Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Analýza artefaktů počítačové forenziky v podnikovém prostředí

Ella Ponomareva

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ella Ponomareva

Podnikání a administrativa

Název práce

Analýza artefaktů počítačové forenziky v podnikovém prostředí

Název anglicky

Analysis of computer forensics artifacts in an enterprise environment

---

Cíle práce

Hlavním cílem bakalářské práce je navrhnout postup pro sběr artefaktů v operačním systému Microsoft Windows.
Dílčím cílem je analyzovat artefakty počítačové forenziky v operačním systému Microsoft Windows za účelem získání užitečných informací k potvrzení přítomnosti činností souvisejících s ekonomickými podvody na zařízení.

Metodika

Teoretická části práce se bude zabývat hospodářskou kriminalitou v IT na základě studia odborné a vědecké literatury. Budou analyzovány druhy hospodářské kriminality, motivační faktory vedoucí k hospodářské kriminalitě a podvodům, a také bude zdůrazněn význam klasického a digitálního forenzního auditu při vyšetřování trestných činů. Dále budou zpracovány přehledy forenziky jako vědy zabývající se vyšetřováním kyberkriminality a počítačové kriminality jako oboru forenzní vědy. V rámci toho budou rozebrány oblasti, fáze vyšetřování, forenzní metody, základní vyšetřovací techniky, artefakty a existující řešení pro jejich sběr v IT.

V praktické části práce bude navržena vhodná metoda pro sběr artefaktů v operačním systému Microsoft Windows. Metoda bude obsahovat popis způsobů sbíraní a analýzy různých artefaktů.

Doporučený rozsah práce

30 -40 stran

Klíčová slova

Digitální stopy, forenzní analýza, IT, bezpečnost, počítačová kriminalita, hospodářská kriminalita, ekonomický podvod, digitální forenzní audit

---

Doporučené zdroje informací

Albrecht, Albrecht, Albrecht, & Zimbelman. (2009). Fraud Examination . USA.

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

Brodowski, & Freiling. (2011). Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft. Berlin

Casey. (2011). Digital Evidence and Computer Crime, Forensic Science, Computers and Internet.

Larry E. Daniel and Lars E. Daniel. (2012). Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom

Porada Viktor a kolektiv. (2019). Kriminalistika – Technické, forenzní a kybernetické aspekty. Plzeň

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Ivana Hellerová

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 7. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 11. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Analýza artefaktů počítačové forenziky v podnikovém prostředí" jsem vypracovala samostatně pod vedením vedoucího bakalářské 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 autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2024 _____

Poděkování

Ráda bych touto cestou poděkovala své vedoucí Ing. Ivaně Hellerově za odborné vedení, cenné rady, připomínky a trpělivost při zpracování mé bakalářské práce a Ing. Václavu Lohrovi, Ph.D. za pomoc a užitečné rady. A také své rodině za podporu v nejtěžších obdobích.

Analýza artefaktů počítačové forenziky v podnikovém prostředí

Abstrakt

Tato bakalářská práce se věnuje studiu digitálních podvodů a skrytých podvodů ve firmách a metodám odhalování těchto trestných činů v počítačovém prostředí. Hlavním cílem práce je vyvinout metodu sběru artefaktů pro vyšetřování trestných činů a identifikaci narušitelů, jakož i analýzu dokumentů pozměněných nebo prozrazených třetím stranám za účelem nalezení stop po nezákonné činnosti. Obsahuje teoretickou i praktickou část. Teoretická část popisuje základní pojmy hospodářské činnosti a kriminalistiky, dále počítačovou forenzní vědu a přehled počítačových forenzních artefaktů potřebných pro vyšetřování. Praktická část se zaměřuje na vypracování metody sběru artefaktů pro vyšetřování a odhalování pachatelů a pro její použití v soudním řízení, jakož i na základní postupy používané při ohledání místa činu k získání spolehlivých digitálních důkazů a na analýzu artefaktů za účelem získání užitečných informací.

Klíčová slova: Ekonomické podvody, hospodářská kriminalita, motivační faktory, vyšetřování trestných činů, forenzní věda, počítačová kriminalistika, klasický a digitální forenzní audit, řešení pro sběr artefaktů, metoda pro detekci artefaktů, operační systém Microsoft Windows

Analysis of computer forensics artifacts in an enterprise environment

Abstract

This bachelor's thesis is devoted to the study of digital fraud and hidden frauds in companies, as well as methods for detecting such crimes in the computer environment. The main objective of the work is to develop a method of collecting artefacts to investigate crimes and identify intruders, as well as to analyse documents altered or betrayed to third parties, in order to find traces of illegal activities. The thesis includes both theoretical and practical parts. The theoretical section describes the basic concepts of economic activity and forensics, as well as computer forensics and an overview of computer forensics artefacts necessary for investigation. The practical part focuses on the development of a method for collecting artefacts for investigation and detection of offenders and for its use in legal proceedings, as well as the basic procedures used in crime scene investigation to obtain reliable digital evidence and the analysis of artefacts to extract useful information.

Keywords: Economic fraud, economic crime, motivating factors, criminal investigation, forensic science, computer forensics, traditional and digital forensic auditing, artifact collection solutions, artifact detection method, Microsoft Windows operating system

Obsah

1 Úvod 10

2 Cíl práce a metodika 11

2.1 Cíl prace 11

2.2 Metodika 11

3 Teoretická východiska 12

3.1 Hospodářská činnost 12

3.1.1 Zásada zákonnosti 12

3.1.2 Zásada svobody hospodářské činnosti 12

3.1.3 Zásada spravedlivé hospodářské soutěže 14

3.1.4 Zásada integrity subjektů hospodářské činnosti 14

3.1.5 Princip zákazu vědomě kriminálních forem chování 15

3.2 Kriminalistika obecně 15

3.3 Pojem hospodářská kriminalita 16

3.4 Charakteristické rysy hospodářské kriminality 17

3.5 Hlavní faktory, které vedou k páchání hospodářských trestných činů 17

3.6 Pachatel hospodářské kriminality 21

3.7 Kyberkriminalita 22

3.8 Digitální bezpečnost 24

3.9 Klasický a digitální forenzní audit 25

3.10 Přehled forenzní vědy jako vědy vyšetřující počítačovou kriminalitu 26

3.10.1 Oblasti výzkumu forenzní vědy 27

3.10.2 Fáze vyšetřování digitálních incidentů 28

3.10.3 Forenzní metody 29

3.11 Přehled počítačové kriminalistiky jako oboru forenzní vědy 30

3.11.1 Základní vyšetřovací techniky 30
3.11.2 Přehled počítačových forenzních artefaktů potřebných pro vyšetřování 31
3.11.3 Přezkoumání a analýza artefaktů 31

4 Vlastní práce 37

4.1 Metoda pro detekci artefaktů 37
4.1.1 První fáze: Modelování incidentu a vytváření hypotézy 37
4.1.2 Druhá fáze: Vývoj souboru opatření pro sběr artefaktů v počítačové kriminalistice 38
4.1.3 Třetí fáze: Sběr artefaktů 40
4.1.4 Čtvrtá fáze: Analýza získaných informací 53
4.1.5 Pátá fáze: Shrnutí a závěr 55

5 Výsledky a diskuse 56

5.1 Výsledky a diskuse o použití vyvinuté metody 56
5.2 Výsledky vypracovaného souboru opatření před zahájením sběru artefaktů 56

6 Závěr 58

7 Bibliografie 59

8 Seznam obrázků a tabulek 64

8.1 Seznam obrázků 64
8.2 Seznam tabulek 65

1 Úvod

V dnešním světě hrají digitální informace hlavní roli. Každá společnost ukládá svá nejdůležitější a nejcennější data do elektronických zařízení a doufá, že je uchová v bezpečí. Bohužel v dnešní době každá společnost, bez ohledu na míru svého zapojení do informačních technologií, čelí reálné hrozbě neoprávněného přístupu k jejím informacím ze strany osob porušujících zákon. Manipulace s těmito informacemi, zejména v ekonomické sféře, může být kritická. Zneužití těchto údajů může v případě špatně navržených procesů zabezpečení informací poškodit jak malé podniky, tak velké korporace.

Tato jednání mohou sahat od manipulace s výkazy o výsledcích hospodaření až po šíření důvěrných informací. Význam těchto údajů je často kritický a jejich neoprávněné použití může vést nejen ke značným finančním ztrátám, ale také k poškození dobrého jména společnosti.

