z instant messaging aplikací;
- Vizualizace pomocí grafů. (www.accessdata.com, online)

Obrázek 7: FTK Toolkit GUI



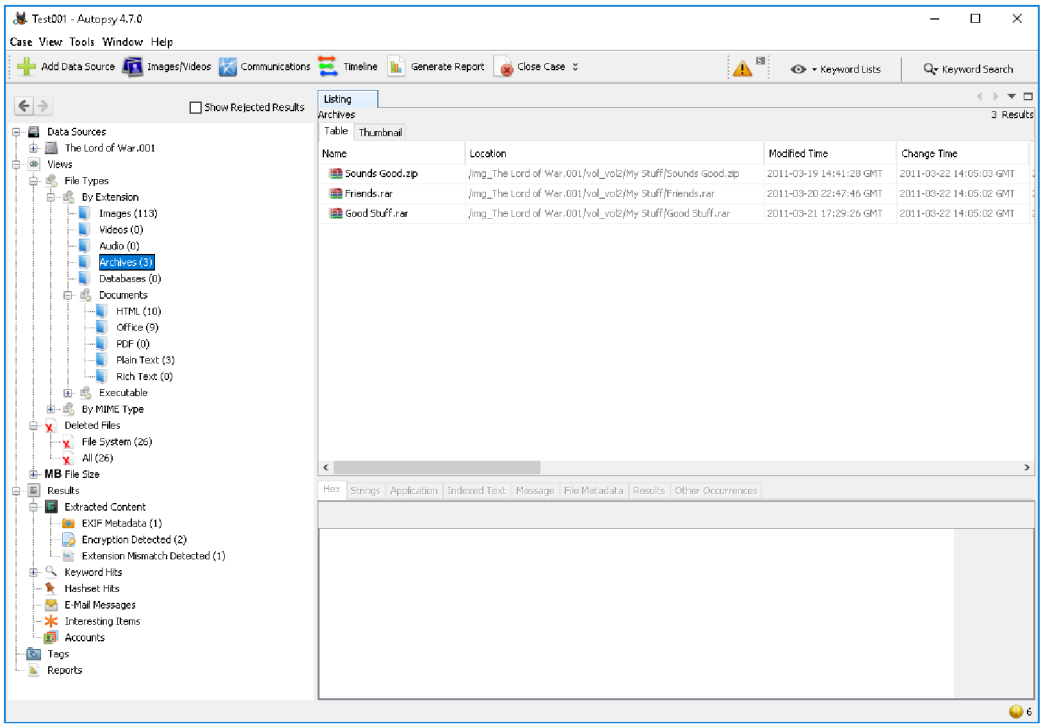
Zdroj: https://www.getapp.com/legal-law-software/a/forensic-toolkit-ftk/

3.6.2 Autopsy

Autopsy je open source nástroj pro účely forenzní analýzy, který je dostupný zcela zdarma. Jedná se o grafické a uživatelské rozhraní pro The Sleuth Kit (TSK). TSK byl původně vydán v roce 2001. Jde o soubor příkazů příkazového řádku, pomocí nichž lze zkoumat paměťová média pro účely digitální forenzní analýzy. Obsahuje funkce například jako: (https://www.sleuthkit.org/, online)

- Obnovení smazaných souborů;
- Vyhledávání podle klíčového slova nebo čtení ze souborů metadat;
- Multi-user network kolaborace;
- Efektivní korelace dat;
- Extrakce e-mailových zpráv;
- Podpora přídavných modulů. (https://www.sleuthkit.org/, online)

Obrázek 8: Autopsy GUI



Zdroj: https://www.sleuthkit.org/autopsy/

3.6.3 DEFT

DEFT (Digital Evidence and Forensic Toolkit) je modifikovaná distribuce Ubuntu Live CD, která byla poprvé publikována v roce 2005. Je složena z GNU/Linux prostředí a DART (Digital Advanced Response Toolkit). DEFT je často využíván v bezpečnostně informační komunitě a forenzními techniky příslušných orgánů. (www.linuxandubuntu.com, online)

Mezi nejdůležitější nástroje obsažené v DEFT patří:

- Diskový manažer se statusem připojení disku;
- Kompletní podpora bitlockerem encrypted disků;
- The SleuthKit;
- Digital Forensic Framework;
- Podpora Android a IOS akvizicí dat;
- Skype extractor a další, ...

Obrázek 9: Deft

Zdroj: https://archiveos.org/deft/

Součást DART obsahuje Windows aplikace, které jsou využitelné z důvodu neexistujících alternativ Unixových verzí. DART je aplikace, která sbírá, organizuje a spouští software v nouzovém režimu pro účely živé forenzní analýzy. Důležitou funkcionalitou je kontrola integrity aplikace před jejím samotným spuštěním. (www.linuxandubuntu.com, online)

3.6.4 CAINE

Podobně jako DEFT je CAINE další GNU/Linux Live CD distribucí pro účely digitální forenzní analýzy. CAINE nabízí forenzní prostředí, které obsahuje integrované a organizované již existující softwarové nástroje a moduly s přehledným uživatelským rozhraním. (www.caine-live.net, online)

Hlavní cíle tohoto projektu jsou:

- Poskytnout interoperativní prostředí pro forenzního technika ke všem fázím digitálního zkoumání;
- Uživatelsky přívětivé grafické rozhraní;
- Uživatelsky přívětivé nástroje. (www.caine-live.net, online)

Obrázek 10: Caine

Zdroj: https://www.caine-live.net/

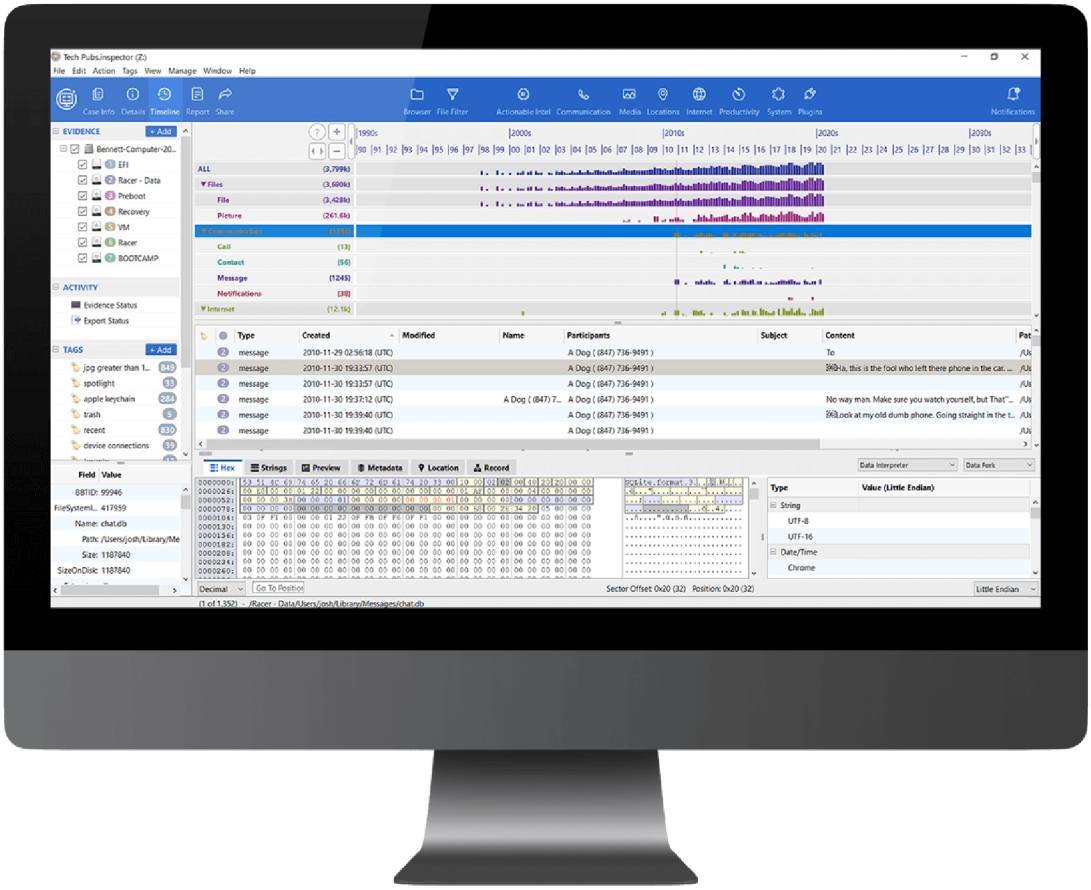
3.6.5 Cellebrite Inspector

Společnost Cellebrite založená roku 1999 v Izraeli Petagem Tikvou disponuje širokou nabídkou forenzních a bezpečnostních nástrojů vhodných pro různé účely. Poskytuje taktéž služby federální sféře a soukromým institucím, mezi tyto služby patří například sběr forenzních dat a jejich analýza. (www.cellebrite.com, online)

Pro potřeby digitálního zkoumání zařízení se systémem Windows slouží především produkt Cellebrite Inspector. Funkcionalitu zastává software používaný pro šetření a kategorizaci dat z digitálních forenzních kopií, např: (www.cellebrite.com, online)

- Rychlá a efektivní kategorizace a lokalizace dat;
- Silné filtrovací možnosti;
- Možnost procházet nestandardní datové objemy;
- Reporty jedním kliknutím;
- Dokáže zobrazit historii stínových kopií Windows souborů;
- Vestavěná analýza operační paměti a registrů systému;
- Automatické parsování uživatelských dat a aktivit do časové osy.

Obrázek 11: Cellebrite Inspector



Zdroj: https://cellebrite.com/en/inspector/

3.6.6 Další nástroje

WireShark

Světově široce využívaný nástroj k analýze síťového protokolu, který byl založen jako projekt Geraldem Combsem roku 1998, disponuje celou řadou funkcí, jako jsou například: (www.wireshark.org, online)

- Hloubková inspekce stovek protokolů;
- Živé odchytávání packetů a offline analýza;
- VoIP analýza;
- Umožňuje číst a zapisovat do několika různých souborových formátů (tcpdump, Pcap NG, Cisco Secre IDS iplog, Novell LANAnalyzer, Microsoft Network Monitor a další.);
- Export dat do XML, CSV, PostScript a pouhý text. (www.wireshark.org, online)

Registry Recon

Software vyvinutý společností Arsenal Record, který slouží jako forenzní digitální analýza pro účely získání, obnovení a parsování dat z registrů operačního systému Windows. Manuální získávání obsahu dat registrů je velice časově náročný proces a zároveň vzniká možnost neúmyslného vynechání důležitých častí dat. Registry Recon uživatelům nabízí například: (www.forensicfocus.com, online)

- Obnovení Windows registrů z předešlých instalací operačního systému;
- Přístup ke smazaným hodnotám registrů;
- Přístup ke všem instancím klíčů registrů a jejich hodnot;
- Bod obnovy a podpora shadow copy;
- Zobrazit klíče a jejich hodnoty ve specifickém bodě času. (www.forensicfocus.com, online)

Magnet RAM Capture

Jedná se o zdarma distribuovaný nástroj umožňující zachycení obsahu (dump) operační paměti počítače, umožňuje forenznímu technikovi obnovit a analyzovat důležité artefakty, které se zpravidla nachází pouze v paměti. Soubory jsou vygenerovány ve formátu .DMP,

RAW nebo .BIN, z toho důvodu lze posléze vygenerovaná data uploadovat a zkoumat v nejmodernějších forenzních nástrojích. (www.magnetforensics.com, online)

ExifTool

ExifTool je zdarma dostupný open-source nástroj sloužící ke čtení a zápisu metadat obrázkových souborů, video souborů, audio nahrávek a PDF. Aplikace je dostupná ve formě Perl knihovny nebo aplikace příkazového řádku. ExifTool podporuje celou řadu druhů metadat (Exif, IPTC, XMP, JFIF,GeoTIFF atd.). (https://exiftool.org/, online)

Nmap

Nmap („Network Mapper“) je zdarma ke stažení open source software určený k zjišťování síťových prvků na síti a k bezpečnostnímu auditu. Užívá se také k inventurním účelům pro potřeby administrátorů. Nmap využívá raw IP paketů ke zjištění, jaká zařízení se nacházejí na síti, jaké služby tato zařízení nabízí a také jakým operačním systémem disponují. Mimo jiné lze nástroj Nmap využít ke zjišťování bezpečnostních zranitelností v sítích, jako je například identifikace otevřených portů. (https://nmap.org/, online)

Hlavní funkcionality Nmap nástroje jsou:

- Zjišťování zařízení – Identifikace hostů v síti (utváření seznamu zařízeních, která odpovídají na TCP/ICMP dotazy nebo mají otevřené náležité porty);
- Skenování portů – Enumerace otevřených portů na daném hostu;
- Identifikace verzí – Zjišťování názvů a verzí aplikací na vzdálených zařízeních;
- TCP/IP otisk – Určení operačního systému a popisu hardware charakteristik síťových zařízení na základě inspekce síťové komunikace;
- Skriptování – Nmap podporuje skriptovací engine NSE a Lua programovací jazyk. (https://nmap.org/, online)

Magnet internet evidence finder

Magnet IEF umožňuje obnovit data hned z několika zdrojů a integrovat je v jeden report určený pro analýzu. IEF dokáže parsovat stovky artefaktů z počítačových systémů, včetně dat z úseků nepřiděleného místa na disku (unallocated space carving data). Automatická analýza poskytuje data v uživatelsky přívětivém formátu setříděná do stejných skupin.

Výstupem IEF může být např. HTML, PDF, Excel, CSV nebo XML soubor. (https://www.magnetforensics.com/products/magnet-ief/, online)

Volatility

První verze Volatility Frameworku byla vydána roku 2007. Vývoj tohoto softwaru byl podložen letitým akademickým výzkumem v oblasti pokročilé forenzní analýzy operační paměti. Do této doby byla digitální forenzní analýza primárně předmětem zkoumání artefaktů obsažených v bitových kopií datových medií. Volatility Framework lze využít pro zkoumání volatilních dat v RAM paměti. (https://www.volatilityfoundation.org/about, online)

USBDeview

USBDeview představuje freeware pomocný nástroj vyvinutý společností NirSoft. Po jeho spuštění dostane uživatel informace o všech USB zařízeních, která byla k pracovní stanici připojena. Nezobrazí pouze informace o aktuálně připojených zařízeních, ale taktéž o historii všech zařízeních, která byla připojena k zařízení v minulosti. USBDeview poskytne uživateli informace např. jako název a typ zařízení, sériové číslo, kdy bylo zařízení naposledy připojeno apod. Tato aplikace nevyžaduje ke spuštění instalaci do operační systému, tudíž lze spustit i z externích médií, což ji dělá vhodnou pro využití při zajišťování digitálních forenzních dat. (https://www.volatilityfoundation.org/about, online)

CMD Příkazy

Operační systém Windows 10 disponuje dvěma příkazovými řádky, a to sice Command shellem a PowerShellem. Každý z nich poskytuje přímou komunikaci mezi uživatelem a operačním systémem nebo aplikací. Command shell byla první příkazová řádka vestavěna do operačního systému. Pomocí CMD příkazů lze např. automatizovat rutinní úkoly nebo spouštět složité scripty.

PowerShell byl vytvořen pro rozšíření schopností CommanShellu. V příkazové řadce PowerShell se spouští příkazy tzv. Cmdlety. Tyto příkazy poskytují větší flexibilitu pomocí rozšíření externího skriptovacího jazyka. (https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands, online)

Příklady užitečných příkazů pro potřeby forenzní analýzy:

- Net user – spuštění příkazu vyobrazí seznam všech uživatelských účtů na počítači;
- Netstat – vypíše aktivní TCP spojení a porty, na kterých počítač naslouchá;
- Tasklist – zobrazí seznam aktuálně běžících procesů na lokálním počítači;
- Manage-bde-status – poskytuje informace relevantních pro BitLocker o všech discích připojených k počítači. (https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands, online)

4 Vlastní práce

Praktická část diplomové práce se bude zabývat provedením bitové forenzní kopie dvou pracovních stanic disponujících operačním systémem Microsoft Windows 10. Forenzní kopie a data v nich obsažená budou posléze analyzována prostřednictvím vhodného softwaru, taktéž bude dodrženo zachování korektního postupu při provádění potřebných kroků vycházejících z odborné literatury citované v teoretické části této práce.

4.1 Testovací prostředí a využitý software

Pro potřeby instalace operačního systému byla zvolena platforma virtuálních stanic Oracle VM VirutalBox, kde došlo k vytvoření a instalaci dvou virtuálních desktopů. Každá ze stanic disponuje operačním systémem Microsoft Windows 10 Home, taktéž instalací uživatelského software, který se již na každé stanici mírně odlišuje. Každá stanice bude podléhat odlišnému scénáři zajišťování dat, a sice živé analýze v prvním případě a analýze neživé v případě druhém. Uživatelská činnost v rámci operačního systému byla nasimulována činností reálných uživatelů. K analytické práci byl využit software AccessData FTK Imager, USBDeview, Autopsy, Internet Evidence Finder, Volatility a také relevantní příkazy v příkazovém řádku operačního sytému. Výše zmíněný software byl zvolen na základě přívětivosti uživatelského rozhraní, funkcionality, licenční politiky a vlastností, které dělají software vhodný pro užití k účelům forenzní analýzy.

Instalace dodatečného uživatelského softwaru:

- Google Chrome;
- Mozzila Firefox;
- Avast;
- Total Commander;
- WinRAR;
- LibreOffice;
- CCleaner;
- InfranView;
- VLC media player;

- Java Runtime;
- Adobe Acrobat DC;
- CDBurnerXP.

4.2 První scénář

V prvním scénáři je zamýšleno užití přístupu zajišťování dat ze živého systému, z toho důvodu počítač před počátkem zajišťování dat nebude vypnut, a dojde tak k simulaci přístupu forenzního technika k aktivnímu počítači. Z tohoto důvodu lze na pracovní stanici na jednu stranu zajistit větší množství dat, jako jsou screenshoty plochy, výpis běžících procesů, přihlášených uživatelů, aktivní síťové konektivity a provedení dumpu operační paměti. Na druhou stranu je nemožné zajistit, aby nedošlo k nežádoucímu zápisu dat na paměťové médium zkoumaného počítače z důvodu aktivity forenzního technika na dotčené stanici.

4.3 Druhý scénář

V případě druhém bude využito přístupu zajišťování forenzních digitálních dat z neživého systému, proto bude pracovní stanice před počátkem zajišťování digitálních dat ve vypnutém stavu. Forenzní technik by se v této situaci nedostal ke všem takovým datům jako v prvním scénáři. Zanikla by možnost zajistit důležitá data, jako jsou např. výpis běžících procesů, výpis aktuálně přihlášených uživatelů, možnost zobrazit aktivní síťové toky, taktéž by nebylo možné zajistit dump operační paměti, stejně jako kterákoliv jiná data, ke kterým je nutný běh operačního systému.

4.4 Zajištění forenzních dat

Předtím, než je možné data analyzovat, musí nejprve dojít k jejich zajištění. Cílem zajištění forenzních dat je vytvoření forenzní bitové kopie média a dalších relevantních forenzních dat. Vše je provedeno tak, aby nedošlo k modifikaci obsahu a bylo ho možné zajistit kontrolními hashi. Pokud je to možné, je vhodné využít metodiky, která zabrání zápisu dat na médium, jako jsou např. write blockery.

Jednotlivé kroky zajištění jsou prioritizovány na základě míry volatilty forenzních důkazů. To v praxi znamená, že nejprve je nutné zajistit taková data, která jsou nejvíce fragilní ve smyslu náchylnosti k zásahu do integrity forenzních dat. Důvodem je minimalizace jakékoliv formy poškození či modifikace dat.

4.4.1 Proces zajištění dat ze živého systému

Prvotním krokem před samotným zajišťováním potřebných dat bylo připojení externího hard disku s nutným předinstalovaným softwarovým vybavením, které je následně použito pro sběr dat. Hard disk bude také využit jako médium, na které se veškerá zajištěná data uloží a budou tam uchována, aby byl k datům možný pozdější přístup pro účely dalšího zkoumání.

Po připojení hard disku došlo ke spuštění příkazové řádky v privilegovaném režimu, jelikož měl uživatelský účet, který byl přihlášený v rámci operačního systému zkoumané stanice, k těmto právům potřebný přístup. Pomocí použití příkazu netstat -a došlo k zachycení aktuálně navázaných síťových spojení, posléze byl virtuální počítač odpojen z internetové sítě. V další fázi došlo k vypnutí hibernace systému. Tento krok je vhodný provést, jinak by mohlo dojít k hibernaci systému, která může způsobit odhlášení uživatele nebo vypnutí pevného disku, jehož časový limit je ve výchozím nastavení explicitně nakonfigurován na 20 minut. Příkaz tasklist následně poskytuje informace o probíhajících procesech a příkaz net user vypíše na obrazovku uživatele, kteří jsou v systému přítomni. Dále došlo k použití nástroje USBDeview pro zobrazení historie připojených zařízeních prostřednictví USB.

Před samotným provedením bitové kopie je nutno zkontrolovat, zda není zapnuta funkcionalita BitLockeru a šifrování diskového pole. V poslední fázi dochází ke spuštění FTK Imager a provedení dumpu operační paměti a bitové kopie hard disku. Bitová kopie hard disku a dump paměti je taktéž pomocí FTK Imager ověřen hashi. Hashe lze využít například k pozdější kontrole nepozměnitelnosti forenzních dat.

4.4.2 Proces zajištění dat z neživého systému

V tomto případě došlo k simulaci druhého scénáře, kdy forenzní technik získá přístup k počítačové stanici, která je ve vypnutém stavu. Aby v žádném případě nedošlo ke znehodnocení důkazního materiálu, nelze počítač zapnout, a tak se zajišťují pouze data z pevného disku. Na hostovací stanici virtuálního zařízení došlo k identifikaci image pevného virtuálního disku, z něj byla vytvořena bitová forenzní kopie.

Tímto způsobem nemohlo dojít k narušení integrity dat, jelikož nebyl prokazatelně proveden zápis na zkoumaný pevný disk. V praxi by toto odpovídalo vyjmutí pevného disku z počítačové stanice a jeho připojení pomocí write blockeru k forenzní stanici, poté následnému provedení bitové forenzní kopie pevného disku vhodným způsobem.

4.5 Analýza, klasifikace a zpracování dat prvního scénáře

Tato část práce bude pojednávat o zpracování a intepretaci zajištěných dat z virtuální pracovní stanice prvního scénáře. Mimo zajištěné bitové kopie datového média došlo taktéž i k zajištění volatilních dat, jako jsou např. data obsažená v dumpu operační paměti, výpisy procesů při běhu systému, zajištěná aktivní síťová spojení a další.

Dojde ke zpracování dat formou klasifikace, intepretace a další analýzy dostupných dat ze zajištěných forenzních digitálních materiálů. Budou analyzována především taková data, která by mohla v případě reálných případů hrát důležitou roli při potenciálním šetření různého typu.

4.5.1 Data živé analýzy (aktivní síťová spojení, uživatelé, procesy, dump)

Aktivní síťová spojení

Pomocí spuštění příkazu netstat –a v příkazovém řádku dojde k výpisu aktivních síťových spojení na daném zařízení. Výpis příkazu netstat obsahuje také informace o stavu portů a to, který protokol je pro komunikaci využíván. V případě navázaného spojení dojde taktéž k vyobrazení IP adres. Netstat je vhodný nástroj k zachytávání forenzních informací o aktivních spojení v případě živé forenzní analýzy systému.

Jeho spuštění nevyžaduje administrátorská oprávnění účtu. Modifikace příkazu > E:\LiveExaminationOfUser1PC\netstat.txt pošle výstup do textového dokumentu umístěného na připojeném externím disku.
Na základě Přílohy C lze identifikovat celou řadu aktivních síťových spojení. Výpis taktéž obsahuje informace o lokální či vzdálené adrese, stavu portu a typu protokolu.

Spuštěné procesy

Příkazem tasklist > E:\LiveExaminationOfUser1PC\processes.txt lze získat výpis běžících procesů systému a další dodatečné informace o procesech jako například PID, session name a využití RAM paměti. Modifikátorem příkazu došlo k odeslání výstupu místo na konzoli CMD do textového souboru na nadefinované místo na disku E.

V Příloze D výpis vyobrazuje název spuštěných procesů, jejich identifikátor, počet instancí nebo také využití operační pamětí.

Uživatelé systému

Po použití příkazu příkazového řádku net user na zkoumané počítačové stanici E:\LiveExaminationOfUser1PC\users.txt dojde k získání informací všech uživatelských účtů, které jsou na stanici nakonfigurované. V tomto případě byl identifikován pouze jeden uživatelský účet, tudíž tato pracovní stanice neobsahuje více lokálních adresářových uživatelských struktur lokálních dat, která se zpravidla nativně vytváří automaticky pro všechny uživatele.

Výpis příkazu do CMD konzole:

Uživatelské účty pro \\DESKTOP-3T5SL6T

Administrator DefaultAccount Guest

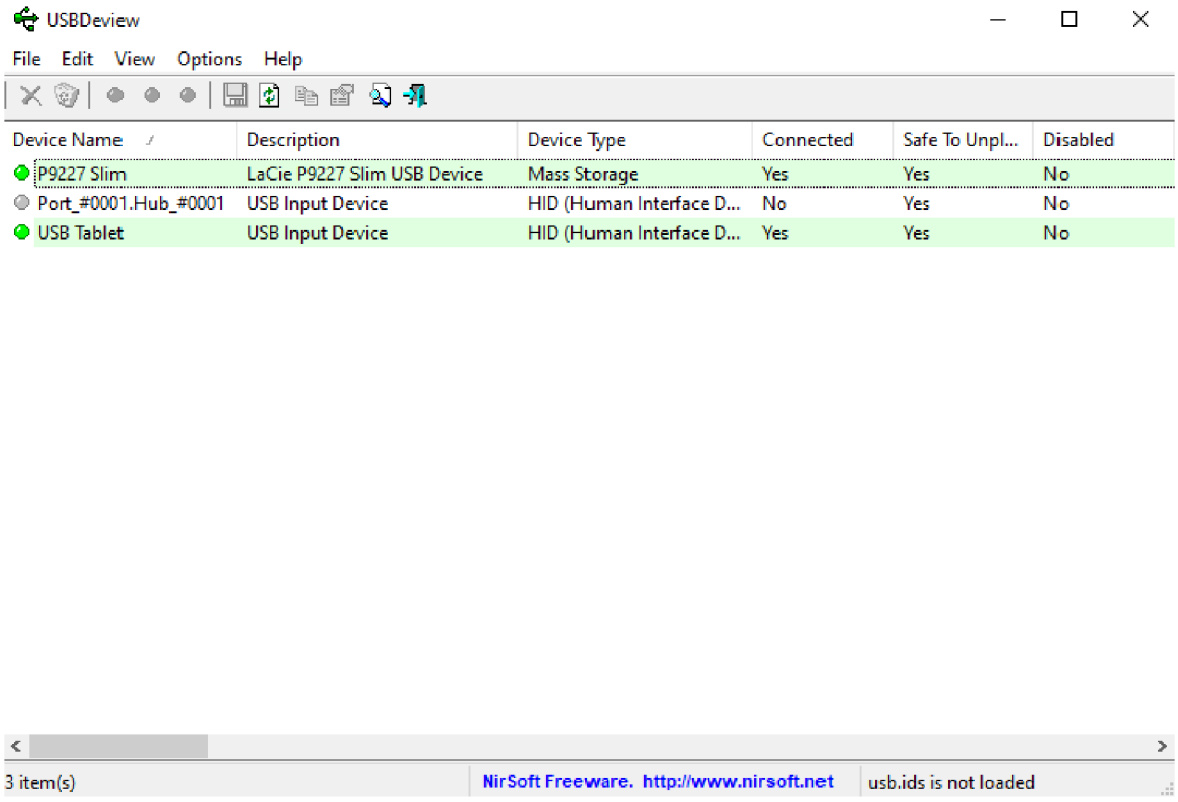
User1 WDAGUtilityAccount

Příkaz byl úspěšně dokončen.

Historie USB zařízení

Spuštěním aplikace USBDeview z externího přenosného disku byla zjištěna přítomnost tří USB zařízení. Vzhledem k tomu, že se jedná o virtualizované zařízení, zjištěné zařízení s Device Name Port_ #0001.Hub_ #0001 a USB Tablet, jsou identifikovaná rozhraní připojená myši s klávesnicí, USB Web Kamerou a Mikrofonem, zatímco Device Name P9227 Slim Lacie P92227 je externí přenosný disk, který byl využit pro spouštění a uchování forenzních aplikací a souborů. Není evidováno využití ostatních uživatelských USB zařízení.

Obrázek 12: Výpis USBDeview



Zdroj: Vlastní zpracování

Encrypce dat

Příkaz CMD manage-bde –status poskytuje uživateli s administrátorskými právy informace o nativní Microsoft Windows BitLocker šifrovací službě. Z důvodu nutnosti disponovat uživatelským účtem s administrátorskými právy může nastat případ, ve kterém není možné využít takového účtu a také spuštění samotného příkazu.

Výstup příkazu obsahuje informace o systémovém disku C a také o disku E, který byl připojen k testovací virtuální stanici z důvodu spuštění FTK Imager, a dalších aplikací, a z důvodu minimalizace narušení integrity dat v případě, že by bylo nutné instalovat forenzní nástroje přímo do zkoumané pracovní stanice. Ani jeden z nalezených disků není však touto aplikací šifrován. Nevylučuje se ale možnost, že uživatel použil k zašifrování software výrobce třetích stran.

BitLocker Drive Encryption: Configuration Tool version 10.0.19041

Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with

BitLocker Drive Encryption:

Volume E: [LaCie]

[Data Volume]

Size:	931,51 GB
BitLocker Version:	None
Conversion Status:	Fully Decrypted
Percentage Encrypted:	0,0%
Encryption Method:	None
Protection Status:	Protection Off
Lock Status:	Unlocked
Identification Field:	None
Automatic Unlock:	Disabled
Key Protectors:	None Found

Volume C: []

[OS Volume]

Size: 49,45 GB

BitLocker Version:	None
Conversion Status:	Fully Decrypted
Percentage Encrypted:	0,0%
Encryption Method:	None
Protection Status:	Protection Off
Lock Status:	Unlocked
Identification Field:	None
Key Protectors:	None Found

Volatilní paměťová data

Nejdůležitějšími daty, která lze získat z dumpu operační paměti, jsou jedinečné informace, které umožní forenznímu analytikovi nahlédnout, co se dělo při běhu operačního systému. Jedná se především o probíhající síťová spojení, procesy, načtené registry operačního systému, certifikáty systému a jiné. V mnoha případech nežádoucích útoků na počítačové systémy se může jednat o jediné informace, které jsou forenzním analytikům dostupné. Každý program, ať už se jedná o závadný program, musí být načten do operační paměti pro spuštění, tato skutečnost činí analýzu dumpu operační paměti kritickou disciplínou při objevování digitálních forenzních stop.

Nejzákladnějším příkazem Volatility frameworku je příkaz vol.py -f D:\LiveExaminationOfUser1PC\memdump.mem windows.info.Info, který vypíše na CMD konzoli informace o operačním systému. Poskytuje informace, jako jsou např. bitová verze systému, verze buildu operačního systému, systémový čas atd.

Obrázek 13: Volatility příkaz

Zdroj: Vlastní zpracování

Dalšími použitými příkazy jsou:

- netscan windows.pslist.PsList;
- windows.registry.hivelist.HiveList;
- windows.dlllist.DllList;
- netscan;
- windows.registry.certificates.Certificates.

Na základě Přílohy A této práce, ve které jsou vyobrazeny ukázky výstupů výše zmíněných Volatility framework příkazů, lze identifikovat množství a typ informací, které je možné využít v případě forenzního šetření. V případě potřeby analýzy dodatečných forenzních stop obsažených v dumpu operační paměti Volatility poskytuje framework širokou škálu dalších příkazů. (online, https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#)

4.5.2 Souborový systém (kořenový strom, user data, smazané soubory)

Pomocí forenzního analytického nástroje Autopsy došlo k načtení bitového image disku včetně ověření kontrolních hash souborů. Autopsy posléze započne automatickou analýzou obsahu image, ve kterém dojde k setřídění a indexování obsahu. Uživatelské rozhraní

softwaru Autopsy poskytuje forenzním analytikům možnosti zobrazení nalezeného obsahu, včetně dalších dodatečných funkcionalit. V rámci praktické části této práce bude brán v potaz nejdůležitější úsek dat, který v sobě často ukrývá možné forenzní digitální stopy, které by mohly být využitelné v případě reálných případů.

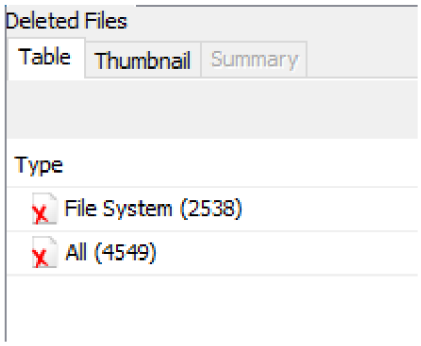
Obrázek 14: Souborový systém

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
$OrphanFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
$CarvedFiles				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
$Extend				2022-01-29 17:27:04 CET	2022-01-29 17:27:04 CET	2022-01-29 17:27:04 CET	2022-01-29 17:27:04 CET	656
$Recycle.Bin				2022-02-01 13:47:11 CET	2022-02-01 13:47:11 CET	2022-02-01 14:53:47 CET	2019-12-07 10:14:52 CET	712
$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
$WinREAgent				2022-02-01 12:05:55 CET	2022-02-01 12:05:55 CET	2022-02-01 14:53:47 CET	2022-02-01 12:05:55 CET	144
[current folder]				2022-02-01 12:05:55 CET	2022-02-01 12:05:55 CET	2022-02-06 17:20:25 CET	2019-12-07 10:03:44 CET	56
Documents and Settings				2022-01-29 17:31:25 CET	2022-01-29 17:31:25 CET	2022-01-29 17:31:25 CET	2022-01-29 17:31:25 CET	48
Instalace				2022-02-01 11:59:59 CET	2022-02-01 11:59:59 CET	2022-02-01 14:53:47 CET	2022-02-01 11:50:57 CET	56
PerfLogs				2019-12-07 10:14:52 CET	2022-01-29 17:29:23 CET	2022-02-04 22:02:18 CET	2019-12-07 10:14:52 CET	48
Pomocny adresar				2022-02-01 11:50:52 CET	2022-02-01 11:50:52 CET	2022-02-01 14:53:47 CET	2022-02-01 11:50:52 CET	48
Program Files				2022-02-01 12:11:59 CET	2022-02-01 12:11:59 CET	2022-02-06 17:20:25 CET	2019-12-07 10:14:52 CET	168
Program Files (x86)				2022-02-01 12:12:01 CET	2022-02-01 12:12:01 CET	2022-02-06 17:13:57 CET	2019-12-07 10:14:52 CET	56
ProgramData				2022-02-01 12:12:01 CET	2022-02-01 12:12:01 CET	2022-02-06 17:16:24 CET	2019-12-07 10:14:52 CET	56
Recovery				2022-02-01 11:59:24 CET	2022-02-01 11:59:24 CET	2022-02-01 14:53:45 CET	2022-01-29 17:31:29 CET	256
System Volume Information				2022-01-29 17:31:32 CET	2022-01-29 17:31:32 CET	2022-02-06 17:20:26 CET	2022-01-29 17:29:51 CET	56
Users				2022-01-29 17:51:29 CET	2022-01-29 17:51:29 CET	2022-02-06 17:20:24 CET	2019-12-07 10:03:44 CET	56
Windows				2022-02-06 16:59:38 CET	2022-02-06 16:59:38 CET	2022-02-06 17:20:25 CET	2019-12-07 10:03:44 CET	352

Zdroj: Vlastní zpracování

Data souborového systému jsou podstatná data, která musí být analyzována. V případě, že se forenznímu nástroji nepodaří file systém ze zkoumaného datového image zpracovat, může být patřičný file systém opatřen heslem, nebo poškozen. Na obrázku níže je zobrazen výpis kořenové datové struktury disku C, která zobrazuje mimo jiné také systémové skryté složky a smazané soubory. Mezi složkami a soubory lze libovolně procházet, číst dodatečná informace o souborech, popřípadě je možné zvolené soubory exportovat na místní úložiště pro další účely. Důležitými informacemi mohou být poslední datum změny, přístupu či vytvoření souboru nebo složky.

Obrázek 15: Smazané soubory



Zdroj: Vlastní zpracování

Bylo identifikováno celkové množství smazaných souborů ve výši 4 549. Mezi tyto soubory se neřadí pouze uživatelská data, ale i data, která jsou součástí běhu systému, aplikací, registrů atd. Mezi těmito daty nelze rychlým způsobem z důvodu značné rozmanitosti a četnosti smazaných dat identifikovat data uživatelská. Lze využít vyhledávání v Autopsy uživatelském rozhraní, kde lze specifikovat část názvu souboru, koncovka souboru případně hash.

Obrázek 16: Obsah koše

Recycle Bin

Table | Thumbnail | Summary

Source Name	S	C	O	Path	Time Deleted	Username	Data Source
$RERLJ0N.exe				C:\Users\User1\Downloads\vlc-3.0.16-win64.exe	2022-02-01 11:51:10 CET		User1PC.001
$RGL7UJ4.exe				C:\Users\User1\Downloads\ChromeSetup.exe	2022-02-01 11:51:10 CET		User1PC.001
$RGMLSUX.exe				C:\Users\User1\Downloads\ccsetup589.exe	2022-02-01 11:51:10 CET		User1PC.001
$RP98V1I.exe				C:\Users\User1\Downloads\tcmd1000x64.exe	2022-02-01 11:51:10 CET		User1PC.001
$RRIXZS7.exe				C:\Users\User1\Downloads\winrar-x64-610.exe	2022-02-01 11:51:10 CET		User1PC.001
$RVAQZQX.msi				C:\Users\User1\Downloads\LibreOffice_7.2.5_Win_x64.msi	2022-02-01 11:51:10 CET		User1PC.001
$RXA7OK7.exe				C:\Users\User1\Downloads\Firefox Installer.exe	2022-02-01 12:13:13 CET		User1PC.001
$RYJJXXG.exe				C:\Users\User1\Downloads\JavaSetup8u321.exe	2022-02-01 11:51:10 CET		User1PC.001

Zdroj: Vlastní zpracování

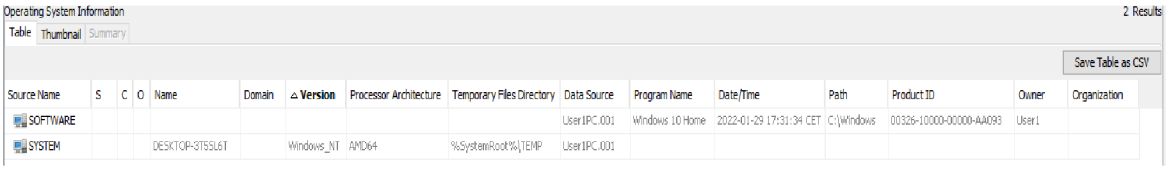
Autopsy umožňuje vyobrazení obsahu Recycle Binu, zvaného taktéž jako Koše. Do této složky se přesouvají soubory, které uživatel systému smaže pomocí klávesy Delete nebo je odstraní využitím menu pravého kliknutí. V tomto případě došlo k nálezu několika souborů s koncovkou exe či msi, jedná se tedy o instalační soubory různého typu softwaru. Ve sloupcích lze identifikovat cestu k souboru a také, kdy byl soubor smazán. V případě

potřeby lze využít zobrazení rozšířených informací o souborech nebo soubor exportovat na vlastní datové médium.

4.5.3 Nativní podstatná systémová data (registry atd.)

Do kategorie nativních systémových dat se řadí informace o stanici, o jejím operačním systému, uživatelských účtech, registrech, systémové logy, jako jsou např. security logy, systém logy a jiné. V uživatelském rozhraní autopsy došlo k výběru takových dat, která odpovídají tomuto popisu.

Obrázek 17: Informace o systému



Zdroj: Vlastní zpracování

V záložce Operating Systém information byly nalezeny důležité informace o stanici. Identifikována byla verze operačního systému, název zařízení, architektura procesoru a uživatel stanice jako vlastník operačního systému.