Metody neoprávněného přístupu k digitálním datům se v dnešní době používají poměrně často a není vzácné, že útočníci dosáhnou svého cíle. Proto má každá větší společnost oddělení specializované na vyšetřování digitální kriminality. Pro úspěšné vyšetřování kybernetické kriminality je nutné shromáždit důkazy. Hlavním typem důkazů jsou v takových případech artefakty, které jsou nezbytné pro trestní stíhání nebo jako důkaz v soudním řízení; jejich včasné shromáždění může zajistit nejen identifikaci pachatele, ale také plnou finanční náhradu škody způsobené společnosti.

Tato bakalářská práce se věnuje aplikaci moderních technik a přístupů k forenznímu sběru a analýze digitálních artefaktů, jakož i praktickému využití nástrojů při sběru nejrůznějších artefaktů z osobních počítačů s operačním systémem Windows 10. Techniky počítačové forenziky představené v této práci pomohou identifikovat osoby porušující zákon a odhalit dokumenty, které byly pozměněny nebo sdíleny s třetími stranami za účelem manipulace s finančními výkazy nebo důvěrnými informacemi.

2 Cíl práce a metodika

2.1 Cíl prace

Hlavním cílem bakalářské práce je navrhnout postup pro detekci artefaktů v operačním systému Microsoft Windows.

Dílčím cílem je analyzovat artefakty počítačové forenziky v operačním systému Microsoft Windows za účelem získání užitečných informací pro odhalování ekonomických podvodů ve společnostech.

2.2 Metodika

Teoretická část práce se zabývá hospodářskou kriminalitou v IT na základě studia odborné a vědecké literatury. Byly analyzovány druhy hospodářské kriminality, motivační faktory vedoucí k hospodářské kriminalitě a podvodům, a také byl zdůrazněn význam klasického a digitálního forenzního auditu při vyšetřování trestných činů. Dále byly zpracovány přehledy forenziky jako vědy zabývající se vyšetřováním kyberkriminality a počítačové kriminalistiky jako oboru forenzní vědy. V rámci toho byly rozebrány oblasti, fáze vyšetřování, forenzní metody, základní vyšetřovací techniky, artefakty a existující řešení pro jejich sběr v IT.

V praktické části práce byla navržena vhodná metoda pro sběr artefaktů v operačním systému Microsoft Windows. Metoda obsahovala popis způsobů sbíraní a analýzy různých artefaktů.

Za účelem dosažení uvedeného cíle byl v praktické části práce modelován případ podvodné činnosti ve fiktivní společnosti. Tento incident sloužil jako základ pro vývoj a aplikaci metody zaměřené na vyhledávání a sběr digitálních artefaktů v operačním systému Microsoft Windows.

3 Teoretická východiska

3.1 Hospodářská činnost

V moderním slova smyslu ekonomika (z řeckého oikos – dům, ekonomika a nomos – pravidlo, zákon; v souhrnu – pravidla hospodaření) - je hospodářská činnost, soubor prostředků, předmětů, procesů, které lidé používají k zajišťovaní života, uspokojovaní potřeb vytvářením potřebných statků, podmínek a prostředků k obživě s využitím práce (BERTOVSKIJJ, 2016).

Ekonomická činnost je založena na souboru zásad pro její realizaci. Patří mezi ně: zásada zákonnosti; zásada svobody hospodářské činnosti; zásada spravedlivé hospodářské soutěže; zásada integrity subjektů hospodářské činnosti; princip zákazu vědomě kriminálních forem chování (BERTOVSKIJJ, 2016).

Zásady hospodářské činnosti jsou základní řídící normy, jejichž cílem je zajistit zákonnost a spravedlnost v tržních vztazích. Slouží jako vodítko pro účastníky hospodářského systému a tvoří základ, na němž je postaveno udržitelné a efektivní fungování ekonomiky. Tyto zásady hrají klíčovou roli při regulaci interakcí mezi účastníky trhu a přispívají k vytváření spravedlivých podmínek pro hospodářský růst a rozvoj (BERTOVSKIJJ, 2016).

3.1.1 Zásada zákonnosti

Zásada uskutečňování hospodářské činnosti na zákonných základech znamená, že tato činnost je vykonávána v souladu s právními předpisy různých právních odvětví, neodporuje jí. Hospodářská činnost ze zákona, je-li prováděna v souladu s ustanoveními hospodářského, občanského, daňového, celního, finančního a jiných odvětví práva (BERTOVSKIJJ, 2016).

3.1.2 Zásada svobody hospodářské činnosti

Ekonomická svoboda je právo na ekonomické sebeurčení jednotlivce, možnost zlepšit si život vlastním jednáním. V užším slova smyslu jde o svobodu podnikání; v širokém smyslu je to také svoboda profesní, spotřebitelské, majetkové, finanční volby (MIROSHINA, 2016).

Každý jedinec má právo rozhodovat svobodně o svém zaměstnání a přípravě na něj, a také právo podnikat a provozovat jinou ekonomickou činnost. Každý má také právo využívat své schopnosti a majetek pro podnikání a další ekonomické aktivity, pokud to není zakázáno zákonem (PŘEDSEDNICTVO ČESKÉ NÁRODNÍ RADY, 1992).

Ekonomická svoboda je založena na třech hlavních principech volného trhu: svoboda podnikání, svoboda volby a svoboda obchodu (NEMCHENKO, 2016).

V dnešní době by měl být koncept „ekonomické svobody“ více rozšířen (NEMCHENKO, 2016):

- Možnost pro podnikatelské subjekty zvolit si formy vlastnictví a rozsah využití svých schopností, znalostí, příležitostí, zaměstnání, způsobů rozdělování příjmů a spotřeby hmotných statků. Ekonomická svoboda je uplatňována na základě právních norem státu a je neoddělitelná od ekonomické odpovědnosti občanů;
- Svoboda ekonomických subjektů (podnikatelských subjektů) vlastnit různé věci, volit oblasti využití svých znalostí a schopností v rámci různých typů majetku a organizačně-právních forem podnikání, a také způsoby získávání zdrojů, distribuce příjmů a spotřeby zboží;
- Právo jednotlivce svobodně nakládat se svým majetkem, příjmy, časem a úsilím;
- Svoboda provádět jakoukoli činnost, včetně práva volby a přijetí spojených rizik a odpovědností.

Ekonomická svoboda v tržní ekonomice je základní podmínkou spravedlivé distribuce zboží a důvěry občanů ve vládní instituce. Posloupnost utváření stabilních, transparentních a chráněných mechanismů, které zajišťují realizaci práv a svobod ekonomické činnosti, vytváří veřejné blaho “ekonomické svobody” jako imperativ optimalizace rovnováhy zájmů (NEMCHENKO, 2016).

Ekonomická svoboda je jednou z nejdůležitějších podmínek fungování ekonomiky v moderním světě. Podnikatelské subjekty by měly mít na výběr rozsah činností, prostředky k dosažení cíle, způsoby prodeje výrobků (NEMCHENKO, 2016).

O ekonomické svobodě lze hovořit jak na úrovni světa jako celku, tak na úrovni jednotlivých zemí. Stávající index ekonomické svobody je schopen posoudit, jak svobodná je ekonomika konkrétního státu. Od roku 1995 Heritage Foundation Research Institute (USA) každoročně vypočítává index ekonomické svobody zemí světa.

Odborníci z této nadace definují ekonomickou svobodu jako “neexistenci vládních zásahů nebo překážek ve výrobě, distribuci a spotřebě zboží a služeb, s výjimkou ochrany a podpory svobody samotné nezbytné pro občany.” (BERTOVSKIJJ, 2016)

Úroveň rozvoje státu do značné míry závisí na stupni rozvoje ekonomické svobody. Musíme si ale pamatovat, že svoboda nemůže být absolutní, je omezena svobodou ostatních. Ekonomické subjekty proto musí při výběru zohledňovat zájmy ostatních účastníků ekonomické činnosti. Ekonomická svoboda je omezena nejen svobodou druhých, ale i právními normami a normami lidského chování ve společnosti, které jsou státem stanoveny pro zákonné a důsledné fungování ekonomiky v zemi (BERTOVSKIJJ, 2016).