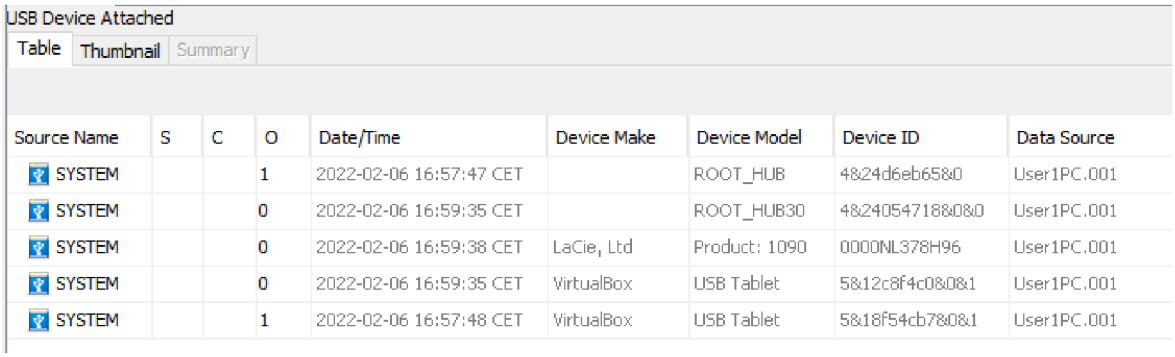
Obrázek 18: Účty

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18				systemprofile	User1PC.001_1 Host	Local		
S-1-5-80-956008885-3418522649-1831038044-185329			1		User1PC.001_1 Host	Local		
S-1-5-21-2917647296-4261490953-2943939948-1001			0	User1	User1PC.001_1 Host	Local		2022-01-29 17:34:15 CET
S-1-5-80-3028837079-3186095147-955107200-370196			1		User1PC.001_1 Host	Local		
S-1-5-19				LocalService	User1PC.001_1 Host	Local		
S-1-5-21-2917647296-4261490953-2943939948-1000			0		User1PC.001_1 Host	Local		
S-1-5-80-2620923248-4247863784-3378508180-26591			1		User1PC.001_1 Host	Local		
S-1-5-20				NetworkService	User1PC.001_1 Host	Local		
S-1-5-21-3933942852-973373972-2766786355-1032			1		User1PC.001_1 Host	Local		
S-1-5-21-2917647296-4261490953-2943939948-500			0	Administrator	User1PC.001_1 Host	Local		2022-01-29 17:31:29 CET
S-1-5-21-2917647296-4261490953-2943939948-501			0	Guest	User1PC.001_1 Host	Local		2022-01-29 17:31:29 CET
S-1-5-21-2917647296-4261490953-2943939948-504			0	WDAGUtilityAccount	User1PC.001_1 Host	Local		2022-01-29 17:31:29 CET
S-1-5-21-2917647296-4261490953-2943939948-503			0	DefaultAccount	User1PC.001_1 Host	Local		2022-01-29 17:31:29 CET

Zdroj: Vlastí zpracování

Na rozdíl od použitého příkazu net user v průběhu živé analýzy v rámci operačního systému bylo pomocí autopsy identifikováno více druhů účtů. Je nutné konstatovat, že uživatelský účet se v systému vyskytuje pouze jeden. Ostatní účty, jako jsou LocalService, NetworkService a další, jsou účty, které systém automaticky zakládá při instalaci, posléze jsou použity pro specifické účely systému.

Obrázek 19: Historie USB zařízení

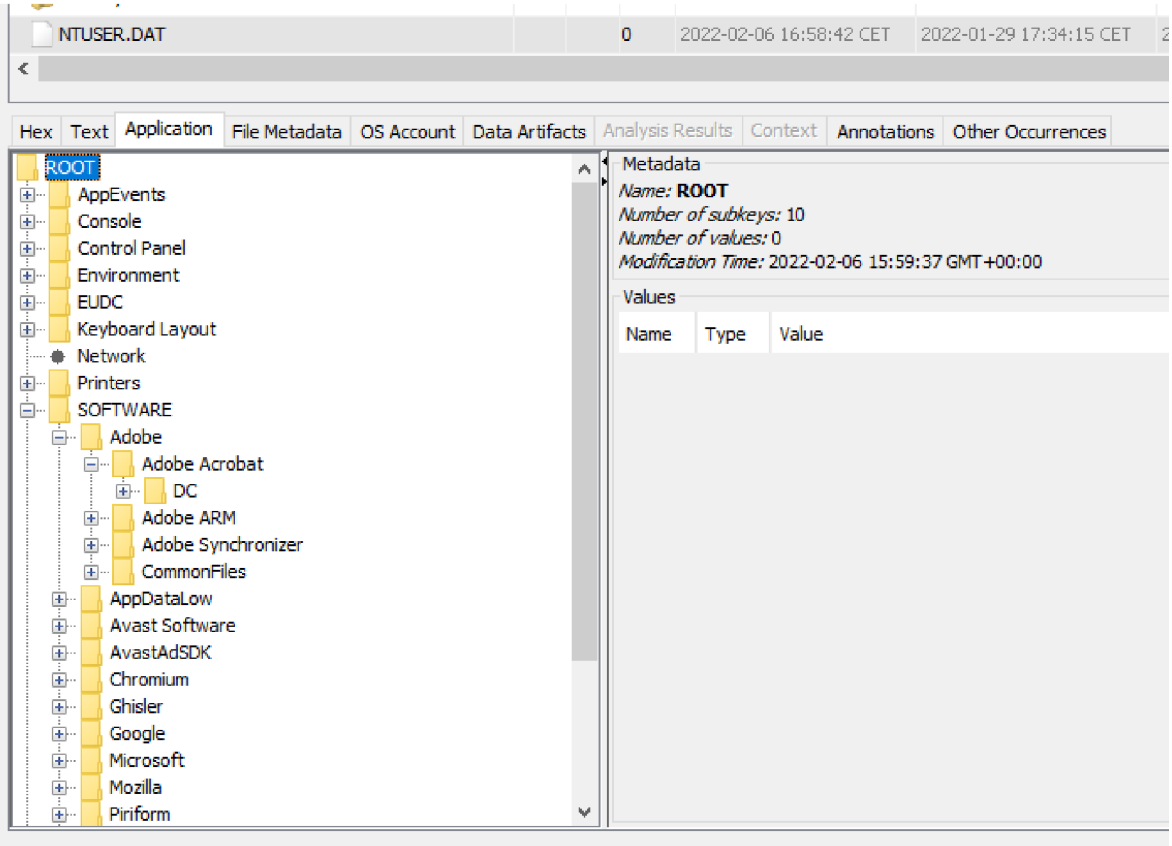


Zdroj: Vlastní zpracování

V historii připojených zařízení bylo nalezeno hned několik záznamů. Ačkoliv se na první pohled zdá, že se jedná o několik rozdílných samostatných připojených zařízení přes USB, není tomu tak. Důvodem je virtualizace a existence hardwarových HUB zařízení připojených k osobnímu počítači. Dojde-li k vyloučení těchto případů, zůstane evidované pouze jedno zařízení LaCie, které bylo připojeno a použito pro účely sběru forenzních dat. Uživatel tedy vlastní USB zařízení k virtuální zkoumané stanici v průběhu testování nepřipojil.

Registry operačního systému lze v softwaru Autopsy zobrazit pomocí vestavěného rozhraní. Je nutné lokalizovat soubor NTUSER.DAT, ve kterém jsou zpravidla ukládány uživatelské hodnoty registrů, které jsou načítány operačním systémem Windows při přihlášení uživatele. Jak lze vidět na obrázku níže, byla identifikována celá řada registrů, které upravují systémové i ostatní aplikace. Z instalovaného software lze načíst data např. pro program Adobe Acrobat, Avast, Mozillu a další.

Obrázek 20: Obsah NTUSER.DAT

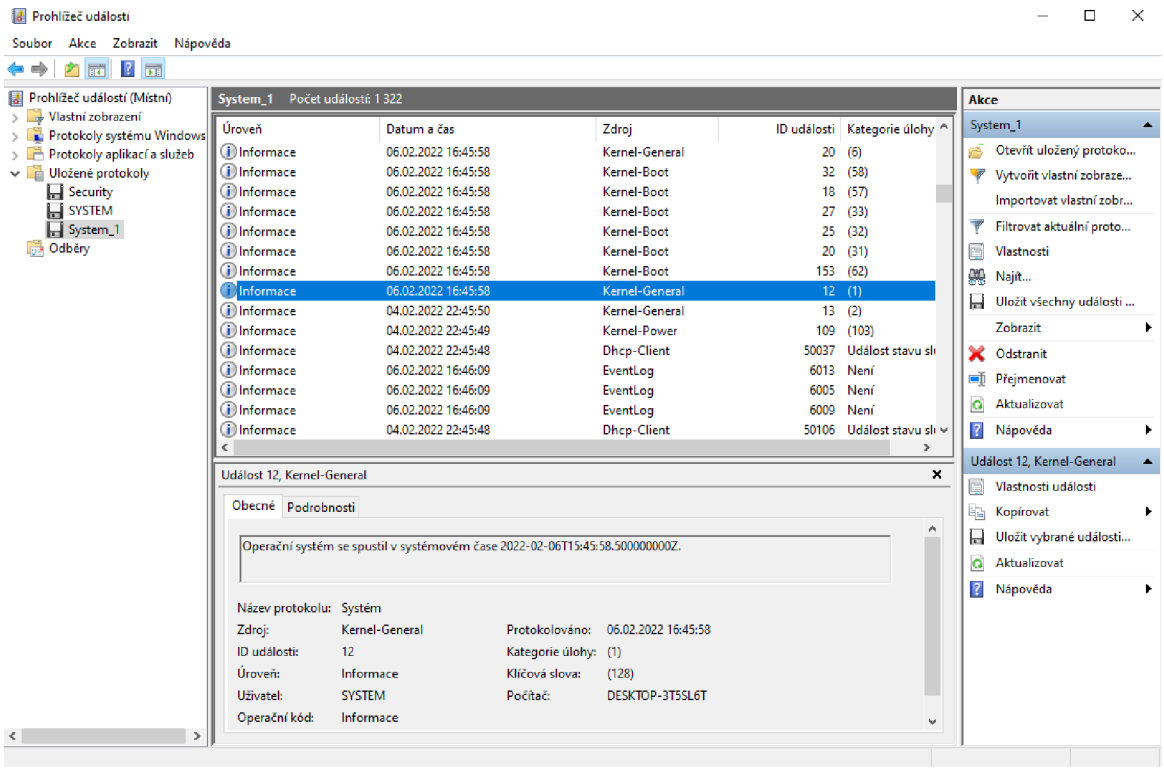


Zdroj: Vlastní zpracování

Podstatným zdrojem systémových informací jsou také logy události operačního systému. Tyto logy se nachází v adresáři /Windows/System32/winevt/Logs. Mezi stěžejní logy se řadí:

- Application log: Aplikační log zachytává události týkající se systémových komponent, jako jsou ovladače a build-in elementy interfacu;
- System log: Systémový log obsahuje logy týkající se instalovaných aplikací v systému;
- Security log: Tento log se týká bezpečnostních událostí systému, jako jsou například pokusy o přihlášení a přístup ke zdrojům. (online, https://www.howtogeek.com/123646/htg-explains-what-the-windows-event-viewer-is-and-how-you-can-use-it/)

Obrázek 21: Systém event log



Zdroj: Vlastní zpracování

4.5.4 Aplikace (instalovaný software)

Na základě získaných informací ohledně seznamu instalovaného softwaru lze posléze tyto informace využít pro nalezení předpokládaných asociovaných souborů využívaných právě uživatelským softwarem. Např. Pokud se na počítačové stanici nachází nainstalovaný software Microsoft Word, lze analogicky provést vyhledání všech podporovaných spustitelných souborů touto aplikací pomocí explicitně stanovených koncovek souborů.

Obrázek 22: Instalované programy

Installed Programs

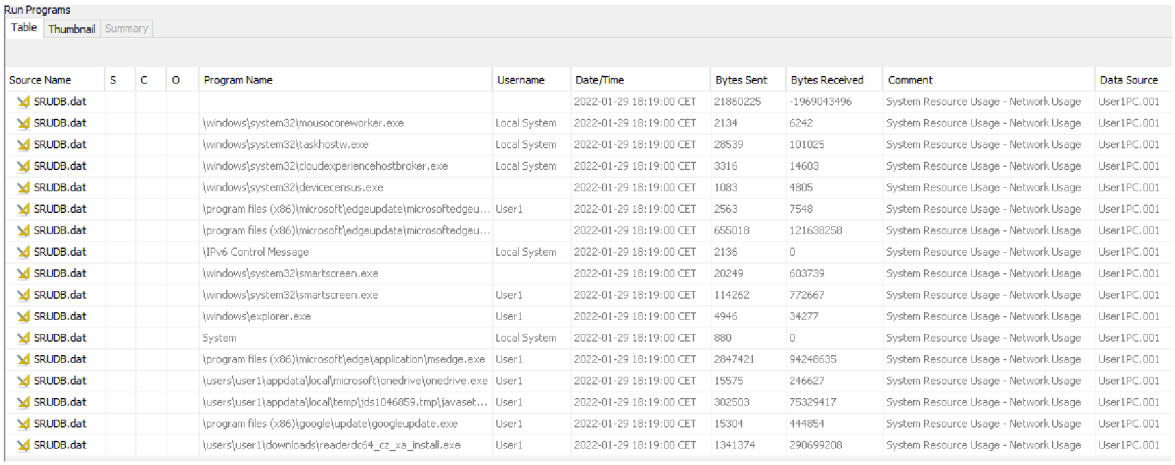
Table | Thumbnail | Summary

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	Mozilla Maintenance Service v.96.0.3	2022-02-01 11:12:02 CET	User1PC.001
SOFTWARE			0	Mozilla Firefox (x64 cs) v.96.0.3	2022-02-01 11:12:01 CET	User1PC.001
SOFTWARE			0	Avast Free Antivirus v.21.11.2500	2022-02-01 10:59:24 CET	User1PC.001
SOFTWARE			1	Microsoft Update Health Tools v.2.93.0.0	2022-01-29 17:00:17 CET	User1PC.001
SOFTWARE			1	CCleaner v.5.89	2022-01-29 16:59:19 CET	User1PC.001
SOFTWARE			1	Adobe Acrobat DC (64-bit) v.21.011.20039	2022-01-29 16:59:08 CET	User1PC.001
SOFTWARE			1	LibreOffice 7.2.5.2 v.7.2.5.2	2022-01-29 16:56:34 CET	User1PC.001
SOFTWARE			1	WinRAR 6.10 (64-bit) v.6.10.0	2022-01-29 16:54:32 CET	User1PC.001
SOFTWARE			1	Total Commander 64-bit (Remove or Repair) v.10.00	2022-01-29 16:54:23 CET	User1PC.001
SOFTWARE			1	VLC media player v.3.0.16	2022-01-29 16:49:45 CET	User1PC.001
SOFTWARE			1	DXM_Runtime	2019-12-07 14:44:20 CET	User1PC.001
SOFTWARE			1	MPlayer2	2019-12-07 14:44:20 CET	User1PC.001
SOFTWARE			1	AddressBook	2019-12-07 09:17:28 CET	User1PC.001
SOFTWARE			1	Connection Manager	2019-12-07 09:17:28 CET	User1PC.001
SOFTWARE			1	DirectDrawEx	2019-12-07 09:17:28 CET	User1PC.001
SOFTWARE			1	Fontcore	2019-12-07 09:17:28 CET	User1PC.001
SOFTWARE			1	IE40	2019-12-07 09:17:28 CET	User1PC.001

Zdroj: Vlastní zpracování

Na obrázku níže byla identifikována historie spuštěných aplikací. Tento seznam taktéž obsahuje dodatečné informace jako cestu ke spuštěnému souboru, který uživatel aplikaci spustil, případně zda aplikace nebyla vyvolána v běh samotným operačním systémem. Dalším poskytovaným identifikátorem je čas spuštění aplikace, počet přijatých a odeslaných bitů aplikací a dále.

Obrázek 23: Spuštěné programy



Run Programs

Table | Thumbnail | Summary

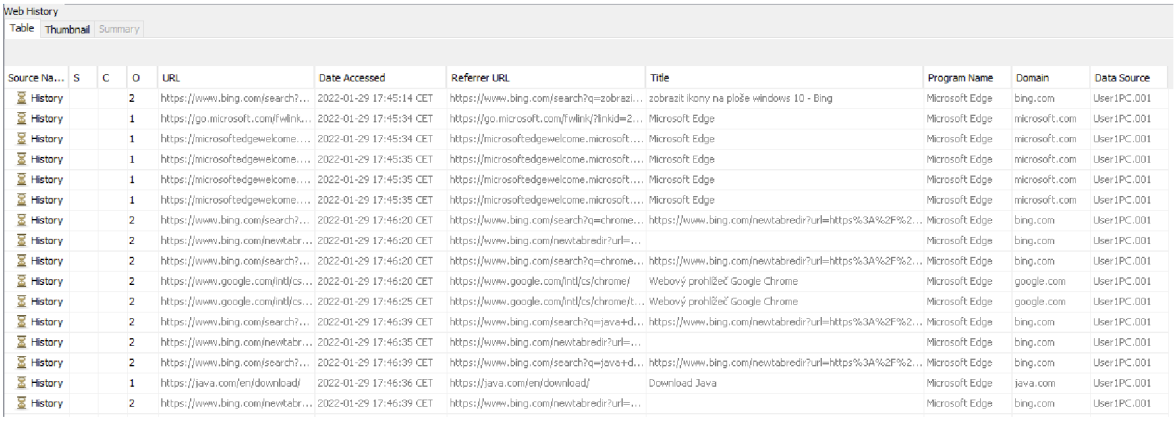
Source Name	S	C	O	Program Name	Username	Date/Time	Bytes Sent	Bytes Received	Comment	Data Source
SRUDB.dat						2022-01-29 18:19:00 CET	21860225	-1969043496	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\windows\system32\mousocoreworker.exe	Local System	2022-01-29 18:19:00 CET	2134	6242	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\windows\system32\taskhostw.exe	Local System	2022-01-29 18:19:00 CET	28539	101025	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\windows\system32\cloudexperiencehostbroker.exe	Local System	2022-01-29 18:19:00 CET	3316	14603	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\windows\system32\devicecensus.exe		2022-01-29 18:19:00 CET	1083	4805	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\program files (x86)\microsoft\edgeupdate\microsoftedgeu...	User1	2022-01-29 18:19:00 CET	2563	7548	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\program files (x86)\microsoft\edgeupdate\microsoftedgeu...		2022-01-29 18:19:00 CET	655018	121638258	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\IPv6 Control Message	Local System	2022-01-29 18:19:00 CET	2136	0	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\windows\system32\smartscreen.exe		2022-01-29 18:19:00 CET	20249	603739	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\windows\system32\smartscreen.exe	User1	2022-01-29 18:19:00 CET	114262	772667	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\windows\explorer.exe	User1	2022-01-29 18:19:00 CET	4946	34277	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				System	Local System	2022-01-29 18:19:00 CET	880	0	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\program files (x86)\microsoft\edge\application\msedge.exe	User1	2022-01-29 18:19:00 CET	2847421	94248635	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\users\user1\appdata\local\microsoft\onedrive\onedrive.exe	User1	2022-01-29 18:19:00 CET	15575	246627	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\users\user1\appdata\local\temp\{jds1046859.tmp\javaset...	User1	2022-01-29 18:19:00 CET	302503	75329417	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\program files (x86)\google\update\googleupdate.exe	User1	2022-01-29 18:19:00 CET	15304	444854	System Resource Usage - Network Usage	User1PC.001
SRUDB.dat				\users\user1\downloads\readerdc64_cz_xa_install.exe	User1	2022-01-29 18:19:00 CET	1341374	290699208	System Resource Usage - Network Usage	User1PC.001

Zdroj: Vlastní zpracování

4.5.5 Data webového prohlížeče

Webové prohlížeče jsou velice často používanou aplikací. Jsou využívány pro mnoho účelů jako např. vyhledávání informací, e-mail, e-commerce, novinky, bankovnictví, sociální sítě a další. Z tohoto důvodu se jedná o velice podstatnou část dat pro digitální forenzní analýzu. Webové prohlížeče uchovávají některá data v různých místech v rámci operačního systému. Tato data byla pomocí Autopsy identifikována. Mezi nalezené záznamy se řadí historie webového prohlížeče, záložky webového prohlížeče, login data, cookies a cache.

Obrázek 24: Historie webového prohlížeče



Web History

Table | Thumbnail | Summary

Source Na...	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name	Domain	Data Source
History			2	https://www.bing.com/search?...	2022-01-29 17:45:14 CET	https://www.bing.com/search?q=zobrazi...	zobrazit ikony na ploše windows 10 - Bing	Microsoft Edge	bing.com	User1PC.001
History			1	https://go.microsoft.com/fwlink...	2022-01-29 17:45:34 CET	https://go.microsoft.com/fwlink/?linkid=2...	Microsoft Edge	Microsoft Edge	microsoft.com	User1PC.001
History			1	https://microsoftedgewelcome....	2022-01-29 17:45:34 CET	https://microsoftedgewelcome.microsoft....	Microsoft Edge	Microsoft Edge	microsoft.com	User1PC.001
History			1	https://microsoftedgewelcome....	2022-01-29 17:45:35 CET	https://microsoftedgewelcome.microsoft....	Microsoft Edge	Microsoft Edge	microsoft.com	User1PC.001
History			1	https://microsoftedgewelcome....	2022-01-29 17:45:35 CET	https://microsoftedgewelcome.microsoft....	Microsoft Edge	Microsoft Edge	microsoft.com	User1PC.001
History			1	https://microsoftedgewelcome....	2022-01-29 17:45:35 CET	https://microsoftedgewelcome.microsoft....	Microsoft Edge	Microsoft Edge	microsoft.com	User1PC.001
History			2	https://www.bing.com/search?...	2022-01-29 17:46:20 CET	https://www.bing.com/search?q=chrome...	https://www.bing.com/newtabredir?url=https%3A%2F%2...	Microsoft Edge	bing.com	User1PC.001
History			2	https://www.bing.com/newtabr...	2022-01-29 17:46:20 CET	https://www.bing.com/newtabredir?url=...		Microsoft Edge	bing.com	User1PC.001
History			2	https://www.bing.com/search?...	2022-01-29 17:46:20 CET	https://www.bing.com/search?q=chrome...	https://www.bing.com/newtabredir?url=https%3A%2F%2...	Microsoft Edge	bing.com	User1PC.001
History			2	https://www.google.com/intl/cs...	2022-01-29 17:46:20 CET	https://www.google.com/intl/cs/chrome/	Webový prohlížeč Google Chrome	Microsoft Edge	google.com	User1PC.001
History			2	https://www.google.com/intl/cs...	2022-01-29 17:46:25 CET	https://www.google.com/intl/cs/chrome/t...	Webový prohlížeč Google Chrome	Microsoft Edge	google.com	User1PC.001
History			2	https://www.bing.com/search?...	2022-01-29 17:46:39 CET	https://www.bing.com/search?q=java+d...	https://www.bing.com/newtabredir?url=https%3A%2F%2...	Microsoft Edge	bing.com	User1PC.001
History			2	https://www.bing.com/newtabr...	2022-01-29 17:46:35 CET	https://www.bing.com/newtabredir?url=...		Microsoft Edge	bing.com	User1PC.001
History			2	https://www.bing.com/search?...	2022-01-29 17:46:39 CET	https://www.bing.com/search?q=java+d...	https://www.bing.com/newtabredir?url=https%3A%2F%2...	Microsoft Edge	bing.com	User1PC.001
History			1	https://java.com/en/download/	2022-01-29 17:46:36 CET	https://java.com/en/download/	Download Java	Microsoft Edge	java.com	User1PC.001
History			2	https://www.bing.com/newtabr...	2022-01-29 17:46:39 CET	https://www.bing.com/newtabredir?url=...		Microsoft Edge	bing.com	User1PC.001

Zdroj: Vlastní zpracování

Obrázek 25: Záložky webového prohlížeče

Web Bookmarks

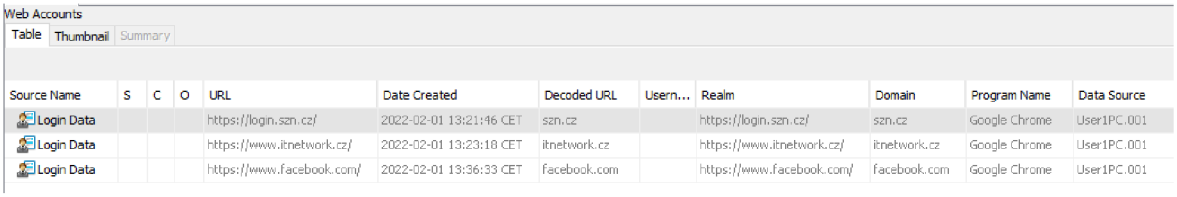
Table | Thumbnail | Summary

Save Table

Source Name	S	C	O	URL	Title	Date Created	Program Name	Domain	Data Source
Bookmarks			1	https://www.zalando.cz/urban-classics-tep...	Urban Classics Mikina na zip - charcoal/tmavÃ› Ľ˘edÃ˘ - Zal...	2022-02-01 13:43:37 CET	Google Chrome	zalando.cz	User1PC.001
Bookmarks			1	https://www.zalando.cz/panove-domovska...	PÃ˘nskÃ˘ mÃłda - obrovskÃ˘ vÃ˘bÃ›r v ZALANDO - dopra...	2022-02-01 13:43:41 CET	Google Chrome	zalando.cz	User1PC.001
Bookmarks			2	https://www.seznam.cz/	Seznam â€“ najdu tam, co neznÃ˘m	2022-02-01 13:43:48 CET	Google Chrome	seznam.cz	User1PC.001
Bookmarks			2	https://www.youtube.com/	YouTube	2022-02-01 13:43:57 CET	Google Chrome	youtube.com	User1PC.001
Bookmarks			2	https://www.google.com/	Google	2022-02-01 13:44:01 CET	Google Chrome	google.com	User1PC.001
places.sqlite			1	https://support.mozilla.org/cs/products/fir...	Získat pomoc	2022-02-01 12:12:04 CET	FireFox	mozilla.org	User1PC.001
places.sqlite			1	https://support.mozilla.org/cs/kb/customiz...	Přizpůsobení Firefoxu	2022-02-01 12:12:04 CET	FireFox	mozilla.org	User1PC.001
places.sqlite			1	https://www.mozilla.org/cs/contribute/	Zapojte se	2022-02-01 12:12:04 CET	FireFox	mozilla.org	User1PC.001
places.sqlite			1	https://www.mozilla.org/cs/about/	O nás	2022-02-01 12:12:04 CET	FireFox	mozilla.org	User1PC.001
places.sqlite			1	https://www.mozilla.org/cs/firefox/central/	Jak začít	2022-02-01 12:12:04 CET	FireFox	mozilla.org	User1PC.001

Zdroj: Vlastní zpracování

Obrázek 26: Login data



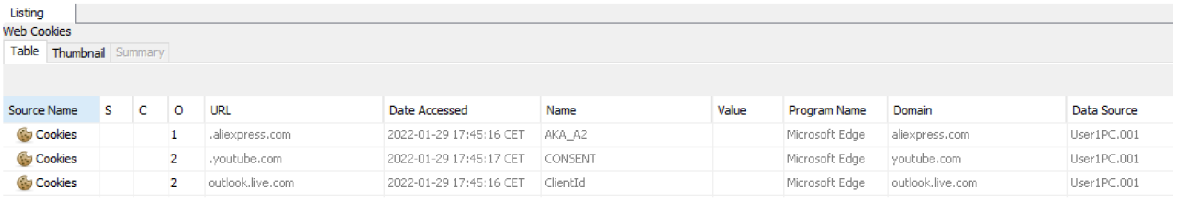
Web Accounts

Table | Thumbnail | Summary

Source Name	S	C	O	URL	Date Created	Decoded URL	Usern...	Realm	Domain	Program Name	Data Source
Login Data				https://login.szn.cz/	2022-02-01 13:21:46 CET	szn.cz		https://login.szn.cz/	szn.cz	Google Chrome	User1PC.001
Login Data				https://www.itnetwork.cz/	2022-02-01 13:23:18 CET	itnetwork.cz		https://www.itnetwork.cz/	itnetwork.cz	Google Chrome	User1PC.001
Login Data				https://www.facebook.com/	2022-02-01 13:36:33 CET	facebook.com		https://www.facebook.com/	facebook.com	Google Chrome	User1PC.001

Zdroj: Vlastní zpracování

Obrázek 27: Cookies



Listing

Web Cookies

Table | Thumbnail | Summary

Source Name	S	C	O	URL	Date Accessed	Name	Value	Program Name	Domain	Data Source
Cookies			1	.aliexpress.com	2022-01-29 17:45:16 CET	AKA_A2		Microsoft Edge	aliexpress.com	User1PC.001
Cookies			2	.youtube.com	2022-01-29 17:45:17 CET	CONSENT		Microsoft Edge	youtube.com	User1PC.001
Cookies			2	outlook.live.com	2022-01-29 17:45:16 CET	ClientId		Microsoft Edge	outlook.live.com	User1PC.001

Zdroj: Vlastní zpracování

Obrázek 28: Cache webového prohlížeče

Web Cache

Table | Thumbnail | Summary

Source Name	S	C	O	URL	Domain	Date Created	Headers
data_1			1	1/0/_dk_https://seznam.cz https://seznam.cz https://d53-...	sdn.cz	2022-02-04 21:33:16 CET	date : Fri, 04 Feb 2022 20:33:17 GMT server : nginx conte...
data_1			1	1/0/_dk_https://sauto.cz https://sauto.cz https://d19-a.s...	sdn.cz	2022-02-01 16:13:34 CET	date : Tue, 01 Feb 2022 16:09:14 GMT server : nginx cont...
data_1			1	1/0/_dk_https://alza.cz https://alza.cz https://cdn.alza.cz/...	alza.cz	2022-02-01 11:44:08 CET	date : Tue, 01 Feb 2022 10:44:09 GMT content-length : 92...

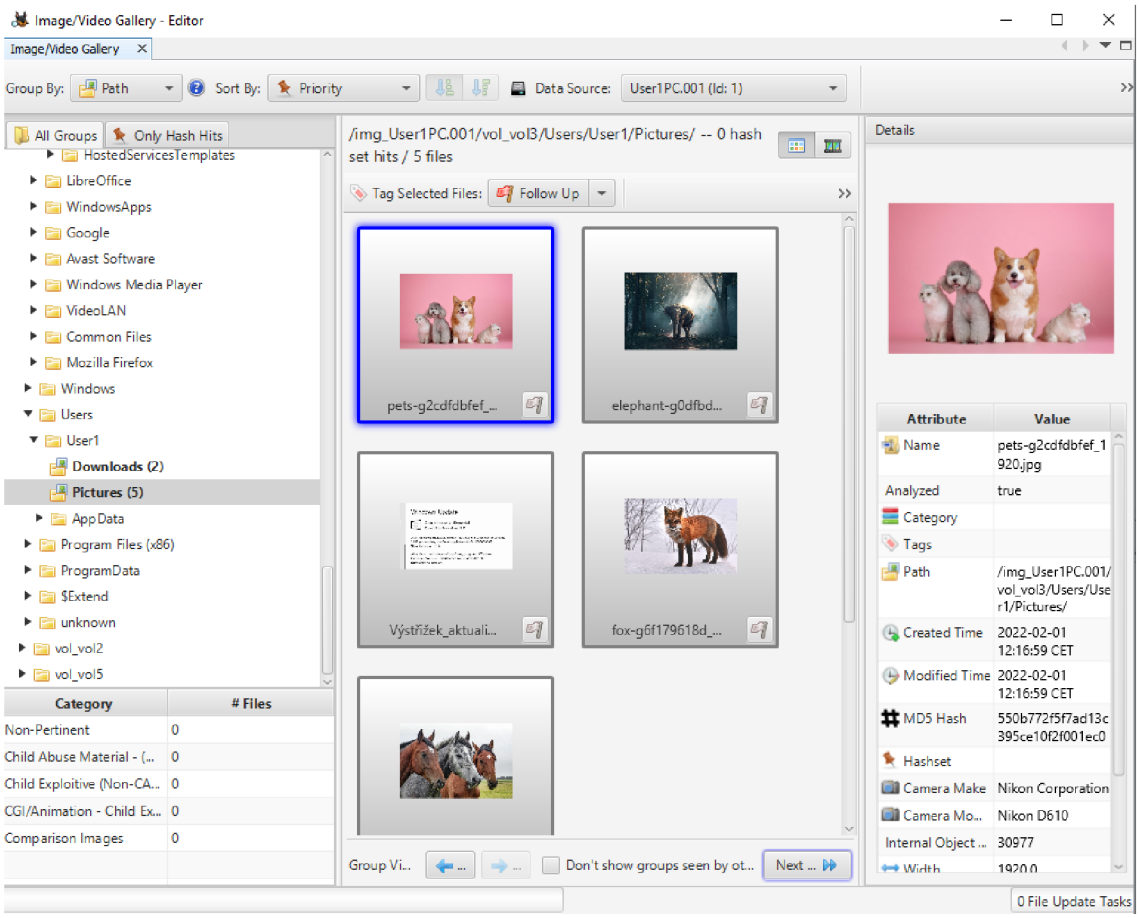
Zdroj: Vlastní zpracování

4.5.6 Obrazové soubory

Obrazové fotosoubory a videosoubory byly analyzovány prostřednictvím Autopsy vestavěné funkcionality Image/Video Gallery – Editor. Pomocí výpisu tohoto prostředí došlo k nalezení několika tisíc jednotlivých souborů. Převážná většina souborů avšak nenaznačuje nic o uživatelské činnosti, jelikož se jedná o soubory, které podléhají činnosti operačního systému. Jedná se převážně o miniatury a grafiku prostředí operačního systému Microsoft Windows a instalovaných aplikací.

Pro identifikaci uživatelských souborů je nutné využít rozšířené vyhledávání a pomocí dodatečných parametrů, jako jsou koncovky souborů, velikosti souborů a jiné, hledání specifikovat. Uživatelské fotosoubory a videosoubory se často nacházejí ve složkách uživatele, jako jsou složky Videos, Photos, Documents, Downloads a další. V tomto případě bylo identifikováno pět uživatelských JPG souborů. Autopsy poskytuje možnost čtení metadat (pravá část obrázku), kde na označeném obrázku lze např. zjistit zařízení, kterým byla fotografie pořízena.

Obrázek 29: Nalezené obrazové soubory



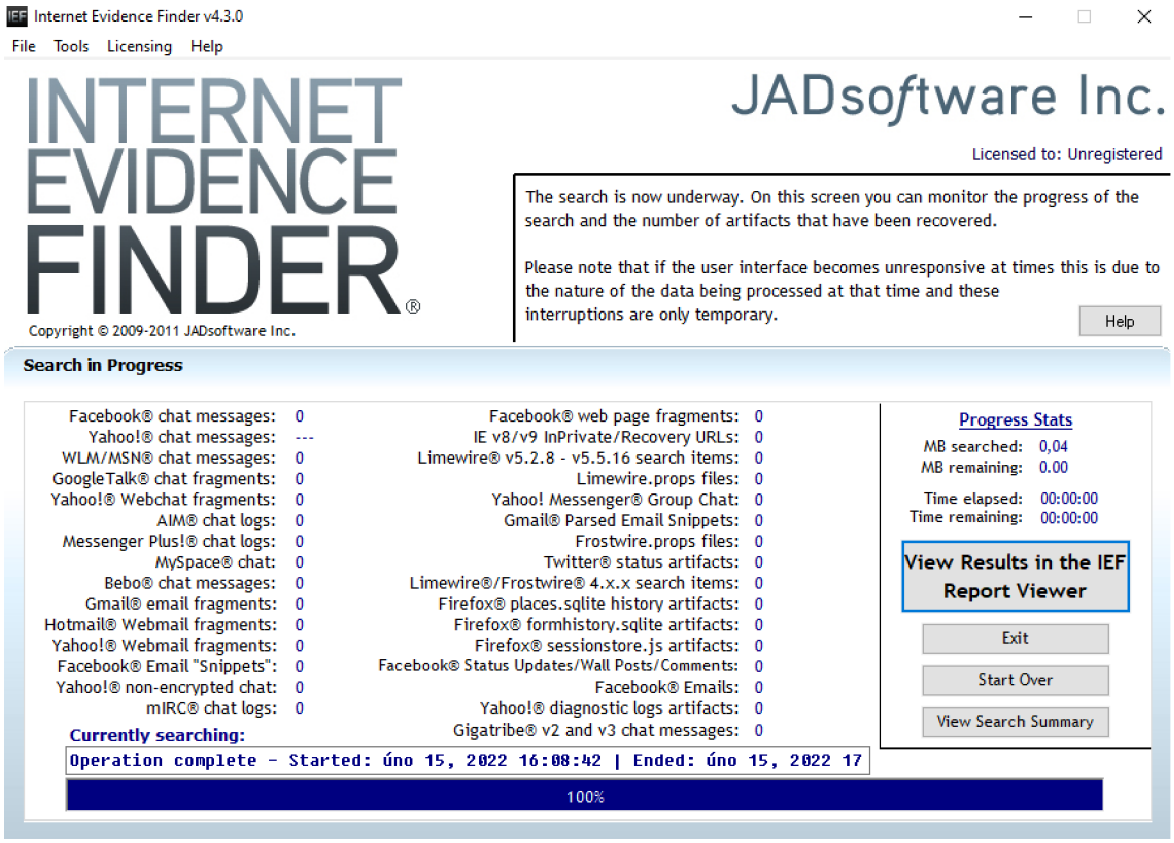
Zdroj: Vlastní zpracování

4.5.7 E-mail a messaging nástroje

Jelikož pomocí softwaru Autopsy nebyla na analyzované bitové kopii nalezena přítomnost žádných e-mailových klientů a messaging aplikací, byla pro potvrzení této skutečnosti využita zkušební verze softwaru Internet Evidence Finder od společnosti Magnet.

Přestože se jedná o trial verzi, pro účely této práce je tato verze dostačující. Pomocí nástroje IEF došlo k prozkoumání forenzních bitových kopií, včetně dumpu operační paměti. IEF taktéž neidentifikoval žádný z běžně dostupných messaging nástrojů. Došlo k potvrzení, že uživatel aplikace tohoto typu nevyužíval.

Obrázek 30: Internet evidence finder výsledek hledání



Zdroj: Vlastní zpracování

4.6 Analýza, klasifikace a zpracování dat druhého scénáře

Tento scénář byl nadefinován, aby co nejpřesněji napodobil situaci, kdy forenzní technik, který provádí akvizici dat, dostane přístup k počítačové stanici výhradně ve vypnutém stavu. Důvodem bylo potenciální narušení integrity dat a také samozřejmě možnost poškození forenzních důkazů, proto nebylo možné počítačovou stanici zapnout. Zaniká možnost provedení zajištění forenzních volatilních dat, které je možné docílit využitím patřičných forenzních nástrojů a technik např. takový způsobem, jak je uvedeno v popisu prvního případu scénáře v první polovině vlastní práce tohoto textu.

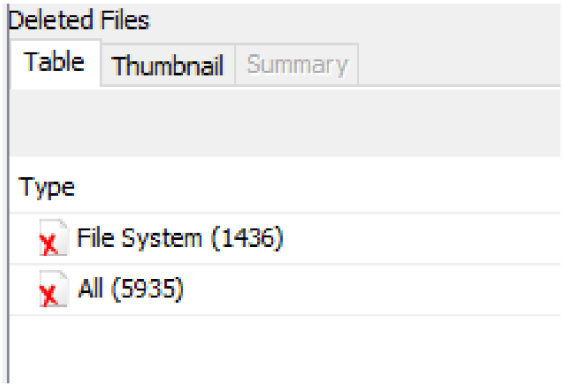
V praktickém případě by došlo k vyjmutí datového média z PC a posléze za použití write-blockeru nebo jiných technik, které znemožňují zápis dat na zkoumané médium, poté k provedení bitové forenzní kopie. Pro napodobení takového chování v testovacím virtuálním prostředí došlo k lokalizaci logického disku zkoumané stanice v rámci

hostovacího PC a použitím FTK imager k vytvoření bitové kopie. Virtuální stanice byla po celou dobu akvizice dat ve vypnutém stavu.

4.6.1 Souborový systém (kořenový strom, user data, smazané soubory)

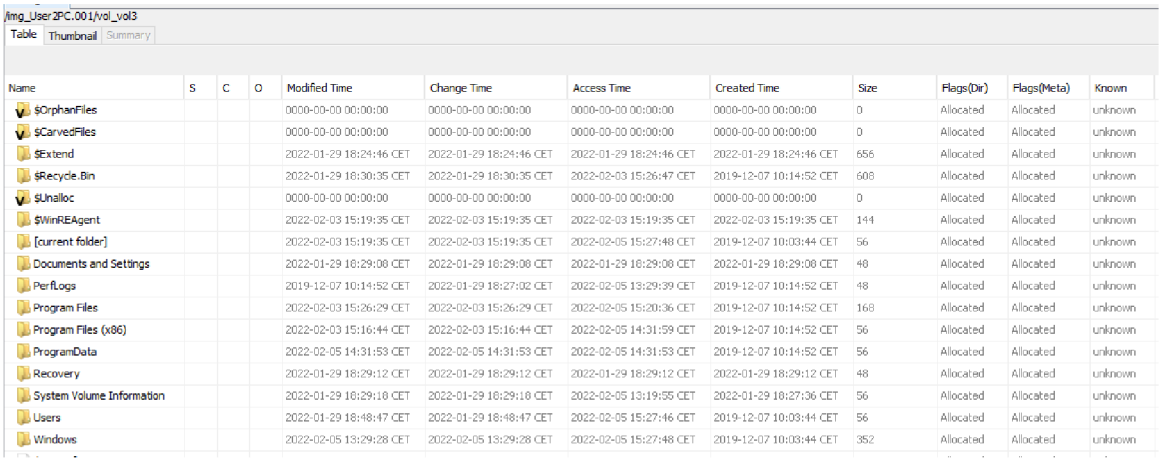
Ve druhém scénáři došlo opět k úspěšnému vyobrazení datové stromové struktury file systému zkoumané stanice. Bylo identifikováno značné množství smazaných souborů, ačkoliv uživatelský Recycle Bin neobsahoval žádné smazané soubory. Po detailnějším prohledání file systému bylo konstatováno, že se jedná o převážně systémová data, která byla mazána samotnou funkcí operačního systému.