3.1.3 Zásada spravedlivé hospodářské soutěže

Zásada spravedlivé hospodářské soutěže je klíčovým konceptem v oblasti ekonomie a práva, který se týká regulace trhu a zachování spravedlivého prostředí pro podniky a spotřebitele. Tato zásada je založena na předpokladu, že zdravá hospodářská soutěž je prospěšná pro ekonomiku a společnost jako celek (BERTOVSKIJJ, 2016).

3.1.4 Zásada integrity subjektů hospodářské činnosti

Zásada integrity subjektů hospodářské činnosti se definuje jako etický princip a hodnota, která vyžaduje, aby jednotlivci, organizace a firmy jednali s upřímností, čestností a morálním závazkem ve všech svých obchodních a hospodářských aktivitách. Tato zásada zahrnuje dodržování etických norem, morálních zásad a pravidel, která jsou v souladu s obecnými hodnotami spravedlnosti, rovnosti a dobrého občanství. Hlavními prvky zásady integrity subjektů hospodářské činnosti jsou (BERTOVSKIJJ, 2016):

- Upřímnost a čestnost;
- Dodržování etických norem;
- Ochrana zájmů zákazníků a spotřebitelů;
- Zodpovědnost za jednání;
- Respektování lidských práv;
- Dodržování právních předpisů.

3.1.5 Princip zákazu vědomě kriminálních forem chování

Zákaz záměrně kriminálních forem chování při realizaci ekonomické činnosti jako jeho zásada znamená, že ekonomické subjekty se za žádných okolností nemohou dopouštět jednání, které mají zjevně trestný charakter. Trestné formy chování (činnosti) jsou prostě nepřijatelné, i když mohou přinášet nejvyšší zisk subjektu. Zákaz forenzních forem chování v hospodářské činnosti je totiž projevem principu legality hospodářské činnosti (BERTOVSKIJJ, 2016).

3.2 Kriminalistika obecně

Tato část práce se zaměřuje na diskusi o hospodářské kriminalitě. Pro přesnější definici "hospodářské kriminality", na kterou se zaměříme v následující kapitole, je klíčové porozumět obecnému významu slova "kriminalita". Kriminalistika, jako relativně mladá vědecká disciplína, se potýká s mnoha různými definicemi, žádná z nich však není univerzálně přijímána. U mnoha autorů kriminalistických publikací nenajdeme přesnou definici slova kriminalistika. JUDr. Milan Vichlenda zdůrazňuje, že při snaze o vyčerpávající definici kriminalistiky existuje riziko ztráty jasnosti a stručnosti definice (VICHLENDA, 2011).

Ve svém díle z roku 1898 zakladatel kriminalistiky Hans Gross definuje kriminalistiku jako vědu o reáliích trestního práva. Nicméně, téma kriminalistiky je rozsáhlé, a jedna definice nemůže pokrýt všechny aspekty této vědní disciplíny. Různorodost trestných činů přináší různorodé stopy (GROSS, 2017).

Novější definice se často snaží o obšírnější vymezení, zahrnující obecné pojmové znaky považované za klíčové pro odlišení kriminalistiky od jiných oborů. Musil upozorňuje, že v publicistice či populárně-naučné literatuře se termín "kriminalistika" často používá nepřesně a zaměňuje se s označeními příbuzných oborů, jako je kriminalistika, nauka o policii nebo nauka o trestním právu. Musil však ve své knize definuje pojem kriminalistika následujícím způsobem: „Kriminalistika je samostatný vědní obor sloužící ochraně občanů a státu před trestnými činy tím, že objasňuje zákonitosti vzniku, trvání a zániku stop a zákonitosti vyhledávání, shromažďování a zkoumání stop a tím, že vypracovává podle potřeb trestního zákona a trestního řádu metody, postupy, prostředky a operace v zájmu úspěšného odhalování, vyšetřování a předcházení trestné činnosti.“ (MUSIL, 2004)

Podle JUDr. Milana Vichlendy je kriminalistika samostatným vědním oborem sloužícím ochraně občanů a státu před trestnými činy. Tento obor se zabývá objasňováním zákonitostí vzniku, vyhledáváním, zajišťováním, zkoumáním a využíváním stop a dalších kriminalisticky relevantních skutečností. Tím vytváří metody, postupy, prostředky a operace pro úspěšné odhalování, vyšetřování a předcházení trestné činnosti (VICHLENDA, 2011).

V souvislosti s definicí kriminalistiky je klíčové určit, které jevy objektivní reality jsou touto disciplínou zkoumány. Musil rozlišuje tři hlavní skupiny objektů zkoumaných kriminalistikou (MUSIL, 2004):

1. skutek trestního činu a osoba pachatele;
2. stopy trestního činu a nositelé stop;
3. činnost policie, orgánů činných v trestním řízení, znalců při odhalování a vyšetřovaní trestných činů a při zkoumání stop.

3.3 Pojem hospodářská kriminalita

Policie České republiky definuje "hospodářskou kriminalitu" jako formu trestné činnosti bez použití násilí, která má výrazný společenský a ekonomický dopad, zasahuje do vnitřní stability státu a narušuje jeho vnitřní funkce, přičemž je v rozporu s platným právním řádem. Tato forma kriminality se projevuje komplexními občanskoprávními, hospodářsko-právními a trestněprávními aspekty, a její řešení vyžaduje zvláštní odborné znalosti, které musí být neustále aktualizovány jak mezi zaměstnanci příslušných orgánů státní správy, tak i mezi pracovníky kriminální policie. Tato forma kriminality vyžaduje zvláštní péči a odborný přístup při vyšetřování a potírání, a to včetně neustálého zdokonalování znalostí v daném oboru (POLICIE ČR, 2023).

Pojem hospodářská kriminalita zahrnuje široké spektrum trestných činů, včetně daňových podvodů, účetních machinací, padělání peněz a platebních karet, korupce, legalizace příjmů z trestné činnosti, trestné činy související s úpadkem, porušování veřejné soutěže, trestné činy v oblasti životního prostředí a porušování autorských a průmyslových práv. Mezi majetkové trestné činy patří například tunelování bank, různé formy krádeží a podvody. S rozvojem technologií se stává stále důležitějším boj proti počítačové kriminalitě (POLICIE ČR, 2023).

Tato trestná činnost má charakter organizovaného zločinu s mezinárodními prvky a výraznou latentností. Europol, se sídlem v Haagu, přispívá k prevenci a boji proti této formě kriminality. Europol hraje klíčovou roli v boji proti počítačové kriminalistice a je v této oblasti důležitým orgánem. Tato organizace spolupracuje s členy Evropské unie a dalšími zeměmi na prevenci a potlačování počítačové a internetové kriminality. Europol definuje hospodářskou kriminalitu, též nazývanou finanční kriminalitou, jako nezákonné činy, které se páchají s cílem získat finanční nebo profesní výhody. Klíčovým motivem těchto trestných činů je dosažení ekonomického zisku (EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION, 2022).

3.4 Charakteristické rysy hospodářské kriminality

Hospodářská kriminalita je druhem kriminality, která se týká nelegálních činností, které mají ekonomický motiv. Tato forma kriminality zahrnuje různé nelegální aktivity, které mají ekonomický motiv a mohou způsobit škody na ekonomice, firmám, investorům a společnosti jako celku. Hospodářská kriminalita může být prováděna jednotlivci, organizacemi nebo dokonce vládními úřady (PAYNE, 2016).

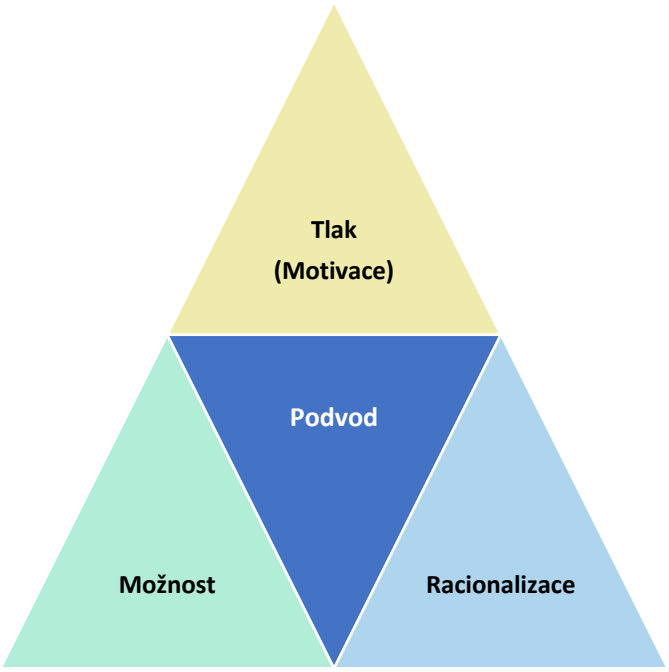
Hospodářská kriminalita může mít různé charakteristické rysy. Samozřejmě hlavním a zřejmým rysem je ekonomický zisk. Hospodářská kriminalita je obvykle motivována finančním ziskem. Pachatelé se snaží získat peníze nebo jiné ekonomické výhody prostřednictvím nelegálních činností, jako jsou podvody, krádeže, úpisy atd (PAYNE, 2016).