Obrázek 31: Smazané soubory



Zdroj: Vlastní zpracování

Obrázek 32: Souborový systém



Zdroj: Vlastní zpracování

4.6.2 Nativní podstatná systémová data (registry, atd)

V oblasti podstatných systémových dat byly identifikovány informace o operačním systému, o uživatelských účtech, o historii připojených USB zařízení, klíčů hodnot registrů a systémové události. V tomto případě nebylo identifikované žádné jiné USB zařízení v minulosti připojené k systému. Ukázky vytěžených dat lze spatřit na několika obrázcích umístěných níže.

Obrázek 33: Účty

Operating System Information — 2 Results

Table | Thumbnail | Summary

Save Table as CSV

Source Name	S	C	O	Name	Domain	Version	Processo...	Temporary Files Direct...	Data Source	Program Name	Date/Time	Path	Product ID	Owner	Organization
SOFTWARE									User2PC.001	Windows 10 Home	2022-01-29 18:29:18 CET	C:\Windows	00326-10000-00000-AA553	User2	
SYSTEM				DESKTOP-ID4RM78		Windows_NT	AMD64	%SystemRoot%\TEMP	User2PC.001						

Zdroj: Vlastí zpracování

Obrázek 34: Informace o systému

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18				systemprofile	User2PC....	Local		
S-1-5-80-956008885-3418522649-1831038044-185329			1		User2PC....	Local		
S-1-5-21-2212228383-1645422737-1310266034-1001			0	User2	User2PC....	Local		2022-01-29 18:30:03 CET
S-1-5-80-3028837079-3186095147-955107200-370196			1		User2PC....	Local		
S-1-5-19				LocalService	User2PC....	Local		
S-1-5-21-2212228383-1645422737-1310266034-1000			0		User2PC....	Local		
S-1-5-80-2620923248-4247863784-3378508180-26591			1		User2PC....	Local		
S-1-5-20				NetworkService	User2PC....	Local		
S-1-5-21-3933942852-973373972-2766786355-1032			1		User2PC....	Local		
S-1-5-21-2212228383-1645422737-1310266034-503			0	DefaultAccount	User2PC....	Local		2022-01-29 18:29:13 CET
S-1-5-21-2212228383-1645422737-1310266034-504			0	WDAGUtilityAccount	User2PC....	Local		2022-01-29 18:29:13 CET
S-1-5-21-2212228383-1645422737-1310266034-500			0	Administrator	User2PC....	Local		2022-01-29 18:29:13 CET
S-1-5-21-2212228383-1645422737-1310266034-501			0	Guest	User2PC....	Local		2022-01-29 18:29:13 CET

Zdroj: Vlastní zpracování

Obrázek 35: Historie USB zařízení

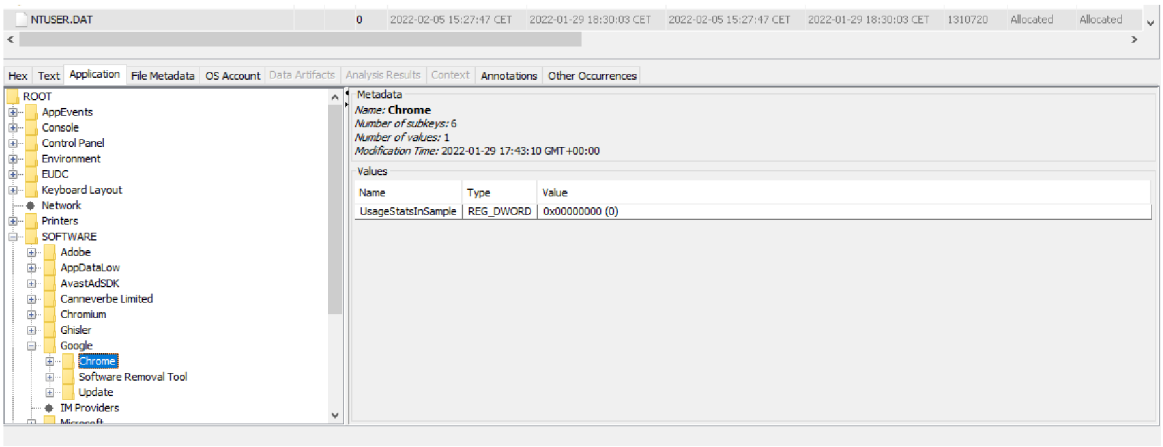
USB Device Attached

Table | Thumbnail | Summary

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM			1	2022-02-05 12:59:02 CET		ROOT_HUB	4&24d6eb65&0	User2PC.001
SYSTEM			1	2022-02-05 12:59:02 CET	VirtualBox	USB Tablet	5&18f54cb7&0&1	User2PC.001

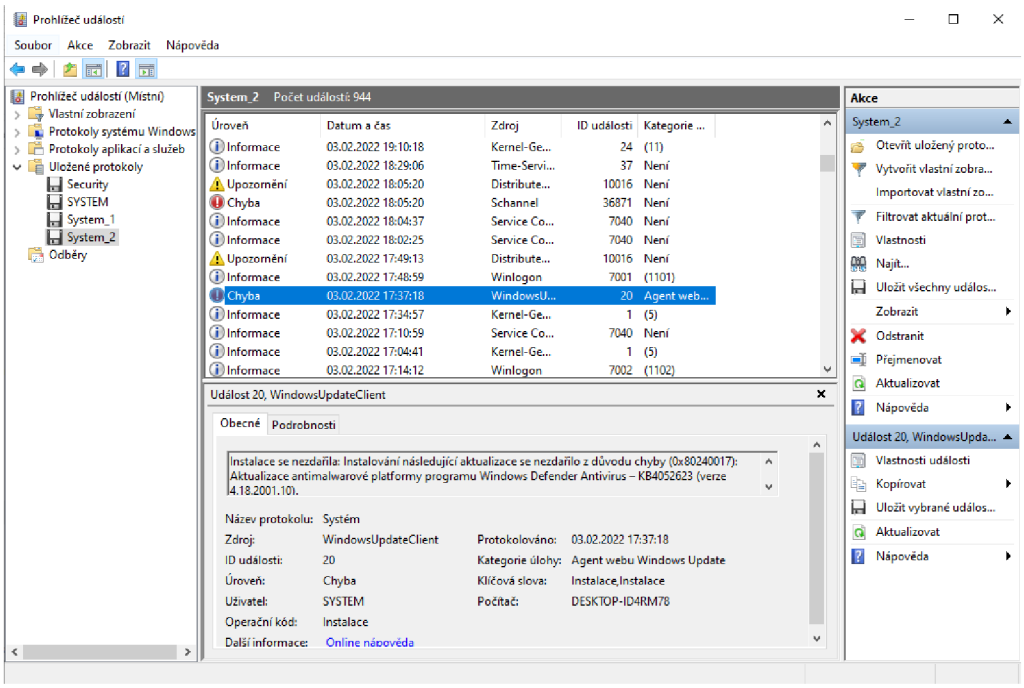
Zdroj: Vlastní zpracování

Obrázek 36: Obsah NTUSER.DAT



Zdroj: Vlastní zpracování

Obrázek 37: Systém event log



Zdroj: Vlastní zpracování

4.6.3 Aplikace (instalovaný software)

I v tomto případě byl úspěšně identifikován repositář instalovaného softwaru na počítačové stanici. Autopsy bere v potaz i aplikace, které jsou vestavěnou součástí operačního

systému. Druhý obrázek představuje opět ukázku výpisu historie spuštěných aplikací, včetně dalších informací.

Obrázek 38: Instalované programy

Installed Programs

Table | Thumbnail | Summary

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	IrfanView 4.59 (64-bit) v.4.59	2022-02-03 14:26:29 CET	User2PC.001
SOFTWARE			1	Adobe Acrobat DC (64-bit) v.21.011.20039	2022-02-03 14:18:36 CET	User2PC.001
SOFTWARE			1	Microsoft Update Health Tools v.2.93.0.0	2022-01-29 17:48:29 CET	User2PC.001
SOFTWARE			1	CCleaner v.5.89	2022-01-29 17:45:50 CET	User2PC.001
SOFTWARE			1	WinRAR 6.10 (64-bit) v.6.10.0	2022-01-29 17:44:10 CET	User2PC.001
SOFTWARE			1	Total Commander 64-bit (Remove or Repair) v.10.00	2022-01-29 17:43:59 CET	User2PC.001
SOFTWARE			1	LibreOffice 7.2.5.2 v.7.2.5.2	2022-01-29 17:42:32 CET	User2PC.001
SOFTWARE			1	VLC media player v.3.0.16	2022-01-29 17:38:24 CET	User2PC.001
SOFTWARE			0	Java 8 Update 321 (64-bit) v.8.0.3210.7	2022-01-29 17:36:05 CET	User2PC.001
SOFTWARE			1	DXM_Runtime	2019-12-07 14:44:20 CET	User2PC.001
SOFTWARE			1	MPlayer2	2019-12-07 14:44:20 CET	User2PC.001
SOFTWARE			1	AddressBook	2019-12-07 09:17:28 CET	User2PC.001
SOFTWARE			1	Connection Manager	2019-12-07 09:17:28 CET	User2PC.001
SOFTWARE			1	DirectDrawEx	2019-12-07 09:17:28 CET	User2PC.001
SOFTWARE			1	Fontcore	2019-12-07 09:17:28 CET	User2PC.001
SOFTWARE			1	IE40	2019-12-07 09:17:28 CET	User2PC.001
SOFTWARE			1	IE4Data	2019-12-07 09:17:28 CET	User2PC.001

Zdroj: Vlastní zpracování

Obrázek 39: Spuštěné programy

Run Programs

Table | Thumbnail | Summary

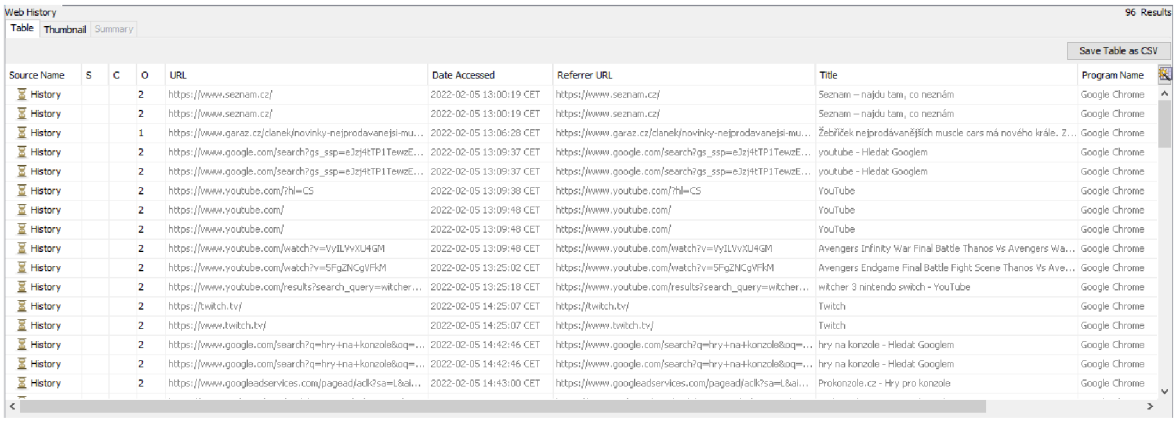
Source Name	S	C	O	Program Name	Username	Date/Time	Bytes Sent	Bytes Received	Comment	Data Source
SRUDB.dat						2022-01-29 19:07:00 CET	18258453	-2135416193	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\program files (x86)\microsoft\edge\application\msedge.exe	User2	2022-01-29 19:07:00 CET	4032994	528781252	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\windows\system32\mousocoreworker.exe	Local System	2022-01-29 19:07:00 CET	2186	6242	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\windows\system32\taskhostw.exe	Local System	2022-01-29 19:07:00 CET	30381	109287	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\windows\explorer.exe	User2	2022-01-29 19:07:00 CET	3585	27656	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				System	Local System	2022-01-29 19:07:00 CET	402	0	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\IPv6 Control Message	Local System	2022-01-29 19:07:00 CET	1526	0	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\program files (x86)\microsoft\edgeupdate\microsoftedgeu...	User2	2022-01-29 19:07:00 CET	13756	46278	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\windows\system32\smartscreen.exe	User2	2022-01-29 19:07:00 CET	97950	733993	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\users\user2\appdata\local\temp\jds417718.tmp\jre-8u32...	User2	2022-01-29 19:07:00 CET	6199	26489	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\program files\google\chrome\application\chrome.exe	User2	2022-01-29 19:07:00 CET	914513	53736273	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\program files (x86)\google\update\googleupdate.exe	User2	2022-01-29 19:07:00 CET	16599	444674	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\users\user2\appdata\local\microsoft\onedrive\onedrive.exe	User2	2022-01-29 19:07:00 CET	16652	257204	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\users\user2\appdata\local\microsoft\onedrive\update\one...	User2	2022-01-29 19:07:00 CET	1311	7685	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\users\user2\downloads\readerdc64_cz_ha_install.exe	User2	2022-01-29 19:07:00 CET	1453327	290036046	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\windows\system32\werfault.exe	User2	2022-01-29 19:07:00 CET	7045	6239	System Resource Usage - Network Usage	User2PC.001
SRUDB.dat				\program files\ccleaner\ccleaner64.exe	User2	2022-01-29 19:07:00 CET	45516	146555	System Resource Usage - Network Usage	User2PC.001

Zdroj: Vlastní zpracování

4.6.4 Data webového prohlížeče

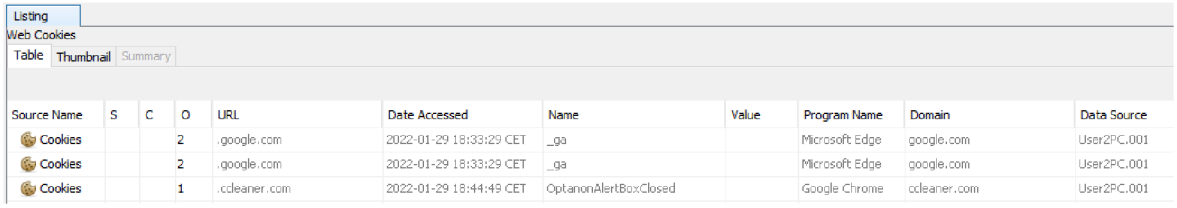
V rámci analýzy dat webového prohlížeče byla identifikována základní data, jako jsou historie aktivity prohlížení, cookies soubory a web cache. V případě potřeby forenzního analytika by bylo možné data extrahovat a podrobit dalšímu zkoumání. Na rozdíl od prvního scénáře nebyla v tomto případě identifikována uživatelská data záložek webového prohlížeče a žádná login data.

Obrázek 40: Historie webového prohlížeče



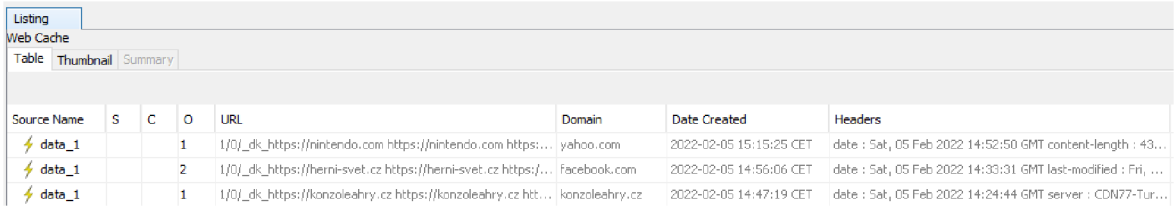
Zdroj: Vlastní zpracování

Obrázek 41: Cookies



Zdroj: Vlastní zpracování

Obrázek 42: Cache webového prohlížeče

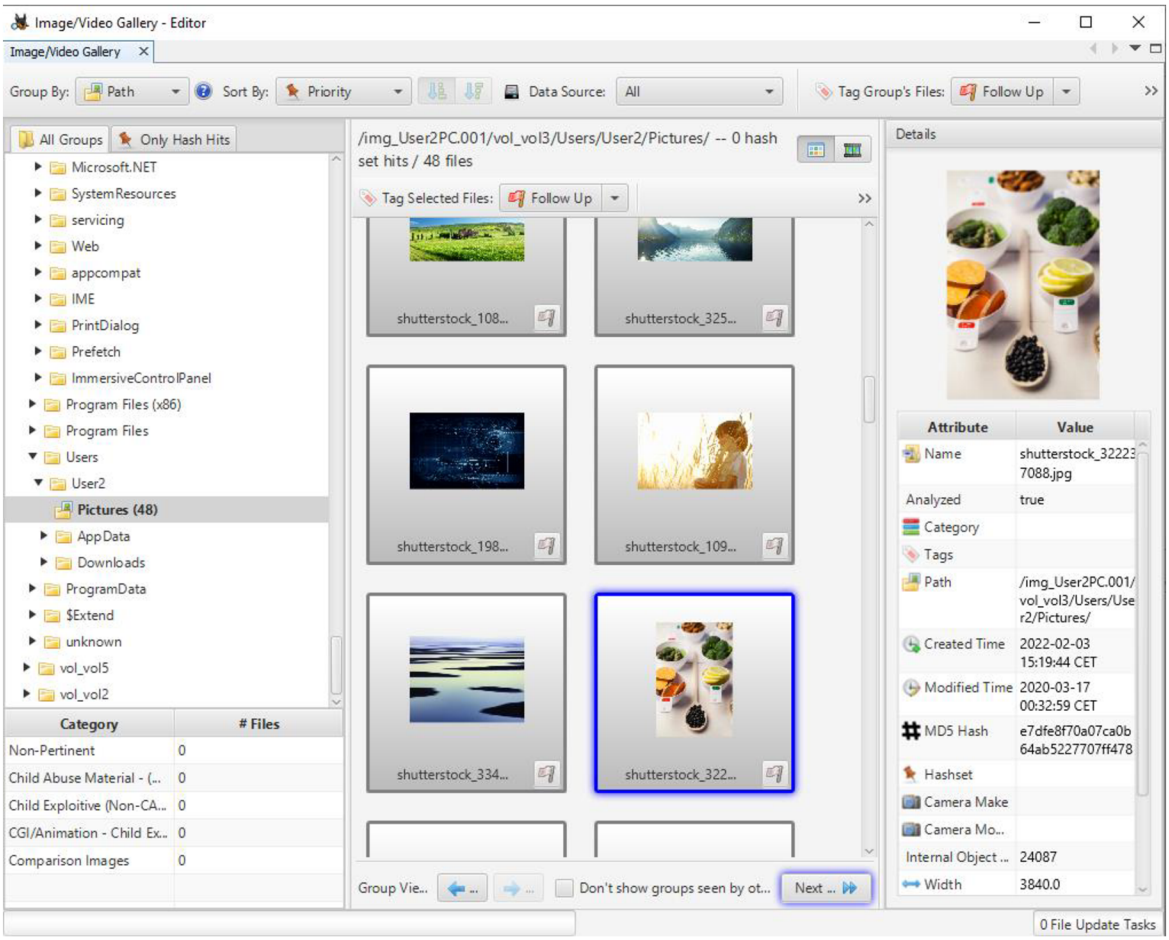


Zdroj: Vlastní zpracování

4.6.5 Obrazové soubory

Identifikace a analýza foto a video souborů identifikovala velké množství systémových obrázků stejně tak, jak se stalo v případě minulého scénáře. Pro ukázku byl vybrán uživatelský soubor ve složce Pictures uživatele.

Obrázek 43: Nalezené obrazové soubory



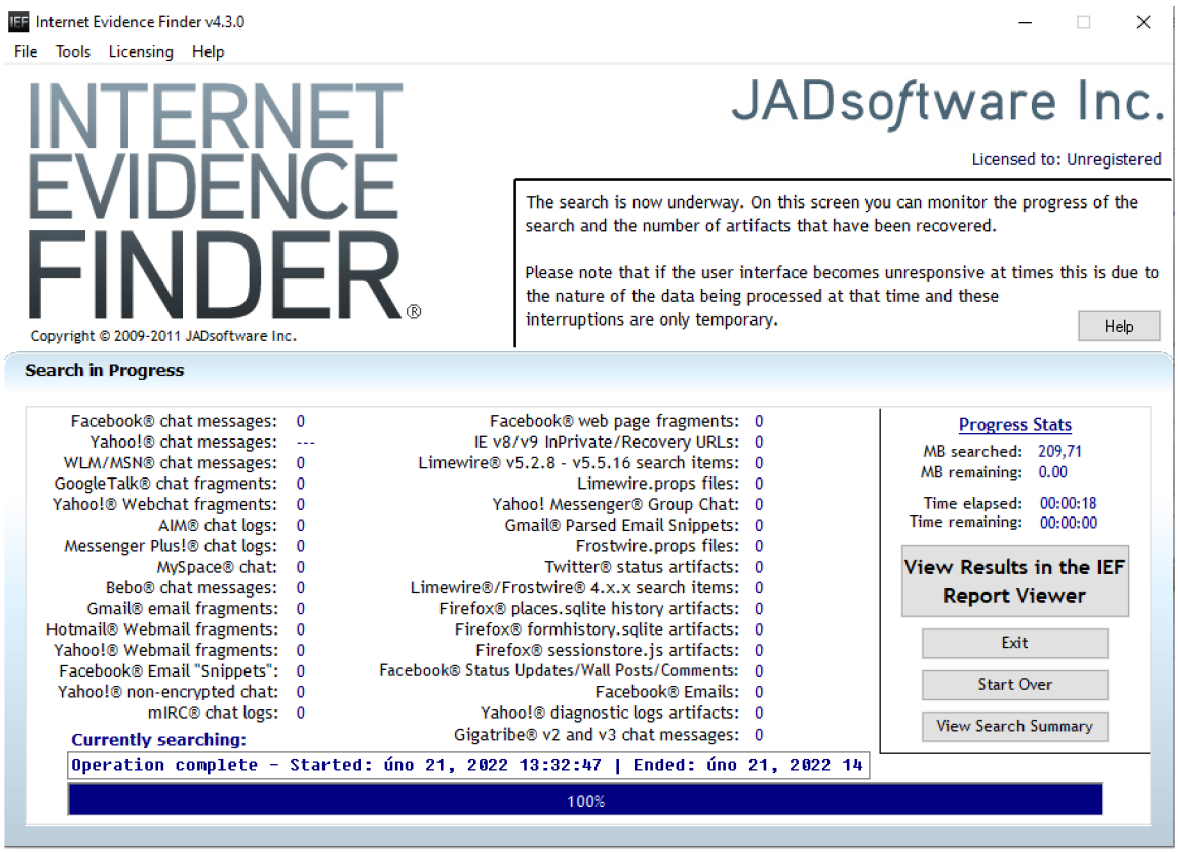
Zdroj: Vlastní zpracování

4.6.6 E-mail a messaging nástroje

Ani v případě druhého scénáře se nepodařilo identifikovat přítomnost e-mail a messaging aplikací. Identifikace byla prováděna jak v prostředí nástroje Autopsy, tak pomocí aplikace Internet Evidence Finder od společnosti Magnet. Lze konstatovat, že uživatel nevyužíval

software spojený s tímto typem komunikace nebo použil webové rozhraní některého z poskytovatelů služeb, které ovšem neukládá data do lokálního systému.

Obrázek 44: Internet evidence finder výsledek hledání



Zdroj: Vlastní zpracování

5 Výsledky a diskuse

5.1 Výsledky a diskuse zajištění a analýzy dat

V systému civilního a trestního soudnictví pomáhá počítačová forenzní věda zajistit integritu digitálních důkazů předložených v soudních případech. Vhledem k tomu, že se počítače a ostatní zařízení, která pracují s různou formou digitálních dat, využívají čím dále častěji v běžných aspektech našich životů, stávají se digitální důkazy a digitální forenzní analýza určená k zajišťování, uchování a zkoumání dat důležitou součástí při řešení různých právních i ostatních problémů.

Průměrná osoba využívající digitální techniku k běžné pracovní či osobní potřebě většinou nemá představu, které všechny informace jsou počítačovými systémy sbírány a zachovávány. Tyto informace mohou být klíčové např. při vyšetřování trestných činů.

Na začátku zpracování vlastní práce bylo vytvořeno virtuální testovací prostředí a napodobena činnost uživatelů operačního systému. Byly vytvořeny dva rozdílné scénáře zajišťování forenzních digitálních dat, které při řešení forenzní analytiky v praxi často nastávají. V jednom ze scénářů je forenzní technik, který provádí zajištění dat, nucen provést potřebné úkony pouze za stavu vypnutého počítače. V druhém případě je tomu naopak, forenzní technik má možnost provést i tzv. analýzu živého systému.

Samotný proces zajištění forenzních dat proběhl v souladu vhodných principů a postupů. Digitální zajištěná forenzní data byla taktéž ošetřena kontrolními hashi MD5 a SHA1, aby byla zaručena nezpochybnitelnost dat.

V rámci rozsahu analýzy, klasifikace a zpracování zajištěných dat byla zkoumána taková data, která by s největší pravděpodobností mohla obsahovat klíčové informace v případě forenzního šetření. Z důvodu množství a obsahu dat na digitálních kopiích nebylo možné analyzovat všechny soubory. V reálné praxi by takovému zkoumání byl podroben specifický typ souborů v závislosti na dané problematice zkoumaného případu.

Bylo identifikováno značné množství systémových dat, taktéž ale i důležitá informace o konfiguraci počítačové stanice, nativních systémových datech, instalovaného softwaru, uživatelské aktivity, jako je např. historie webové aktivity, historie připojení USB zařízení a historie spuštěných aplikací a uživatelských souborů.

Analyzovaná data by v případě potřeby bylo možné vyexportovat a podrobit další expertní analýze v závislosti na potřebách reálného případu.

5.2 Využití forenzní analýzy a její opodstatnění

Využití digitální forenzní analýzy je opodstatněné v širokém spektru případů užití. Jedním z nejdůležitějších případů užití je samotné využití forenzních důkazu zdokumentovaných formou znaleckého posudku jako akceptovatelný důkaz při soudním řízení. Takový znalecký posudek musí být však vyhotoven soudním znalcem s patřičnými oprávněními, musí taktéž podléhat určitým kritériím.

Forenzní analýza však není předmětem pouze policejního či soudního záměru. V dnešní době narůstajících kybernetických hrozeb již vytvářejí soukromé společnosti i státní organizace vlastní interní pozice, aby v případě narušení důvěrnosti, dostupnosti nebo integrity dat existoval interní zaměstnanec s patřičnými vědomostmi a kvalifikací, který je schopen neprodleně učinit nutné kroky k zamezení dalšímu šíření bezpečnostní hrozby a také schopnost zajištění digitálních forenzních dat pro zkoumání příčiny, následků, a pro poučení z dané situace, aby k obdobným případům již nejlépe nedocházelo.

5.3 Možné dopady narušení důvěrnosti, dostupnosti nebo integrity dat

V případě narušení důvěrnosti, dostupnosti nebo integrity dat formou nežádoucího odhalení citlivých dat, modifikací nebo zničení určitých informací může způsobit finanční ztrátu, poškození dobrého jména společnosti a v nejhorších případech i k ohrožení života jejich zaměstnanců nebo klientů.

Aktiva z pohledu informačních systémů je vždy nutné patřičně oklasifikovat a určit, jak vysoký stupeň ochrany si toto aktivum žádá. Stanovení odpovídající ochrany a zabezpečení je možné jedině na základě kvalitní a detailní analýzy rizik.

Vzhledem k tomu, že v praxi není často možné, aby si každý vlastník informačních aktiv prováděl analýzu rizik sám, většinou z časových důvodů, finančních anebo z důvodů neznalosti dané problematiky. Je časté, že vrcholový management společnosti nechá za tímto účelem provést analýzu rizik informačních aktiv společnosti. Cílem takové analýzy je identifikace informačních aktiv, kterými společnost disponuje, a určení hrozeb,

které by mohly ohrozit důvěrnost, integritu nebo dostupnost těchto dat. Tyto tři parametry se označují jako CIA triáda.

Pokud se vezme v potaz narušení této triády, lze hovořit například o vysokých finančních sankcí při úniku dat, která podléhají zákoně o ochraně osobních údajů. Mimo jiné může mít narušení CIA triády ve formě nedostupnosti služby, serveru nebo aplikace přímý finanční dopad ve formě ztráty na zisku po dobu nedostupnosti aktiva. Další častou újmou je poškození dobrého jména firmy např. v důsledku úniku interních dat společnosti.

6 Závěr

Forenzní analýza digitálních dat je v současné době, kdy narůstá množství kybernetických hrozeb, nedílnou součástí při vyšetřování, objasňování a prevencí situací, kdy dochází k narušení triády CIA. Případně mohou její výstupy sloužit jako např. důkazní materiál při občanskoprávních nebo trestně právních řízeních.

K provedení zajištění forenzních digitálních dat je zapotřebí znalých expertů této problematiky. Forenzní technik musí dbát jak na správné technické provedení úkonů, tak na stránku věcí, které vyplývají ze zákonných standardů.

Základem správného provedení zajištění forenzních dat je dodržení takových pravidel, aby byla zaručena v nejlepším žádná změna na zkoumaném médiu v případě, že tak učinit lze. V případě, kdy je forenzní technik nucen činit patřičné operace na živém počítačovém systému, nelze často takové záruky docílit.

Zajištěná forenzní data, jako jsou např. bitové kopie datových médií, dumpy operační paměti a jiné, je nutné minimálně ošetřit pomocí provedení otisku vhodných hashovacích funkcí, aby šlo zpětně zaručit, že s důkazy nebylo manipulováno.

Narušení dostupnosti, integrity nebo důvěrnosti dat je v nynější době řešeno na poli informačně-bezpečnostních entit napříč všemi organizacemi. Organizace by se měly aktivně snažit o provádění analýzy rizik aktiv a provádění patřičných zabezpečení, aby co nejvíce zamezily těmto narušením a dopadům z nich plynoucích.

Při vypracování této práce bylo použito množství různorodých odborných literárních zdrojů, informace získané z nich byly aplikovány v rámci zpracování vlastní části této práce. Vlastní část této práce neanalyzuje veškeré soubory nalezené v rámci zkoumaného file systému z důvodu nemožnosti obsáhnutí klasifikace, analýzy a zpracování každého z nalezených souborů v rámci rozsahu této práce. Tato skutečnost ale nedegraduje přínos práce.

7 Seznam použitých zdrojů

Autopsy [online]. Online: Online, - [cit. 2021-11-07]. Dostupné z: https://www.sleuthkit.org/

BODDINGTON, Richard. *Practical digital forensics*. Birmingham: Packt Publishing, 2016. ISBN 978-1785887109.

Bogdanoski, Mitko. (2018). E-MAIL FORENSICS: TECHNIQUES AND TOOLS FOR FORENSIC INVESTIGATION.

Caine [online]. Online: Online, - [cit. 2021-11-07]. Dostupné z: https://www.caine-live.net/

CASEY, Eoghan. *Handbook of Digital Forensics and Investigation*. Academic Press, 2009. ISBN 978-0123742674.

Cellebrite [online]. Online: Online, - [cit. 2021-11-07]. Dostupné z: https://www.cellebrite.com/en/inspector/

Deft [online]. Online: Online, - [cit. 2021-11-07]. Dostupné z: https://www.linuxandubuntu.com/home/deft-linux-a-linux-distribution-for-computer-forensics

Exiftool [online]. Online: Online, - [cit. 2021-11-07]. Dostupné z: https://exiftool.org/

FAN, Jiayuan, Alex CHICHUNG KOT, Hong CAO a Farook SATTAR. *Modeling the EXIF-Image correlation for image manipulation detection* [online]. online: 18th IEEE International Conference on Image Processing, ICIP 2011, Brussels, Belgium, September 11-14, 2011, 2011 [cit. 2021-11-07]. 10.1109/ICIP.2011.6115853. Dostupné z: https://www.researchgate.net/publication/221122680_Modeling_the_EXIF-Image_correlation_for_image_manipulation_detection

FTK Toolkit [online]. Online: Online, - [cit. 2021-11-07]. Dostupné z: https://accessdata.com/

Github Volatilityfoundation [online]. Online: Online, - [cit. 2022-03-07]. Dostupné z: https://github.com/volatilityfoundation/volatility/wiki/Command-Reference

GOGOLIN, Greg. *Digital forensics explained*. 2nd edition. Abingdon: CRC Press, 2021. ISBN 978-0367503437.

HASSAN, Nihad A. *DIgital Forensics Basics*. New York: Apress, 2019. ISBN 978-1484238370.

HAYES, Darren. *A practical guide to digital forensics investigations*. 2019. Online: Pearson IT Certification, 2019. ISBN 0134892941.

HowToGeek [online]. Online: Online, - [cit. 2022-03-07]. Dostupné z: https://www.howtogeek.com/123646/htg-explains-what-the-windows-event-viewer-is-and-how-you-can-use-it/

KÄVRESTAD, Joakim. *Fundamentals of Digital Forensics*. 2nd edition. Switzerland: Springer Nature, 2020. ISBN 978-3-030-38953-6.

KHANGAR, Smita. *Digital Forensic Investigation for Virtual Machines* [online]. online: International Journal of Modeling and Optimization, 2012 [cit. 2021-11-07]. Dostupné z: https://www.academia.edu/3021092/Digital_Forensic_Investigation_for_Virtual_Machines

Magnet IEF [online]. Online: Online, - [cit. 2022-03-07]. Dostupné z: https://www.magnetforensics.com/products/magnet-ief/

Magnet RAM Capture [online]. Online: Online, - [cit. 2021-11-07]. Dostupné z: https://www.magnetforensics.com/resources/magnet-ram-capture/

Microsoft [online]. Online: Online, 2022 [cit. 2022-03-07]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands

Nmap [online]. Online: Online, - [cit. 2021-11-07]. Dostupné z: https://nmap.org/

Registry Recon [online]. Online: Online, - [cit. 2021-11-07]. Dostupné z: https://www.forensicfocus.com/reviews/registry-recon/

Sgaras, Christos & Kechadi, Tahar & Le-Khac, Nhien-An. (2014). Forensics Acquisition and Analysis of Instant Messaging and VoIP Applications. 10.1007/978-3-319-20125-2_16.

Volatility [online]. Online: Online, - [cit. 2022-03-07]. Dostupné z: https://www.volatilityfoundation.org/about

WILLIAMS, Lawrence. *Digital Forensic* [online]. Online: Online, 2021 [cit. 2021-11-07]. Dostupné z: https://www.guru99.com/digital-forensics.html

Wireshark [online]. Online: Online, - [cit. 2021-11-07]. Dostupné z: https://www.wireshark.org/

ZBROG, Matt. *Guide digital forensic* [online]. online: https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools, 2021 [cit. 2021-11-07].

8 Přílohy

Příloha A: Volatility výstupní data z dumpu operační paměti 76
Příloha B: Ukázka verifikace souborů bitových kopií FTK Imager 81
Příloha C: Výpis Aktivních síťových připojení 83
Příloha D: Výpis spuštěných procesů 85

Příloha A: Volatility výstupní data z dumpu operační paměti

Ukázka výpisu příkazu vol.py -f D:\LiveExaminationOfUser1PC\memdump.mem windows.pslist.PsList

Obrázek 45: Běžící procesy

pslist – Poznámkový blok

Soubor Úpravy Formát Zobrazení Nápověda

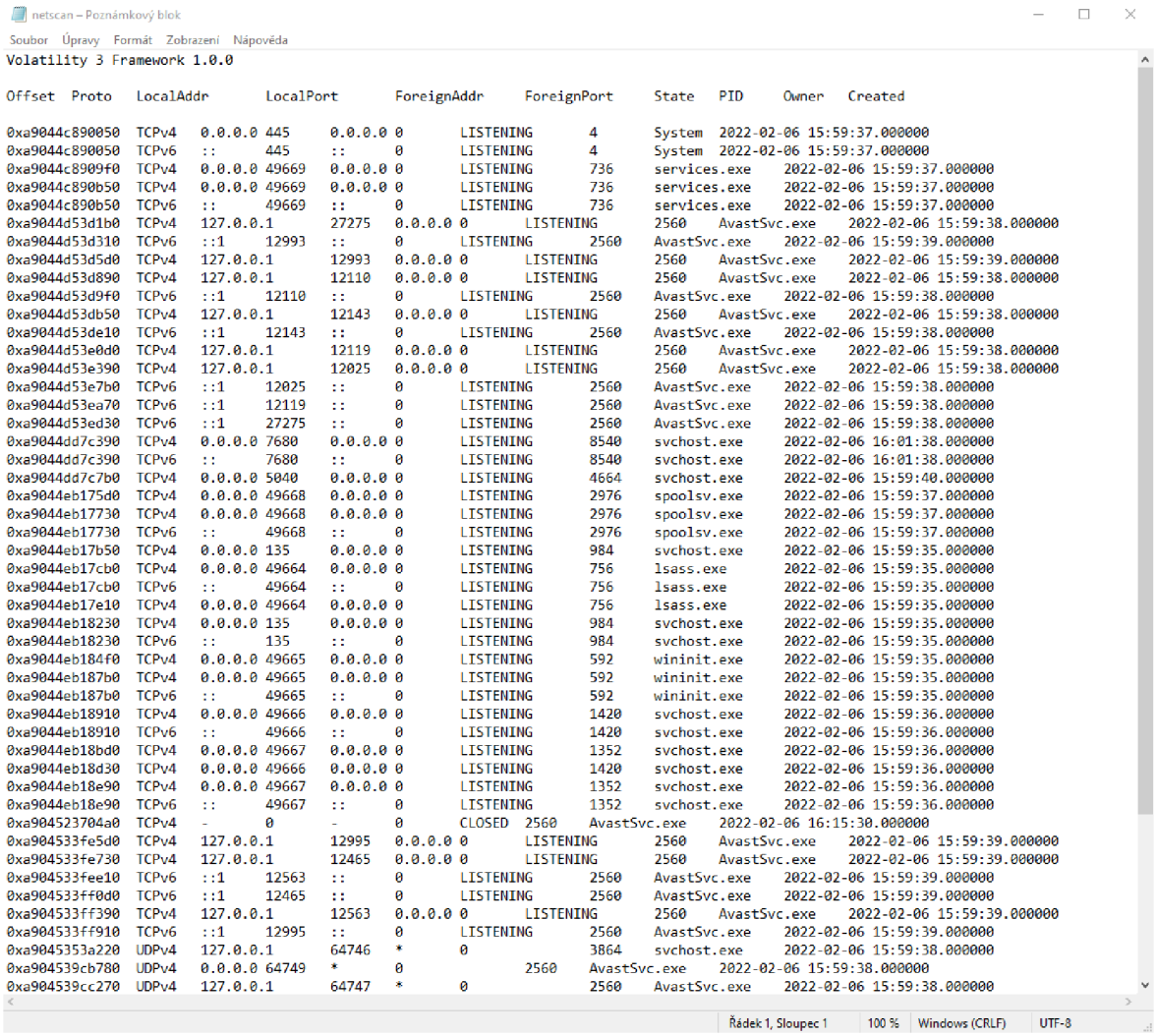
```
Volatility 3 Framework 1.0.0

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xa9044c868040  129     -       N/A     False   2022-02-06 15:59:32.000000      N/A     Disabled
100     4       Registry        0xa9044c9e1080  4       -       N/A     False   2022-02-06 15:59:26.000000      N/A     Disabled
404     4       smss.exe        0xa9044d45b040  2       -       N/A     False   2022-02-06 15:59:32.000000      N/A     Disabled
516     500     csrss.exe       0xa9044eabd080  12      -       0       False   2022-02-06 15:59:35.000000      N/A     Disabled
592     500     wininit.exe     0xa9044e917080  1       -       0       False   2022-02-06 15:59:35.000000      N/A     Disabled
608     584     csrss.exe       0xa9044e916080  13      -       1       False   2022-02-06 15:59:35.000000      N/A     Disabled
692     584     winlogon.exe    0xa9044e953080  5       -       1       False   2022-02-06 15:59:35.000000      N/A     Disabled
736     592     services.exe    0xa9044e979100  8       -       0       False   2022-02-06 15:59:35.000000      N/A     Disabled
756     592     lsass.exe       0xa9044e97f080  9       -       0       False   2022-02-06 15:59:35.000000      N/A     Disabled
872     736     svchost.exe     0xa9044ef6c080  11      -       0       False   2022-02-06 15:59:35.000000      N/A     Disabled
896     692     fontdrvhost.ex  0xa9044ef6b080  5       -       1       False   2022-02-06 15:59:35.000000      N/A     Disabled
904     592     fontdrvhost.ex  0xa9044ef6a080  5       -       0       False   2022-02-06 15:59:35.000000      N/A     Disabled
984     736     svchost.exe     0xa9044ef69080  10      -       0       False   2022-02-06 15:59:35.000000      N/A     Disabled
440     736     svchost.exe     0xa9044ef68080  5       -       0       False   2022-02-06 15:59:35.000000      N/A     Disabled
808     692     dwm.exe 0xa9044ef66080  19      -       1       False   2022-02-06 15:59:35.000000      N/A     Disabled
1120    736     svchost.exe     0xa9044ef29080  3       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1136    736     svchost.exe     0xa9044ef28080  0       -       0       False   2022-02-06 15:59:36.000000      2022-02-06 16:06:34.000000
1240    736     svchost.exe     0xa9044ef27080  2       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1252    736     svchost.exe     0xa9044ef26080  2       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1352    736     svchost.exe     0xa9044ef25080  7       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1420    736     svchost.exe     0xa9044ef242c0  8       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1448    736     svchost.exe     0xa904523a4080  2       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1460    736     svchost.exe     0xa904523a30c0  5       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1528    736     svchost.exe     0xa904523a1080  4       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1540    736     svchost.exe     0xa904523a0080  7       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1604    736     svchost.exe     0xa9045239f080  6       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1788    736     svchost.exe     0xa9045239b080  5       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1820    736     wsc_proxy.exe   0xa9045239a080  10      -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1836    736     svchost.exe     0xa90452399080  4       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1848    736     svchost.exe     0xa90452398080  5       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1864    736     svchost.exe     0xa90452397080  3       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1920    4       MemCompression  0xa90452396040  26      -       N/A     False   2022-02-06 15:59:36.000000      N/A     Disabled
1952    736     svchost.exe     0xa90452395080  5       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1984    736     svchost.exe     0xa904523920c0  2       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
1776    736     svchost.exe     0xa9044edd9080  3       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2004    736     svchost.exe     0xa9044edd8080  2       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2160    736     svchost.exe     0xa9044edd7080  3       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2184    736     svchost.exe     0xa9044edd6080  6       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2240    736     svchost.exe     0xa9044edd5080  9       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2352    736     svchost.exe     0xa9044edd4080  11      -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2456    736     svchost.exe     0xa9044edd2080  3       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2472    736     svchost.exe     0xa9044edd1080  3       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2484    736     svchost.exe     0xa9044edd0080  4       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2536    736     svchost.exe     0xa9044edcf080  4       -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2560    736     AvastSvc.exe    0xa9044ed54080  132     -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2764    736     aswToolsSvc.ex  0xa9044ed532c0  27      -       0       False   2022-02-06 15:59:36.000000      N/A     Disabled
2976    736     spoolsv.exe     0xa9044edd3080  7       -       0       False   2022-02-06 15:59:37.000000      N/A     Disabled
3048    736     svchost.exe     0xa9045239e080  11      -       0       False   2022-02-06 15:59:37.000000      N/A     Disabled
```