Jako každé protiprávní jednání má i hospodářská kriminalita skrytý a manipulativní charakter. Tato činnost často zahrnuje sofistikované metody a triky na skrytí pachatelství a manipulaci s finančními záznamy nebo transakcemi, aby se uniklo odhalení (PAYNE, 2016).

3.5 Hlavní faktory, které vedou k páchání hospodářských trestných činů

Spáchání ekonomických zločinů je mnohostranný a rozmanitý jev, který je podmíněn různými faktory a motivy. Pro zodpovězení otázky "Proč lidé páchají trestnou činnost?" byla zkoumána teorie "Trojúhelník podvodu". Trojúhelník podvodu, vyvinutý Donaldem Cresseyem v roce 1953, je model, který vysvětluje faktory, které vedou člověka k profesionálnímu podvodu. Skládá se ze tří komponent, které dohromady vedou

k nelegálnímu chování a porušování práva. Trojúhelník podvodu je základ používaný k vysvětlení důvodů, proč se člověk rozhodne spáchat podvod. Trojúhelník podvodu se skládá ze tří komponent: Tlak (Motivace), Možnost a Racionalizace (EMBROKER, 2023).



Obrázek 1 Schéma trojúhelníku podvodu

Zdroj: Albrecht a kol., Fraud Examination Fourth Edition, 2012

Prvek tlaku

Podvod může být spáchán za účelem získání výhody pro sebe nebo pro organizaci. Podvody ze strany zaměstnanců, kdy jedinec kradl od svého zaměstnavatele, obvykle přinášejí prospěch pachatelovi. Podvody ze strany vedení, kdy osoby ve vedení organizace klamaly investory a věřitele manipulací s finančními zprávami, jsou často prováděny ve prospěch organizace a jejích vedoucích pracovníků. V této sekci budou uvedeny tři hlavní skupiny tlakových faktorů, které motivují lidi k podvodu (ALBRECHT, 2012):

- Finanční tlak

Finanční tlak je nejběžnějším typem tlaku přispívajícího k podvodu. Studie ukazují, že většina všech podvodů souvisí buď s finančním tlakem, nebo s tlakem spojeným s lidskými slabostmi. Mnozí lidé spáchají podvody, protože jsou chudí, jiní necítí uspokojení z toho, co mají, a usilují o luxusní život prostřednictvím podvodu a krádeže.

Běžné finanční tlaky zahrnují: lakomost, život nad poměry, vysoké účty k úhradě nebo dluhy, špatná úvěrová historie, osobní finanční ztráty nebo neočekávané finanční potřeby (ALBRECHT, 2012).

- Tlak spojený s lidskými slabostmi

S finančním tlakem úzce souvisí motivy vyplývající ze slabostí, jako jsou hazardní hry, drogy, alkohol a podobně. Tyto slabosti jsou nejhorší formou tlaku vedoucího k podvodu (ALBRECHT, 2012).

- Pracovní tlak

Ačkoli finanční tlak a lidské slabosti motivují většinu podvodů, někteří spáchají podvody jako pomstu svému nadřízenému nebo jiným lidem. Faktory jako nedostatečné uznání pracovních výsledků, pocit neuspokojení z práce, strach o ztrátu zaměstnání, zvýšený zájem o kariéru, pocit nedostatečného placení nebo touha obejít systém, všechny tyto uvedené faktory mohou být důvodem motivace k extrémním nelegálním opatřením (ALBRECHT, 2012).

Prvek možnosti

Možnost spáchat podvod, skrýt ho nebo uniknout trestu je druhým prvkem trojúhelníku podvodu. V trojúhelníku podvodu je to jediný prvek, nad kterým má firma úplnou kontrolu. V této části jsou uvedeny šest hlavních faktorů, které zvyšují možnost jednotlivců spáchat nelegální činnost uvnitř organizace. Následující seznam faktorů není vyčerpávající, ale představuje dostatečné množství parametrů k ilustraci role prvku možnosti v trojúhelníku podvodu (ALBRECHT, 2012).

- Nedostatek kontrolních opatření, která by zabránila a/nebo odhalila podvodné aktivity

Existence efektivního systému kontroly je pravděpodobně nejdůležitějším krokem, který může organizace podniknout k zabránění a odhalení případů podvodu ze strany zaměstnanců (ALBRECHT, 2012).

- Nemožnost posoudit kvalitu práce

Existují práce, jejichž kvalitu je obtížné určit, ale kvalitu určitých typů práce je poměrně snadné určit, stačí se ujistit, zda tato práce odpovídá očekávané kvalitě a smlouvě nebo ne. Nicméně kvalitu jiných prací, jako jsou právníci, psychologové,

automechanici, je často obtížné určit. Takže většina lidí se setkává s tím, že jsou podvedeni, manipulováni se svými problémy a pocity (ALBRECHT, 2012).

- Neschopnost disciplinovat osoby, které spáchaly podvod

Osoba, která spáchala podvod, ale nebyla potrestána nebo jen propuštěna, neponese významné tresty a často obnoví podvodné chování (ALBRECHT, 2012).

- Nedostatek přístupu k informacím

Mnoho podvodů se podaří spáchat, protože oběti nemají přístup k informacím, které mají zločinci. To je obzvláště typické pro mnoho velkých podvodů v oblasti správy, které byly spáchány vůči akcionářům, investorům a držitelům dluhů (ALBRECHT, 2012).

- Neznalost, apatie a neschopnost

Starší lidé, lidé s řečovými vadami a další "zranitelní" občané často padají za oběti podvodníků, protože nemají možnost nebo znalosti, jak odhalit jejich nelegální činy. Různé formy spotřebitelských podvodů, jako jsou bankovní podvody, pyramidové schéma, internetové podvody, telefonní podvody, telemarketingové podvody – jsou to trestné činy přesvědčení, které se snaží donutit oběti neuvědoměle investovat peníze (ALBRECHT, 2012).

- Nedostatek auditorské kontroly

Organizace vynakládají veškeré úsilí na vytvoření dokumentů, které zajišťují auditorský stopu, aby bylo možné obnovení a porozumění operacím. Nicméně mnoho podvodů souvisí s hotovostními platbami nebo manipulacemi s dokumenty, které nelze vystopovat. Chytří podvodníci chápou, že jejich intriky musí být skryty. Také vědí, že tato skrytá manipulace obvykle zahrnuje manipulaci s finančními výkazy (ALBRECHT, 2012).

Prvek racionalizace

Byly již zváženy první dva prvky trojúhelníku podvodu: prvek tlaku a prvek možnosti. Třetím prvkem je racionalizace. Téměř každý podvod zahrnuje prvek racionalizace. Zločinci musí nějakým způsobem racionalizovat nečestnost svých činů. Mezi běžné způsoby racionalizace používané zločinci patří následující (ALBRECHT, 2012):

- *„Organizace mi to dluží.“*
- *„Pouze jsem si půjčil peníze a vrátím je.“*
- *„Nikdo nebude poškozen.“*
- *„Zasloužím si víc.“*
- *„Je to pro dobrý účel.“*
- *„Něco bude muset být obětováno – buď mou ctí nebo reputací.“*

3.6 Pachatel hospodářské kriminality

Hospodářský pachatel je osoba, která se dopustila hospodářské trestné činnosti. Hospodářským pachatelem může být kdokoli, od zaměstnance až po ředitele společnosti. Z kriminalistického hlediska nelze říci, že by existoval specifický nebo univerzální typ osoby, která je schopna spáchat hospodářskou trestnou činnost. Spíše lze říci, že k páchání hospodářské trestné činnosti tlačí člověka určité okolnosti; například každý poctivý a zákonů dbalý občan může pod tlakem problémů v osobním životě ukrást v obchodě nějakou věc. Také každý poctivý člověk se může pod tlakem dopustit peněžního podvodu. Jedinec, který páchá hospodářskou trestnou činnost, se od běžného pachatele liší tím, že často nemá žádné zjevné známky asociálního chování, nemá narušené sociální vztahy, ale pouze negativní odchylku z hlediska právního vědomí, zejména v souvislosti s ekonomickým systémem a disciplínou. Hlavním motivem osob páchajících hospodářskou trestnou činnost zůstává osobní obohacení nebo jiný materiální prospěch. Podle statistik je většina pachatelů hospodářské trestné činnosti ve věku 30 až 50 let. Je to proto, že v tomto věku mají lidé zpravidla vyšší úroveň vzdělání a zkušeností, což jim dává schopnost páchat složitější hospodářské trestné činy (STRAUS, 2008).