Řádek 1, Sloupec 1 | 100 % | Windows (CRLF) | UTF-8

Zdroj: Vlastní zpracování

Ukázka výpisu příkazu vol.py -f D:\LiveExaminationOfUser1PC\memdump.mem netscan

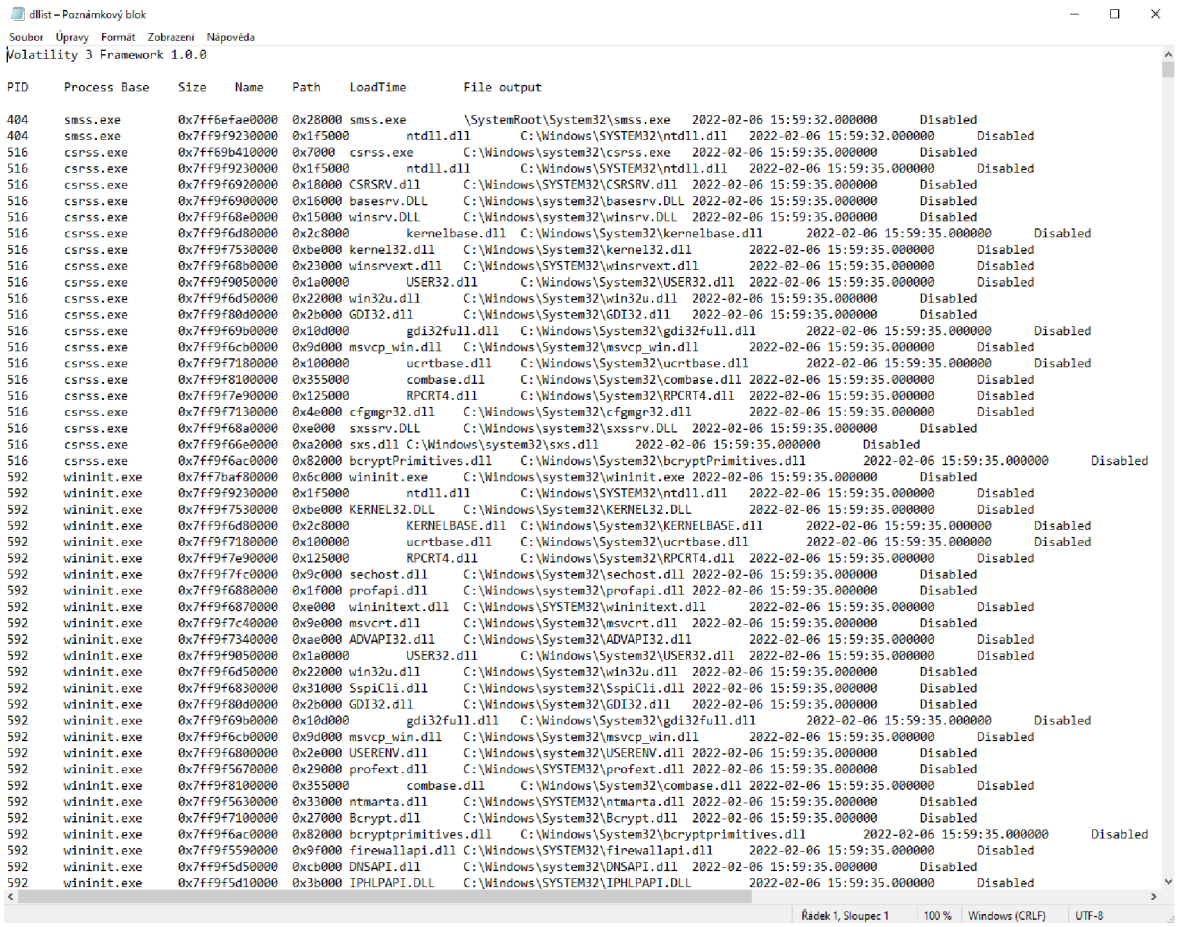
Obrázek 46: Otevřená síťová spojení



Zdroj: Vlastní zpracování

Ukázka výpisu příkazu vol.py -f D:\LiveExaminationOfUser1PC\memdump.mem windows.dlllist.DllList

Obrázek 47: Načtené DLL knihovny



dllist – Poznámkový blok

Soubor Úpravy Formát Zobrazení Nápověda

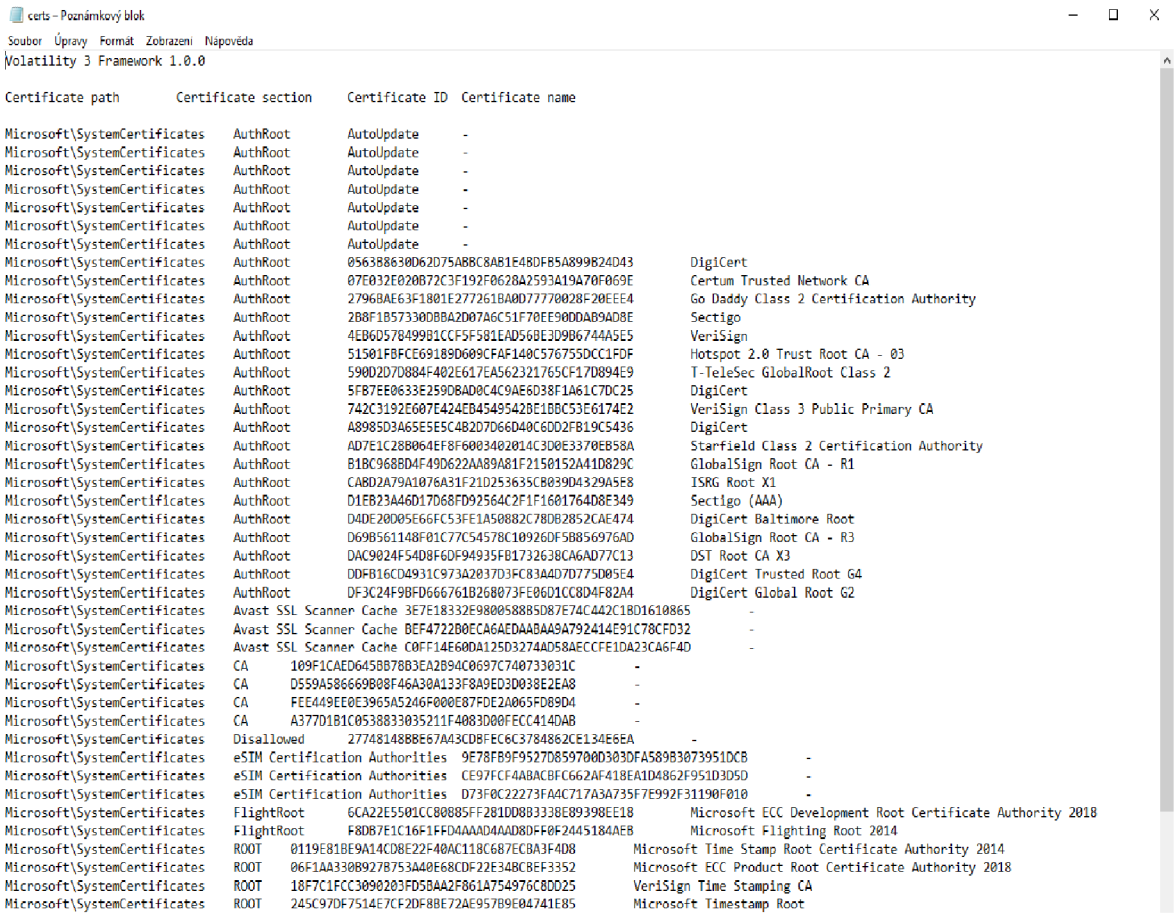
```
Volatility 3 Framework 1.0.0

PID     Process Base    Size    Name    Path    LoadTime        File output

404     smss.exe        0x7ff6efae0000  0x28000 smss.exe        \SystemRoot\System32\smss.exe   2022-02-06 15:59:32.000000      Disabled
404     smss.exe        0x7ff9f9230000  0x1f5000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   2022-02-06 15:59:32.000000      Disabled
516     csrss.exe       0x7ff69b410000  0x7000  csrss.exe       C:\Windows\system32\csrss.exe   2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f9230000  0x1f5000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f6920000  0x18000 CSRSRV.dll      C:\Windows\SYSTEM32\CSRSRV.dll  2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f6900000  0x16000 basesrv.DLL     C:\Windows\system32\basesrv.DLL 2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f68e0000  0x15000 winsrv.DLL      C:\Windows\system32\winsrv.DLL  2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f6d80000  0x2c8000        kernelbase.dll  C:\Windows\System32\kernelbase.dll      2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f7530000  0xbe000 kernel32.dll    C:\Windows\System32\kernel32.dll        2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f68b0000  0x23000 winsrvext.dll   C:\Windows\SYSTEM32\winsrvext.dll       2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f9050000  0x1a0000        USER32.dll      C:\Windows\System32\USER32.dll  2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f6d50000  0x22000 win32u.dll      C:\Windows\System32\win32u.dll  2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f80d0000  0x2b000 GDI32.dll       C:\Windows\System32\GDI32.dll   2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f69b0000  0x10d000        gdi32full.dll   C:\Windows\System32\gdi32full.dll       2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f6cb0000  0x9d000 msvcp_win.dll   C:\Windows\System32\msvcp_win.dll       2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f7180000  0x100000        ucrtbase.dll    C:\Windows\System32\ucrtbase.dll        2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f8100000  0x355000        combase.dll     C:\Windows\System32\combase.dll 2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f7e90000  0x125000        RPCRT4.dll      C:\Windows\System32\RPCRT4.dll  2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f7130000  0x4e000 cfgmgr32.dll    C:\Windows\System32\cfgmgr32.dll        2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f68a0000  0xe000  sxssrv.DLL      C:\Windows\system32\sxssrv.DLL  2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f66e0000  0xa2000 sxs.dll C:\Windows\system32\sxs.dll      2022-02-06 15:59:35.000000      Disabled
516     csrss.exe       0x7ff9f6ac0000  0x82000 bcryptPrimitives.dll    C:\Windows\System32\bcryptPrimitives.dll        2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff7baf80000  0x6c000 wininit.exe     C:\Windows\system32\wininit.exe 2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f9230000  0x1f5000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f7530000  0xbe000 KERNEL32.DLL    C:\Windows\System32\KERNEL32.DLL        2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f6d80000  0x2c8000        KERNELBASE.dll  C:\Windows\System32\KERNELBASE.dll      2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f7180000  0x100000        ucrtbase.dll    C:\Windows\System32\ucrtbase.dll        2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f7e90000  0x125000        RPCRT4.dll      C:\Windows\System32\RPCRT4.dll  2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f7fc0000  0x9c000 sechost.dll     C:\Windows\System32\sechost.dll 2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f6880000  0x1f000 profapi.dll     C:\Windows\System32\profapi.dll 2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f6870000  0xe000  wininitext.dll  C:\Windows\SYSTEM32\wininitext.dll      2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f7c40000  0x9e000 msvcrt.dll      C:\Windows\System32\msvcrt.dll  2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f7340000  0xae000 ADVAPI32.dll    C:\Windows\System32\ADVAPI32.dll        2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f9050000  0x1a0000        USER32.dll      C:\Windows\System32\USER32.dll  2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f6d50000  0x22000 win32u.dll      C:\Windows\System32\win32u.dll  2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f6830000  0x31000 SspiCli.dll     C:\Windows\system32\SspiCli.dll 2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f80d0000  0x2b000 GDI32.dll       C:\Windows\System32\GDI32.dll   2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f69b0000  0x10d000        gdi32full.dll   C:\Windows\System32\gdi32full.dll       2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f6cb0000  0x9d000 msvcp_win.dll   C:\Windows\System32\msvcp_win.dll       2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f6800000  0x2e000 USERENV.dll     C:\Windows\system32\USERENV.dll 2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f5670000  0x29000 profext.dll     C:\Windows\SYSTEM32\profext.dll 2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f8100000  0x355000        combase.dll     C:\Windows\System32\combase.dll 2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f5630000  0x33000 ntmarta.dll     C:\Windows\SYSTEM32\ntmarta.dll 2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f7100000  0x27000 Bcrypt.dll      C:\Windows\System32\Bcrypt.dll  2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f6ac0000  0x82000 bcryptprimitives.dll    C:\Windows\System32\bcryptprimitives.dll        2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f5590000  0x9f000 firewallapi.dll C:\Windows\SYSTEM32\firewallapi.dll      2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f5d50000  0xcb000 DNSAPI.dll      C:\Windows\system32\DNSAPI.dll  2022-02-06 15:59:35.000000      Disabled
592     wininit.exe     0x7ff9f5d10000  0x3b000 IPHLPAPI.DLL    C:\Windows\SYSTEM32\IPHLPAPI.DLL        2022-02-06 15:59:35.000000      Disabled
```

Řádek 1, Sloupec 1 | 100 % | Windows (CRLF) | UTF-8

Zdroj: Vlastní zpracování

Ukázka výpisu příkazu vol.py -f D:\LiveExaminationOfUser1PC\memdump.mem windows.registry.certificates.Certificates

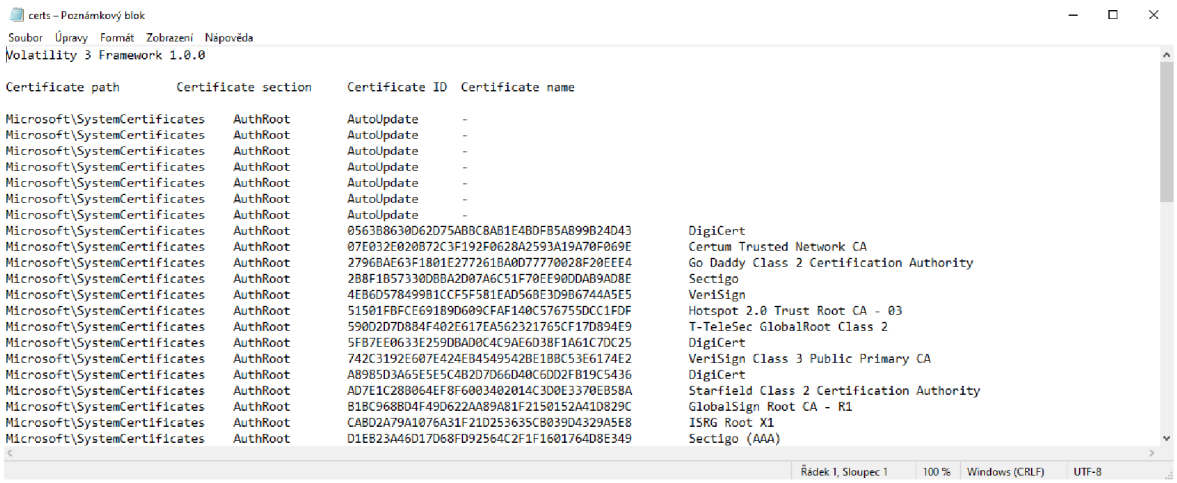
Obrázek 48: Certifikáty



Zdroj: Vlastní zpracování

Ukázka výpisu příkazu vol.py -f D:\LiveExaminationOfUser1PC\memdump.mem windows.registry.hivelist.HiveList a exportu certifikátů

Obrázek 49: Registry



certs – Poznámkový blok

Soubor Úpravy Formát Zobrazení Nápověda

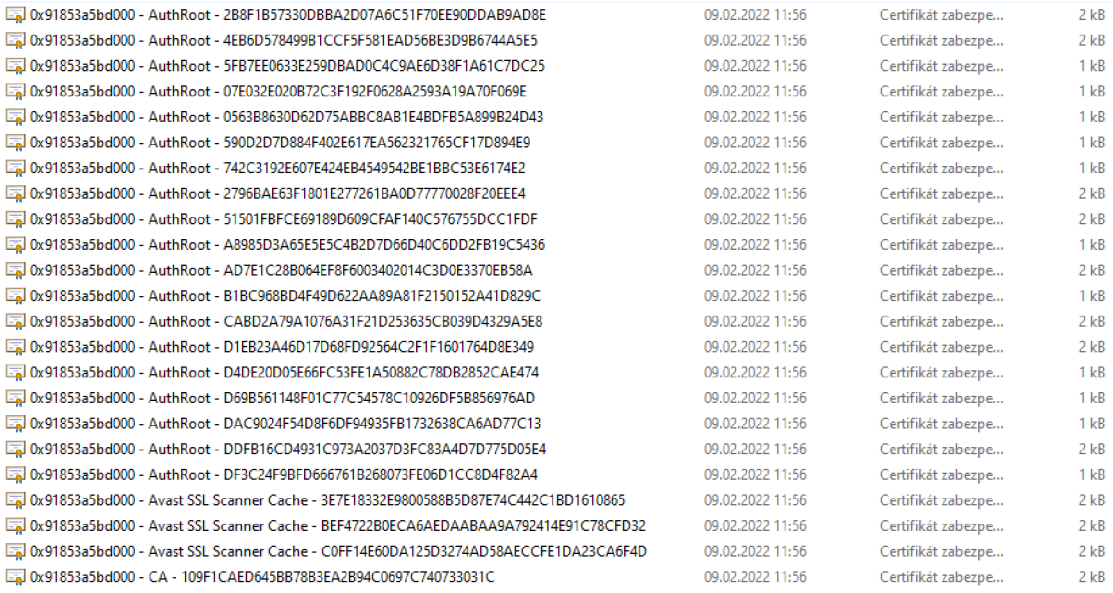
```
Volatility 3 Framework 1.0.0

Certificate path        Certificate section     Certificate ID  Certificate name

Microsoft\SystemCertificates    AuthRoot        AutoUpdate      -
Microsoft\SystemCertificates    AuthRoot        AutoUpdate      -
Microsoft\SystemCertificates    AuthRoot        AutoUpdate      -
Microsoft\SystemCertificates    AuthRoot        AutoUpdate      -
Microsoft\SystemCertificates    AuthRoot        AutoUpdate      -
Microsoft\SystemCertificates    AuthRoot        AutoUpdate      -
Microsoft\SystemCertificates    AuthRoot        AutoUpdate      -
Microsoft\SystemCertificates    AuthRoot        0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43        DigiCert
Microsoft\SystemCertificates    AuthRoot        07E032E020B72C3F192F0628A2593A19A70F069E        Certum Trusted Network CA
Microsoft\SystemCertificates    AuthRoot        2796BAE63F1801E277261BA0D77770028F20EEE4        Go Daddy Class 2 Certification Authority
Microsoft\SystemCertificates    AuthRoot        2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E        Sectigo
Microsoft\SystemCertificates    AuthRoot        4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5        VeriSign
Microsoft\SystemCertificates    AuthRoot        51501FBFCE69189D609CFAF140C576755DCC1FDF        Hotspot 2.0 Trust Root CA - 03
Microsoft\SystemCertificates    AuthRoot        590D2D7D884F402E617EA562321765CF17D894E9        T-TeleSec GlobalRoot Class 2
Microsoft\SystemCertificates    AuthRoot        5FB7EE0633E259DBAD0C4C9AE6D38F1A61C7DC25        DigiCert
Microsoft\SystemCertificates    AuthRoot        742C3192E607E424EB4549542BE1BBC53E6174E2        VeriSign Class 3 Public Primary CA
Microsoft\SystemCertificates    AuthRoot        A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436        DigiCert
Microsoft\SystemCertificates    AuthRoot        AD7E1C288064EF8F6003402014C3D0E3370EB58A        Starfield Class 2 Certification Authority
Microsoft\SystemCertificates    AuthRoot        B1BC968BD4F49D622AA89A81F2150152A41D829C        GlobalSign Root CA - R1
Microsoft\SystemCertificates    AuthRoot        CABD2A79A1076A31F21D253635CB039D4329A5E8        ISRG Root X1
Microsoft\SystemCertificates    AuthRoot        D1EB23A46D17D68FD92564C2F1F1601764D8E349        Sectigo (AAA)
```

Řádek 1, Sloupec 1 | 100 % | Windows (CRLF) | UTF-8

Zdroj: Vlastní zpracování

Ukázka exportu certifikátů z memdump.mem

Obrázek 50: Exportované certifikáty

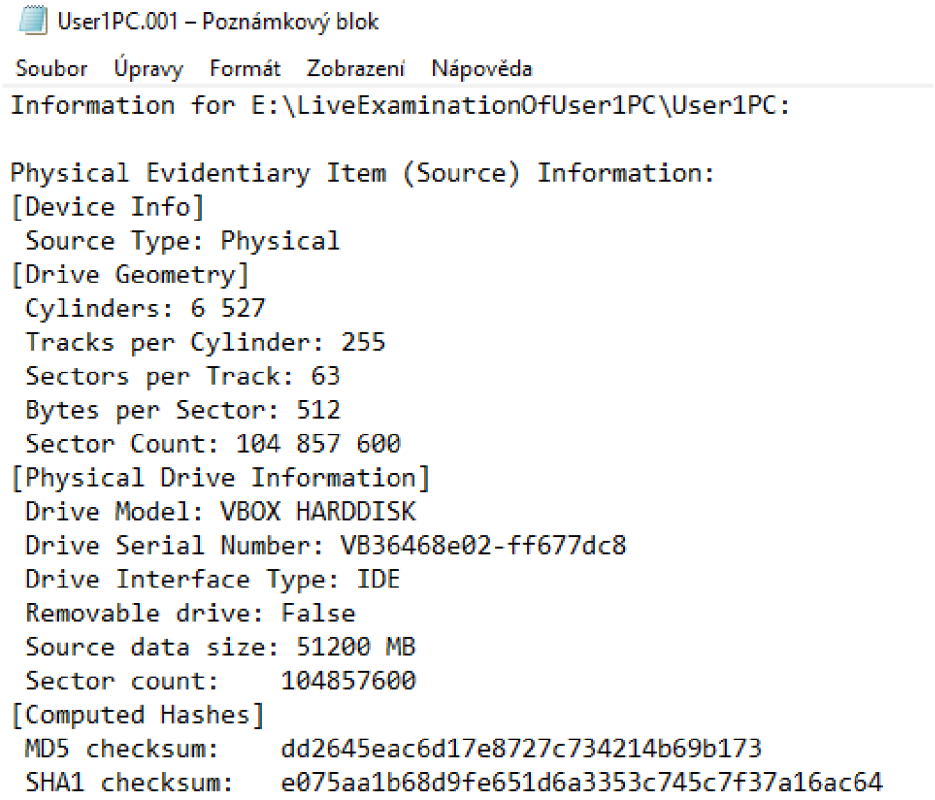


0x91853a5bd000 - AuthRoot - 2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E	09.02.2022 11:56	Certifikát zabezpe...	2 kB
0x91853a5bd000 - AuthRoot - 4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5	09.02.2022 11:56	Certifikát zabezpe...	2 kB
0x91853a5bd000 - AuthRoot - 5FB7EE0633E259DBAD0C4C9AE6D38F1A61C7DC25	09.02.2022 11:56	Certifikát zabezpe...	1 kB
0x91853a5bd000 - AuthRoot - 07E032E020B72C3F192F0628A2593A19A70F069E	09.02.2022 11:56	Certifikát zabezpe...	1 kB
0x91853a5bd000 - AuthRoot - 0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43	09.02.2022 11:56	Certifikát zabezpe...	1 kB
0x91853a5bd000 - AuthRoot - 590D2D7D884F402E617EA562321765CF17D894E9	09.02.2022 11:56	Certifikát zabezpe...	1 kB
0x91853a5bd000 - AuthRoot - 742C3192E607E424EB4549542BE1BBC53E6174E2	09.02.2022 11:56	Certifikát zabezpe...	1 kB
0x91853a5bd000 - AuthRoot - 2796BAE63F1801E277261BA0D77770028F20EEE4	09.02.2022 11:56	Certifikát zabezpe...	2 kB
0x91853a5bd000 - AuthRoot - 51501FBFCE69189D609CFAF140C576755DCC1FDF	09.02.2022 11:56	Certifikát zabezpe...	2 kB
0x91853a5bd000 - AuthRoot - A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436	09.02.2022 11:56	Certifikát zabezpe...	1 kB
0x91853a5bd000 - AuthRoot - AD7E1C28B064EF8F6003402014C3D0E3370EB58A	09.02.2022 11:56	Certifikát zabezpe...	2 kB
0x91853a5bd000 - AuthRoot - B1BC968BD4F49D622AA89A81F2150152A41D829C	09.02.2022 11:56	Certifikát zabezpe...	1 kB
0x91853a5bd000 - AuthRoot - CABD2A79A1076A31F21D253635CB039D4329A5E8	09.02.2022 11:56	Certifikát zabezpe...	2 kB
0x91853a5bd000 - AuthRoot - D1EB23A46D17D68FD92564C2F1F1601764D8E349	09.02.2022 11:56	Certifikát zabezpe...	2 kB
0x91853a5bd000 - AuthRoot - D4DE20D05E66FC53FE1A50882C78DB2852CAE474	09.02.2022 11:56	Certifikát zabezpe...	1 kB
0x91853a5bd000 - AuthRoot - D69B561148F01C77C54578C10926DF5B856976AD	09.02.2022 11:56	Certifikát zabezpe...	1 kB
0x91853a5bd000 - AuthRoot - DAC9024F54D8F6DF94935FB1732638CA6AD77C13	09.02.2022 11:56	Certifikát zabezpe...	1 kB
0x91853a5bd000 - AuthRoot - DDFB16CD4931C973A2037D3FC83A4D7D775D05E4	09.02.2022 11:56	Certifikát zabezpe...	2 kB
0x91853a5bd000 - AuthRoot - DF3C24F9BFD666761B268073FE06D1CC8D4F82A4	09.02.2022 11:56	Certifikát zabezpe...	1 kB
0x91853a5bd000 - Avast SSL Scanner Cache - 3E7E18332E9800588B5D87E74C442C1BD1610865	09.02.2022 11:56	Certifikát zabezpe...	2 kB
0x91853a5bd000 - Avast SSL Scanner Cache - BEF4722B0ECA6AEDAABAA9A792414E91C78CFD32	09.02.2022 11:56	Certifikát zabezpe...	2 kB
0x91853a5bd000 - Avast SSL Scanner Cache - C0FF14E60DA125D3274AD58AECCFE1DA23CA6F4D	09.02.2022 11:56	Certifikát zabezpe...	2 kB
0x91853a5bd000 - CA - 109F1CAED645BB78B3EA2B94C0697C740733031C	09.02.2022 11:56	Certifikát zabezpe...	2 kB

Zdroj: Vlastní zpracování

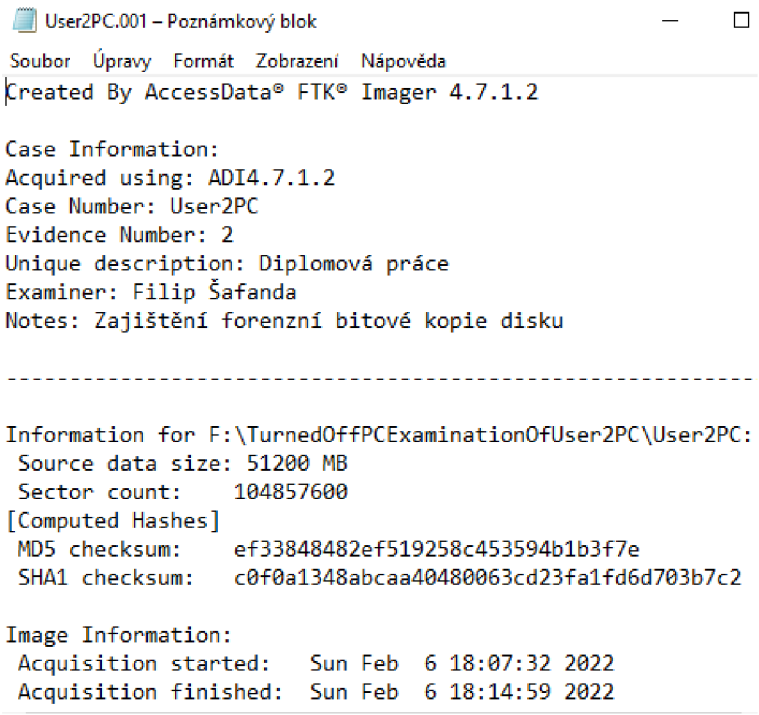
Příloha B: Ukázka verifikace souborů bitových kopií FTK Imager

Obrázek 51: Ověření bitové kopie



Zdroj: Vlastní zpracování

Obrázek 52: Ověření bitové kopie



Zdroj: Vlastní zpracování

Příloha C: Výpis Aktivních síťových připojení

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	DESKTOP-3T5SL6T:0	LISTENING
TCP	0.0.0.0:445	DESKTOP-3T5SL6T:0	LISTENING
TCP	0.0.0.0:5040	DESKTOP-3T5SL6T:0	LISTENING
TCP	0.0.0.0:7680	DESKTOP-3T5SL6T:0	LISTENING
TCP	0.0.0.0:49664	DESKTOP-3T5SL6T:0	LISTENING
TCP	0.0.0.0:49665	DESKTOP-3T5SL6T:0	LISTENING
TCP	0.0.0.0:49666	DESKTOP-3T5SL6T:0	LISTENING
TCP	0.0.0.0:49667	DESKTOP-3T5SL6T:0	LISTENING
TCP	0.0.0.0:49668	DESKTOP-3T5SL6T:0	LISTENING
TCP	0.0.0.0:49669	DESKTOP-3T5SL6T:0	LISTENING
TCP	127.0.0.1:12025	DESKTOP-3T5SL6T:0	LISTENING
TCP	127.0.0.1:12110	DESKTOP-3T5SL6T:0	LISTENING
TCP	127.0.0.1:12119	DESKTOP-3T5SL6T:0	LISTENING
TCP	127.0.0.1:12143	DESKTOP-3T5SL6T:0	LISTENING
TCP	127.0.0.1:12465	DESKTOP-3T5SL6T:0	LISTENING
TCP	127.0.0.1:12563	DESKTOP-3T5SL6T:0	LISTENING
TCP	127.0.0.1:12993	DESKTOP-3T5SL6T:0	LISTENING
TCP	127.0.0.1:12995	DESKTOP-3T5SL6T:0	LISTENING
TCP	127.0.0.1:27275	DESKTOP-3T5SL6T:0	LISTENING
TCP	[::]:135	DESKTOP-3T5SL6T:0	LISTENING
TCP	[::]:445	DESKTOP-3T5SL6T:0	LISTENING
TCP	[::]:7680	DESKTOP-3T5SL6T:0	LISTENING
TCP	[::]:49664	DESKTOP-3T5SL6T:0	LISTENING
TCP	[::]:49665	DESKTOP-3T5SL6T:0	LISTENING
TCP	[::]:49666	DESKTOP-3T5SL6T:0	LISTENING
TCP	[::]:49667	DESKTOP-3T5SL6T:0	LISTENING
TCP	[::]:49668	DESKTOP-3T5SL6T:0	LISTENING
TCP	[::]:49669	DESKTOP-3T5SL6T:0	LISTENING

```
TCP  [::1]:12025      DESKTOP-3T5SL6T:0   LISTENING
TCP  [::1]:12110      DESKTOP-3T5SL6T:0   LISTENING
TCP  [::1]:12119      DESKTOP-3T5SL6T:0   LISTENING
TCP  [::1]:12143      DESKTOP-3T5SL6T:0   LISTENING
TCP  [::1]:12465      DESKTOP-3T5SL6T:0   LISTENING
TCP  [::1]:12563      DESKTOP-3T5SL6T:0   LISTENING
TCP  [::1]:12993      DESKTOP-3T5SL6T:0   LISTENING
TCP  [::1]:12995      DESKTOP-3T5SL6T:0   LISTENING
TCP  [::1]:27275      DESKTOP-3T5SL6T:0   LISTENING
UDP  0.0.0.0:5050      *:*
UDP  0.0.0.0:64749     *:*
UDP  127.0.0.1:1900    *:*
UDP  127.0.0.1:50817   *:*
UDP  127.0.0.1:64746   *:*
UDP  127.0.0.1:64747   *:*
UDP  [::1]:1900        *:*
UDP  [::1]:50816       *:*
```

Příloha D: Výpis spuštěných procesů

```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        136 K
Registry                       100 Services                   0     76˙064 K
smss.exe                       404 Services                   0      1˙152 K
csrss.exe                      516 Services                   0      5˙560 K
wininit.exe                    592 Services                   0      6˙992 K
csrss.exe                      608 Console                    1      5˙388 K
winlogon.exe                   692 Console                    1     11˙676 K
services.exe                   736 Services                   0     10˙032 K
lsass.exe                      756 Services                   0     17˙908 K
svchost.exe                    872 Services                   0     25˙276 K
fontdrvhost.exe                896 Console                    1      6˙432 K
fontdrvhost.exe                904 Services                   0      4˙372 K
svchost.exe                    984 Services                   0     14˙000 K
svchost.exe                    440 Services                   0      8˙204 K
dwm.exe                        808 Console                    1     65˙728 K
svchost.exe                   1120 Services                   0      6˙132 K
svchost.exe                   1240 Services                   0      9˙980 K
svchost.exe                   1252 Services                   0      8˙272 K
svchost.exe                   1352 Services                   0     15˙564 K
svchost.exe                   1420 Services                   0     19˙208 K
svchost.exe                   1448 Services                   0      7˙232 K
svchost.exe                   1460 Services                   0     13˙980 K
svchost.exe                   1528 Services                   0      7˙920 K
svchost.exe                   1540 Services                   0     20˙492 K
svchost.exe                   1604 Services                   0      7˙452 K
svchost.exe                   1788 Services                   0     11˙608 K
wsc_proxy.exe                 1820 Services                   0     12˙964 K
```

svchost.exe 1836 Services 0 60˙464 K
svchost.exe 1848 Services 0 7˙828 K
svchost.exe 1864 Services 0 5˙916 K
Memory Compression 1920 Services 0 2˙188 K
svchost.exe 1952 Services 0 9˙320 K
svchost.exe 1984 Services 0 9˙544 K
svchost.exe 1776 Services 0 11˙772 K
svchost.exe 2004 Services 0 7˙596 K
svchost.exe 2160 Services 0 7˙932 K
svchost.exe 2184 Services 0 7˙332 K
svchost.exe 2240 Services 0 8˙056 K
svchost.exe 2352 Services 0 13˙508 K
svchost.exe 2456 Services 0 16˙736 K
svchost.exe 2472 Services 0 7˙420 K
svchost.exe 2484 Services 0 9˙676 K
svchost.exe 2536 Services 0 13˙924 K
AvastSvc.exe 2560 Services 0 142˙388 K
aswToolsSvc.exe 2764 Services 0 49˙216 K
spoolsv.exe 2976 Services 0 15˙516 K
svchost.exe 3048 Services 0 18˙280 K
svchost.exe 2084 Services 0 8˙200 K
aswEngSrv.exe 3236 Services 0 65˙156 K
svchost.exe 3324 Services 0 8˙564 K
svchost.exe 3384 Services 0 10˙364 K
svchost.exe 3392 Services 0 27˙604 K
armsvc.exe 3400 Services 0 6˙284 K
svchost.exe 3408 Services 0 18˙160 K
svchost.exe 3436 Services 0 18˙392 K
svchost.exe 3516 Services 0 9˙244 K
svchost.exe 3544 Services 0 6˙868 K
svchost.exe 3564 Services 0 5˙824 K
svchost.exe 3580 Services 0 20˙836 K
svchost.exe 3728 Services 0 5˙564 K

svchost.exe 3864 Services 0 10˙996 K
svchost.exe 3944 Services 0 12˙788 K
sihost.exe 1684 Console 1 28˙088 K
svchost.exe 4124 Console 1 18˙036 K
svchost.exe 4176 Console 1 38˙360 K
taskhostw.exe 4292 Console 1 15˙056 K
svchost.exe 4364 Services 0 14˙796 K
svchost.exe 4500 Services 0 12˙132 K
svchost.exe 4596 Services 0 8˙136 K
ctfmon.exe 4708 Console 1 21˙212 K
WUDFHost.exe 4816 Services 0 8˙832 K
svchost.exe 4988 Services 0 11˙064 K
aswidsagent.exe 5020 Services 0 42˙540 K
svchost.exe 4664 Services 0 16˙716 K
explorer.exe 5472 Console 1 140˙968 K
svchost.exe 5668 Services 0 10˙012 K
unsecapp.exe 5864 Services 0 6˙948 K
svchost.exe 6116 Console 1 22˙056 K
svchost.exe 6216 Services 0 18˙964 K
svchost.exe 6300 Services 0 40˙184 K
StartMenuExperienceHost.e 6388 Console 1 65˙496 K
RuntimeBroker.exe 6552 Console 1 23˙908 K
svchost.exe 6560 Services 0 8˙820 K
SearchApp.exe 6832 Console 1 214˙256 K
RuntimeBroker.exe 6948 Console 1 51˙412 K
SearchIndexer.exe 7192 Services 0 26˙084 K
YourPhone.exe 7348 Console 1 3˙716 K
ShellExperienceHost.exe 7708 Console 1 50˙368 K
RuntimeBroker.exe 7860 Console 1 17˙248 K
RuntimeBroker.exe 7968 Console 1 19˙868 K
RuntimeBroker.exe 1056 Console 1 18˙292 K
smartscreen.exe 7520 Console 1 24˙608 K
SecurityHealthSystray.exe 7504 Console 1 9˙736 K

SecurityHealthService.exe 6156 Services 0 15˙624 K

AvastUI.exe 6148 Console 1 43˙856 K

CCleaner64.exe 2336 Console 1 24˙932 K

jusched.exe 892 Console 1 8˙016 K

svchost.exe 7204 Services 0 12˙628 K

svchost.exe 8172 Console 1 21˙000 K

ApplicationFrameHost.exe 8528 Console 1 26˙116 K

svchost.exe 8988 Services 0 9˙696 K

TextInputHost.exe 2144 Console 1 39˙120 K

dllhost.exe 3096 Console 1 13˙212 K

svchost.exe 8892 Services 0 7˙824 K

svchost.exe 8540 Services 0 16˙568 K

svchost.exe 9152 Services 0 11˙916 K

SgrmBroker.exe 8644 Services 0 7˙992 K

cmd.exe 8448 Console 1 4˙732 K

conhost.exe 7716 Console 1 21˙548 K

WmiPrvSE.exe 5856 Services 0 9˙384 K

svchost.exe 5908 Services 0 11˙340 K

svchost.exe 3932 Services 0 14˙028 K

svchost.exe 6024 Services 0 6˙572 K

dllhost.exe 2660 Console 1 8˙292 K

AvastUI.exe 1968 Console 1 38˙144 K

AvastUI.exe 8908 Console 1 32˙340 K

AvastUI.exe 436 Console 1 35˙544 K

svchost.exe 2448 Services 0 7˙448 K

svchost.exe 8952 Services 0 7˙988 K

tasklist.exe 2592 Console 1 10˙200 K

WmiPrvSE.exe 8196 Services 0 9˙612 K