Hospodářští zločinci se často vyznačují následujícími vlastnostmi: vysokou úrovní inteligence, znalostí ekonomických a právních norem, charismatem a schopností manipulovat s ostatními a pocitem beztrestnosti (STRAUS, 2008).

Jiří Straus ve své knize Kriminalistická metodika rozlišuje dva typy hospodářských zločinců (STRAUS, 2008):

1. Profesionální zločinci – osoby, pro které je páchání hospodářské trestné činnosti hlavním nebo významným zdrojem příjmů. Specializují se na páchání různých typů hospodářské trestné činnosti, jako jsou podvody, korupce, nepravdivá prohlášení

atd. Profesionální zločinci mají často vysokou úroveň organizace, znalostí a dovedností v oblasti financí a práva (STRAUS, 2008);

2. Organizované zločinecké skupiny – skupiny osob sdružené za účelem páchání hospodářské trestné činnosti. Obvykle mají složité hierarchické struktury, strategie a taktiky. Členové organizovaných zločineckých skupin se mohou specializovat na různé oblasti, jako je praní špinavých peněz, padělání dokladů, nelegální obchod atd. Tyto skupiny obvykle disponují značnými zdroji a mohou působit na mezinárodní úrovni (STRAUS, 2008).

3.7 Kyberkriminalita

Žijeme v době, kdy je díky novým technologiím možné rychle a snadno přistupovat k informacím z různých zdrojů po celém světě, během pár sekund se spojit s dalšími lidmi, nakupovat online atd. Počítače a připojení k internetu jsou relativně levné a staly se součástí každodenního života mnoha lidí (BRODOWSKI, 2011).

Ale bohužel, rozvoj technologií má své negativní důsledky pro uživatele počítačů a internetu. Vytvoření elektronické výpočetní techniky nejnovějších generací s prakticky neomezenými možnostmi, jejich široké rozšíření v ekonomické, sociální a správní sféře, výskyt značného množství osobních počítačů v každodenním životě byly nejen novým důkazem technologického pokroku, ale také to nevyhnutelně vedlo k negativním důsledkům souvisejícím se zneužíváním počítačů a informačních technologií. Pomocí internetu se také velmi snadno a rychle rozvíjí kyberkriminalita. Kyberkriminalita se také stala součástí každodenního života, i když povědomí o tom často chybí (BABU, 2004).

Zejména vysoce rozvinuté země přikládají velký význam boji proti počítačové kriminalitě. Tento problém se stal relevantním bezpečnostním problémem pro mnoho národů. S kyberkriminalitou se musí vypořádat nejen vláda a legislativa, ale celá populace. Za zmínku také stojí, že kyberkriminalita je dlouhodobě jedním z nejrychleji se rozvíjejících druhů trestné činnosti v České republice i ve světě. S více než 18 500 skutky spáchanými v roce 2022 tvořilo přes 10 % z celkového počtu evidovaných trestných činů v ČR. V meziročním srovnání se tato kriminalita zvýšila téměř o 100 % (94,9 %) (BARBOŘÍK, 2023).

Termín "kybernetická kriminalita" dosud nemá pevně vymezenou definici. Podle Organizace pro hospodářskou spolupráci a rozvoj (OECD), která se angažuje v

mezinárodní spolupráci a analyzuje politiky digitální bezpečnosti od počátku 90. let, zahrnuje "jakékoli nezákonné, neetické nebo neuznané jednání související s automatizovaným zpracováním dat a/nebo přenosem dat" (THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 2023).

Rozsah počítačové kriminality zahrnuje širokou škálu činností, které jsou spojeny s počítači a digitálními technologiemi a mají nelegální nebo neetický charakter. Do rozsahu počítačové kriminality spadají tyto činnosti (BROOKS, 2018):

- Hacking – neoprávněný přístup k počítačovým systémům, sítím nebo datům s cílem získat informace, poškodit systém nebo provádět jiné nelegální aktivity;
- Malware – vytváření, šíření a používání škodlivého softwaru, jako jsou viry, trojské koně, ransomware nebo spyware, k poškození nebo ovládnutí cizích počítačů a dat;
- Phishing – falešné e-maily, webové stránky nebo zprávy s cílem získat citlivé informace od uživatelů, jako jsou hesla, bankovní údaje nebo osobní údaje;
- Krádež identity – používání cizích osobních údajů k provádění podvodů nebo získání finančního prospěchu;
- Spamming – masové rozesílání nevyžádaných e-mailů nebo zpráv, často obsahujících podvody nebo nelegální nabídky;
- Kybernetické útoky – útoky na webové stránky, online služby a digitální infrastrukturu s cílem způsobit výpadky nebo poškození;
- Kyberšikanování – zneužívání digitálních prostředků k šikanování a zastrašování jiných osob, například na sociálních sítích;
- Krádež intelektuálního vlastnictví – nelegální kopírování, distribuce nebo užívání chráněných duševních vlastnictví, jako jsou autorská díla nebo patenty;
- Kyberšpionáž – neoprávněné sbírání informací o státních institucích, firmách nebo jednotlivcích za účelem politického, ekonomického nebo vojenského zisku;
- Finanční podvody – využívání počítačových systémů a internetu k provedení různých druhů finančních podvodů;

- Kyberterorismus – používání počítačových technologií k útokům na infrastrukturu nebo k politicky motivovanému terorismu.

3.8 Digitální bezpečnost

Digitální bezpečnost (také nazývaná kybernetická bezpečnost) je oblast, která se zabývá ochranou počítačových systémů, sítí, dat a elektronických zařízení před hrozbami a riziky spojenými s digitálním prostředím. Je to kritický aspekt moderního světa, protože stále více činností, komunikace a transakcí se přesouvá na internet a digitální platformy (STALLINGS, 2017).

V dnešní době kybernetické bezpečnosti je zkratka "CIA" klíčovým prvkem poskytujícím obecný rámec pro pochopení a zabezpečení informačních technologií. Tato zkratka označuje tři základní pilíře kybernetické bezpečnosti: Důvěrnost (Confidentiality), Integrita (Integrity) a Dostupnost (Availability) (MICROSOFT OFFICE, 2023).

Důvěrnost zajišťuje udržení tajemství a omezený přístup k citlivým informacím. Umožňuje identifikovat, jak chránit důležité a soukromé údaje před neoprávněným přístupem. Integrita následně zajistí, že informace zůstanou nedotčeny a nepozměněny, což je klíčové pro zachování spolehlivosti dat a prevenci manipulace nebo úprav. Dostupnost pak zaručuje, že informace jsou k dispozici vždy, když jsou potřeba, což je nezbytné pro nepřetržité fungování systému (MICROSOFT OFFICE, 2023).

Tato zkratka pomáhá organizacím a jednotlivcům identifikovat specifické oblasti rizika ve své kybernetické infrastruktuře. Její význam spočívá v tom, že umožňuje cíleně zaměřit bezpečnostní opatření na klíčové aspekty, což zvyšuje účinnost celkové strategie kybernetické bezpečnosti. Implementace principů "CIA" je klíčovým prvkem pro vytváření odolných a bezpečných systémů v prostředí stále se vyvíjejících hrozeb kybernetického prostoru (MICROSOFT OFFICE, 2023).

Jedním z klíčových prvků digitální bezpečnosti jsou kybernetické hrozby. Kybernetické hrozby jsou různé formy nebezpečí a rizik spojených s digitálním prostředím a počítačovými systémy. Tyto hrozby mohou zahrnovat různé útoky, aktivity a incidenty, které ohrožují kybernetickou bezpečnost jednotlivců, organizací a států (STALLINGS, 2017).

Každá společnost může být ohrožena hackingem. Aby se předešlo případům úniku informací, programovací specialisté vyvíjejí určité systémy a schémata na ochranu firemních dat. Ochrana citlivých a důvěrných dat je jedním z hlavních cílů digitální bezpečnosti. To zahrnuje šifrování, zabezpečení přístupu k datům a zálohování dat. Digitální bezpečnost zahrnuje zabezpečení síťových infrastruktur proti neoprávněnému přístupu a útokům. To zahrnuje firewall, antivirový software, detekci intruzí a další technická opatření. Také ověřování totožnosti uživatelů a zařízení je klíčové pro zajištění bezpečnosti. Toto zahrnuje používání hesel, dvoufaktorové autentizace a biometrického ověřování (STALLINGS, 2017).

3.9 Klasický a digitální forenzní audit

V obecném smyslu je forenzní věda vědní obor, který se zabývá zkoumáním a analýzou hmotných i nehmotných důkazů za účelem zjištění skutečností, zjištění pravdy a pomoci při vyšetřování trestných činů nebo jiných událostí a při řešení sporů. Kriminalisté při vyšetřování shromažďují, uchovávají a analyzují důkazy. Forenzní vědci při vyšetřování shromažďují, uchovávají a analyzují důkazy (RAK, 2013).

Odhalování, zjišťování a dokazování trestných činů zahrnuje specifické charakteristiky, které ovlivňují schopnost získat informace o tom, zda a jak byl trestný čin spáchán. Vzhledem k tomu, že prevence a potírání trestné činnosti často přesahuje možnosti orgánů činných v trestním řízení a daňových orgánů, je pro odhalování podvodů nutná podpora a spolupráce odborníků, včetně účetních (FORENCSIC CERTIFIED PUBLIC ACCOUNTANT, 2018).

Klasický forenzní audit využívá účetní, auditorské a vyšetřovací dovednosti k přezkoumání účetní závěrky podniku. Forenzní auditoři analyzují, interpretují a shrnují složité finanční a obchodní záležitosti. Mohou být najímáni pojišťovnami, bankami, policií, vládními agenturami nebo veřejnými účetními firmami. Forenzní účetní vytvářejí finanční důkazy, vyvíjejí programy pro správu shromážděných údajů a prezentují svá zjištění ve formě zpráv nebo prezentací (FORENCSIC CERTIFIED PUBLIC ACCOUNTANT, 2018).

Forenzní auditoři jsou často svědky v občanskoprávních a trestních řízeních. V této funkci vystupují jako znalci. Nesvědčí o tom, zda byl spáchán podvod. Znalec předkládá důkazy (FORENCSIC CERTIFIED PUBLIC ACCOUNTANT, 2018).

Digitální kriminalistika je soubor činností zahrnující identifikaci a shromažďování, uchovávání, dokazování a znalecké posuzování digitálních důkazů v soudních řízeních týkajících se zneužití interních kontrolních systémů, řešení počítačových incidentů, počítačové a hospodářské kriminality a v občanskoprávních a správních věcech. Tento typ činnosti je také znám jako IT forenzní expertiza. Používání systémů informačních technologií nabízí podnikům možnost snížit náklady a čas, ale také vytváří vysoký potenciál pro zneužití IT (INTERNATIONAL BUSINESS MACHINES, 2022).

Digitální forenzní analýza zahrnuje použití technik informatiky na podporu vyšetřování krádeží, pozměňování nebo ničení dat, podvodů a organizované trestné činnosti. Tento obor lze považovat za účinný doplněk tradičního forenzního vyšetřování a podnikům přináší významné výhody v oblasti informační bezpečnosti (CASEY, 2011).

Proces digitální forenziky zahrnuje všechny fáze vyšetřování podezřelých případů a objasňování trestné činnosti. Zatímco některé trestné činy se odehrávají výhradně ve virtuálním světě informačních technologií, existuje také kategorie trestných činů, které se odehrávají v reálném světě. Proto je důležité kombinovat digitální forenzní analýzu s nedigitální forenzní analýzou, aby bylo zajištěno komplexní vyšetřování (CASEY, 2011).

Experti na počítačovou kriminalistiku jsou obvykle povoláni k prozkoumání počítačů a počítačových sítí za účelem nalezení a uchování důkazů. Provádějí také následující úkoly (CASEY, 2011):

- identifikace pachatelů trestné činnosti nebo jiných nezákonných činností;
- vyhledávání a záchrana dat, dokumentů a elektronické komunikace související s trestními nebo občanskoprávními případy;
- obnova poškozených databází a dokumentů.

Digitální forenzní analýza tedy hraje klíčovou roli při zajišťování bezpečnosti a účinnosti vyšetřování v oblasti informačních technologií (CASEY, 2011).

3.10 Přehled forenzní vědy jako vědy vyšetřující počítačovou kriminalitu

Forenzní (počítačová) věda je aplikovaná věda, která se zabývá kyberkriminalitou. Je to věda, která poskytuje specialistům porozumění tomu, jak správně organizovat odhalování trestného činu, a konkrétněji, jak organizovat proces vyšetřování, kde a jak

shromažďovat informace o trestném činu, jak používat a analyzovat informace o trestném činu, jak identifikovat a uložit užitečná digitální data pro vyšetřování (SAFONOV, 2017).

Charakteristickým rysem této vědy je, že důkazy o kyberzločinu často nejsou materiální, což znamená, že jejich analýzu není schopen provést běžný forenzní specialista, který nemá patřičné znalosti v oblasti informačních technologií. To znamená, že pro vyšetřování kybernetické kriminality je nutné zapojit specialisty z oblasti informační bezpečnosti, kteří budou kompetentní ve sběru a analýze digitálních informací (SAFONOV, 2017).

3.10.1 Oblasti výzkumu forenzní vědy

Počítačová forenzní věda se dělí na mnoho oblastí. V zásadě existuje pět hlavních oblastí (CLOUDIAN, 2023):

Tabulka 1 - Oblasti výzkumu forenzní vědy

Zdroj: https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools

1. Počítačová kriminalistika je obor kriminalistiky, který vyhledává důkazy neboli stop, na lokálních systémech s operačními systémy (Microsoft Windows, Linux);

2. Síťová kriminalistika je obor forenzní vědy, zabývající se především analýzou síťového provozu mezi dvěma informačními systémy;

3. Kriminalistika mobilních zařízení je oblast forenzní vědy, která vyhledává důkazy na chytrých telefonech s operačními systémy Android nebo iOS;

4. Kriminalistická analýza dat je obor forenzní vědy, který se zabývá analýzou souborů, databází, struktur souborů a binárních sekvencí (posloupnosti);

5. Kriminalistika zařízení je obor kriminalistiky, který se zabývá profesionální analýzou technických systémů a hardwaru.

3.10.2 Fáze vyšetřování digitálních incidentů

Bez ohledu na obor studia má forenzní věda speciální systém pro vyšetřování incidentu, který se nazývá fáze forenzního procesu (EADRES, 2021):

Tabulka 2 - Fáze forenzního procesu

Zdroj: https://eadres.ru/blog/--609a5862b46ab.html

1. Sběr informací je první fází šetření, která spočívá v přímém sběru médií obsahujících potřebné údaje a také sběru informací z výše uvedených médií. V této fázi je nesmírně důležité zachovat neměnnost a důvěrnost dat (EADRES, 2021).

Sběr informací uložených elektronicky musí být prováděno tak, aby byla zachována jejich integrita (EADRES, 2021).

2. Analýza – druhá fáze vyšetřování spočívá v systematizaci informací nezbytných pro vyšetřování a jejich analýze, aby se získaly odpovědi na otázky položené specialistovi (EADRES, 2021).

V této fázi vyšetřovatelé analyzují digitální kopie paměťových médií ve sterilním prostředí, aby shromáždili informace pro daný případ. Při tomto procesu se používají různé nástroje, včetně nástrojů pro zkoumání pevných disků a analyzátoru síťového protokolu. Při zkoumání počítače je užitečné použít zařízení pro přepínání myši, které zabrání spánku a ztrátě dat z paměti RAM (Random Access Memory), která se ztratí, když počítač přejde do režimu spánku nebo dojde k výpadku napájení (EADRES, 2021).

3. Výkon je závěrečnou fází šetření, která spočívá v prezentaci výsledků ve formě srozumitelné i laikům (EADRES, 2021).

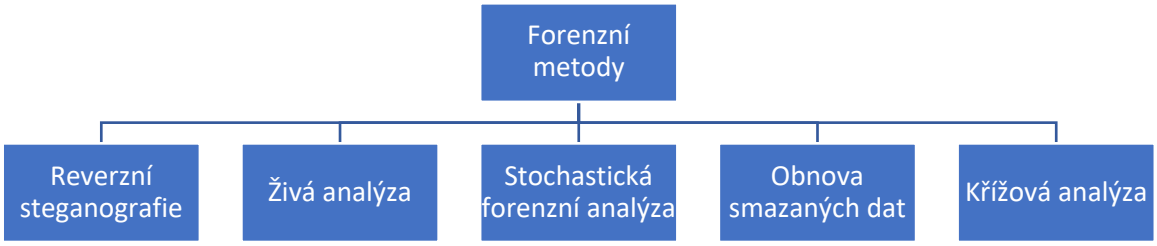
V posledním kroku digitální forenzní experti prezentují svá zjištění během procesu, kde kompetentní osoby použijí poskytnutá zjištění k určení výsledku soudního sporu. V

situaci obnovy dat poskytuje digitální forenzní analýza to, co byla schopna obnovit z kompromitovaného systému (EADRES, 2021).

3.10.3 Forenzní metody

Vyšetřovatelé používají různé metody a forenzní aplikace k prozkoumání kopií zařízení. Prohledávají skryté složky a nepřidělené místo na disku pro kopie odstraněných, zašifrovaných nebo poškozených souborů. Jakýkoli důkaz nalezený na digitální kopii je pečlivě zdokumentován ve zprávě o nálezu a ověřen oproti původnímu zařízení v rámci přípravy na zkoušku zahrnující odhalení, svědectví nebo skutečný soud (EADRES, 2021).

Při provádění počítačové kriminalistiky se využívá kombinace metod a odborných znalostí. V kriminalistice se tedy rozlišují tyto způsoby získávání důkazů (EADRES, 2021):



Tabulka 3 - Forenzní metody

Zdroj: https://eadres.ru/blog/--609a5862b46ab.html

1. Reverzní steganografie je běžná technika používaná ke skrytí dat v jakémkoli typu digitálního souboru, zprávy nebo datového toku. Počítačoví forenzní experti zvrátili pokus o steganografii analýzou hašování dat, která daný soubor obsahuje. Pokud kyberzločinec skrývá citlivé informace uvnitř obrázku nebo jiného digitálního souboru, může to nezkušenému oku vypadat stejně před a po, ale základní hash nebo řetězec dat představující obrázek se změní (EADRES, 2021).

2. Živá analýza – metoda, která se skládá z analýzy zevnitř OS (Operačního Systému), zatímco počítač nebo zařízení běží pomocí systémových nástrojů v počítači. Analýza zkoumá konkrétní data, která jsou často uložena v mezipaměti nebo paměti RAM. Mnoho nástrojů používaných k extrakci konkrétních dat vyžaduje, aby byl počítač

umístěn v kriminální laboratoři, aby byla zachována legitimita řetězce důkazů (EADRES, 2021).

3. Stochastická forenzní analýza je metoda, při které odborníci analyzují a rekonstruují digitální aktivitu bez použití digitálních artefaktů. Artefakty (stopy) jsou neúmyslné změny dat, ke kterým dochází v důsledku digitálních procesů. Artefakty zahrnují důkazy související s digitálním zločinem, jako jsou změny atributů souborů během krádeže dat. Stochastická forenzní technika se často používá při vyšetřování narušení dat, kdy se má za to, že útočník je zasvěcenec, který po sobě nemusí zanechat digitální artefakty (EADRES, 2021).

4. Obnova smazaných souborů je metoda, která spočívá v prohledávání počítačového systému a paměti po fragmentech souborů, které byly částečně odstraněny na jednom místě, ale zanechaly stopy na jiných místech ve stroji. Tato metoda se někdy nazývá file carving nebo data carving (EADRES, 2021).

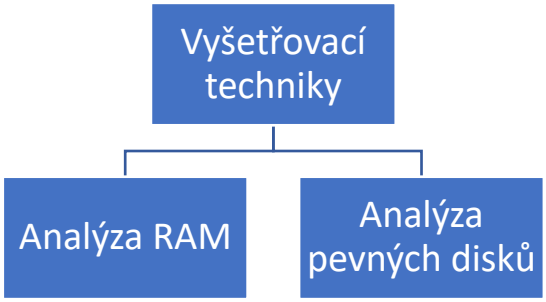
5. Křížová analýza je technika, která zahrnuje porovnávání a vzájemné odkazování informací nalezených na více počítačových discích za účelem vyhledání, analýzy a uložení informací relevantních pro vyšetřování. Podezřelé události se porovnávají s informacemi na jiných jednotkách, aby se hledaly podobnosti a poskytovaly kontext. Tato metoda je také známá jako detekce anomálií (EADRES, 2021).

3.11 Přehled počítačové kriminalistiky jako oboru forenzní vědy

Počítačová kriminalistika je základní a nejrozsáhlejší oblastí kriminalistiky, což je dáno širokým využitím výzkumných objektů, kterými jsou firemní pracoviště napojená na demilitarizovanou zónu, osobní počítače uživatelů atd (EADRES, 2021).

3.11.1 Základní vyšetřovací techniky

V počítačové forenzní vědě existují hlavně dvě vyšetřovací techniky:



Tabulka 4 - Základní vyšetřovací techniky

Zdroj: https://www.atalayar.com/en/articulo/new-technologies-innovation/importance-ram-computer-forensic-analysis/20220124160303154780.html ; https://spy-soft.net/how-to-create-memory-dump-windows/

1. Analýza RAM spočívá v pořízení snímku paměti RAM pro další studium. RAM je často jedním z prvních systémů, kde lze nalézt artefakty související s kybernetickým útokem (GONZÁLEZ, 2022).

2. Analýza pevného disku zahrnuje vytvoření bitové kopie obrazu pevného disku pro další studium (KOZHUKHOV, 2021).

3.11.2 Přehled počítačových forenzních artefaktů potřebných pro vyšetřování

V počítačové kriminalistice se vyšetřování nejčastěji redukuje na hledání artefaktů, tedy na hledání stop průniku do systému. Nalezené informační stopy (artefakty) lze klasifikovat následovně (KOZHUKHOV, 2021):

1. Souborový systém;
2. Systémové protokoly;
3. Systémový registr;
4. Stopy po spuštění programu;
5. Stopy aktivity uživatele.

3.11.3 Přezkoumání a analýza artefaktů

Artefakty souborového systému

Operační systém Microsoft Windows používá souborový systém NTFS, který zase obsahuje artefakty, které potřebujeme (KOZHUKHOV, 2021).

1. $MFT je artefakt, který obsahuje informace o všech souborech a také umožňuje ověřit časová razítka událostí (KASPERSKI, 2020).

2. USN Journal – artefakt, který zaznamenává změny v souborovém systému (vytváření, mazání, úpravy atd.) (COHEN, 2020).

Systémové protokoly

Systémové protokoly jsou soubory se speciální příponou, které zaznamenávají klíčové události, k nimž dochází v operačním systému (EVENT LOG EXPLORER, 2023).

Umístění těchto artefaktů je následující (EVENT LOG EXPLORER, 2023):

1. C:Windows\System32\winevt\Logs;
2. Security (události 4624, 4625, 4648 atd.);
3. Microsoft-Windows-TerminalServices-LocalSessionManager/Operational;
4. Microsoft- Windows- TerminalServices- RemoteConnectionManager/Operational.

Systémový registr

Systémový registr je hierarchicky uspořádané úložiště, obsahující údaje o konfiguraci systému (SHKOLA WINDOWS, 2021).

Umístění artefaktu: C:Windows\System32\config

Konfigurační soubory v systémovém registru jsou pro forenzní specialisty maximálně zajímavé (SHKOLA WINDOWS, 2021):

1. Sam - HKEY_LOCAL_MACHINE\SAM;
2. Security - HKEY_LOCAL_MACHINE\SECURITY;
3. Software - HKEY_LOCAL_MACHINE/SOFTWARE;
4. Systém - HKEY_LOCAL_MACHINE\SYSTEM;
5. C:\Users\<user>\Ntuser.dat - HKEY_USERS\<User SID>;
6. C:\Users\<uživatel>AppData\Local\Microsoft\Windows\Usrclass.dat;
7. HKEY_USERS\<User SID>_Classes.

Stopy spouštění programu

Stopy spouštění programů jsou artefakty, které identifikují interakci mezi uživatelem a konkrétním souborem (KOZHUKHOV, 2021).

Artefakty spuštění programu jsou:

1. Protokoly – soubory se speciální příponou, v nichž jsou zaznamenány klíčové události. Spuštění programu je zvláštním případem takových událostí (ADMIN, 2022);

2. Prefetch – mechanismus systému Windows, jehož cílem je urychlit spouštění programů. Podstata jeho práce spočívá v tom, že kompletně sleduje prvních 10 sekund a ukládá čas posledního spuštění, cestu a soubory, ke kterým program přistupuje. Je třeba poznamenat, že tento mechanismus je na serverech ve výchozím nastavení vypnut. Umístění artefaktu: C:\Windows\Prefetch (ADMIN, 2022);

3. AppCompatCache (známá také jako shimcache) je mechanismus systému Windows, který zajišťuje kompatibilitu nástrojů s jinými verzemi systému Windows. Tento artefakt obsahuje úplný název souboru a datum změny a je uložen v registru, ale aktualizuje se pouze po restartu. Umístění artefaktu: HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\Ap (VIRUSNET, 2019);

4. AmCache je pokročilá verze mechanismu kompatibility ve srovnání s AppCompatCache. Ve srovnání s AppCompatCache. Tento artefakt je uložen v samostatném souboru registru a obsahuje hash: SHA1. Umístění artefaktu: C:\Windows\AppCompat\Programs\Amcache.hve (FORENSICS, 2020);

5. RecentFileCache je stará verze mechanismu Amcache. Tento artefakt je pozoruhodný tím, že obsahuje celé adresáře ke spustitelným souborům. Umístění artefaktu: C:\Windows\AppCompat\ Programs\RecentFileCache.bcf (GITHIB, 2022);

6. SRUM (System Resource Usage Monitor) - artefakt, který zaznamenává spotřebu prostředků aplikacemi. Obsahuje úplné cesty ke spustitelným souborům, čas ukončení aplikace a dobu trvání použití, jakož i množství síťového provozu. Pozoruhodné je, že se objevuje pouze v systému Windows 8. Umístění artefaktu: C:\Windows\System32\sru\SRUDB.dat (COHEN, 2022)

7. RecentlyUsedApplications je artefakt dostupný pro infrastruktury používající SCCM. Tento artefakt obsahuje úplnou cestu ke spustitelnému souboru, čas

posledního spuštění a také zobrazuje uživatele, který aplikaci naposledy spustil. Umístění artefaktu: C:Windows\System32\wbem\Repository (COHEN, 2022).

Sledování aktivit uživatelů

Stopy uživatelské aktivity jsou artefakty, které představují určité typy uživatelských aktivit (KOZHUKHOV, 2021).

Artefakty uživatelské činnosti jsou:

1. Userassist – artefakt vytvořený Průzkumníkem Windows. Obsahuje cesty ke spouštěným spustitelným souborům, zaznamenává některá stisknutá tlačítka v rozhraní Průzkumníka, čas posledního spuštění a čítače spuštění. Umístění artefaktu je: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Us (SUNNYCH, 2018a);

2. MRU (Most Recently Used) - sada artefaktů klíčů registru obsahující některé nedávné aktivity uživatele. Většinou neobsahují jiná časová razítka než to, kdy byl klíč registru naposledy změněn, ale obsahují pořadí, v jakém k němu bylo přistupováno. Umístění artefaktu (MAGNET FORENSICS , 2022):

- \Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs – naposledy otevřené aplikace;

- \Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU – aplikace spuštěné prostřednictvím nabídky „Spustit“;

- \Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU – soubory otevřené nebo uložené prostřednictvím dialogového okna „Otevřít“ nebo „Uložit“.

3. Shellbags – artefakt přistupující k Průzkumníkovi, který ukládá informace o složkách navštívených uživatelem. Informace, které Průzkumník ukládá: o místních složkách, o složkách na externích nebo síťových discích, o mazání složek. Umístění artefaktu (CHANDEL, 2020):

- NTUSER.DAT\Software\Microsoft\Windows\Shell\Software\Microsoft\Windows\ShellNoRoam;

- UsrClass.dat \Local Settings\Software\Microsoft\Windows\Shell **;**

4. JumpLists – artefakt, který uchovává informace o posledních "cílech" otevřených v různých aplikacích (MICROSOFT, 2022):

- Dokumenty;
- Síťová umístění;
- Funkce aplikací.

Umístění artefaktu (MICROSOFT, 2022):

- C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations;
- C:\Users\<uživatel>AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations.

5. Recent – artefakt, který zobrazuje zástupce naposledy otevřených míst, souborů a složek. Je třeba poznamenat, že počet zástupců zapamatovaných systémem je omezený (SUPERUSER, 2023).

Umístění artefaktu (SUPERUSER, 2023): C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent\.

6. Historie prostředí Powershell – artefakt Historie uživatelských vstupů prostředí Powershell. Neobsahuje žádné výsledky příkazů ani časové značky. Je to obdoba bash_history. Umístění artefaktu (MICROSOFT, 2023):

- C:\Users\<user>\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt.

7. Timeline systému Win10 je interní systém pro vytváření artefaktů v systému Windows. Tento systém uchovává informace o činnosti uživatele za jeden měsíc a obsahuje informace o používaných aplikacích, čase, kdy je uživatel začal používat, otevřených dokumentech a odkazech, přičemž vše ukládá do SQLite. Umístění artefaktu (VARGOVA, 2021):

C:\Users\<user>\AppData\Local\ConnectedDevicesPlatform\L.<user>\ActivitiesCache.db

8. Historie prohlížeče – známý artefakt výzkumu historie prohlížeče. Má smysl, pokud existuje podezření, že uživatel mohl otevřít phishingový odkaz nebo něco

stáhnout. Většina moderních prohlížečů ukládá historii ve formátu SQLite a umožňuje také nahlížet do uložené mezipaměti, na data automatického dokončování atd (SUNNYCH, 2018b).

Umístění artefaktu (SUNNYCH, 2018b):

- Firefox: C:\Users\<uživatel>\AppData\Roaming\Mozilla\Firefox\Profiles\<profile>;
- Chrome: C:\Users\<user>AppData\Local\Google\Chrome\User Data\Default.

9. Mail – artefakt, který zahrnuje zkoumání poštovních souborů a používá se v případě podezření na škodlivou poštu (SCULLY, 2021).

Umístění artefaktu (SCULLY, 2021):
C:\Users\<user>\AppData\Local\Microsoft\Outlook

4 Vlastní práce

4.1 Metoda pro detekci artefaktů

4.1.1 První fáze: Modelování incidentu a vytváření hypotézy

Ve společnosti John&Sons zjistilo oddělení interního auditu nesrovnalosti v účetnictví a podezřelé finanční transakce. Vyšetřovatelé hospodářské kriminality rychle zahájili vyšetřování případu. Bylo zahájeno vyšetřování s podezřením na možný hospodářský podvod. Prioritním cílem zájmu se staly finanční údaje, elektronická komunikace a systémové protokoly, protože by mohly obsahovat cenné informace o nezákonných aktivitách ve společnosti.

Hlavní úřad pro hospodářskou bezpečnost a boj proti korupci vydal příkaz k prohlídce kanceláří společnosti John&Sons. Při prohlídce byly zajištěny fyzické dokumenty, USB flash disky a počítače. Bylo zahájeno důkladné prověřování veškeré dokumentace, které vedlo k objevení dokumentu "Finanční zpráva o zvláštním projektu A" podepsaného samotným ředitelem společnosti, který obsahoval důkazy o jeho zapojení do hospodářských podvodů.

Nezvratné důkazy předložené vyšetřovateli vyvolaly popření ze strany ředitele společnosti John&Sons, který tvrdil, že jeho podpis byl zfalšován. Vzhledem k tomu vyšetřovatelé předpokládali možnou účast ředitele a požádali o prošetření incidentu počítačového experta (forenzika).

Úkolem forenzika bylo potvrdit nebo vyvrátit hypotézu vyšetřovatelů a hledat důkazy o zapojení dalších zaměstnanců společnosti. Forenzik začne zkoumat elektronická zařízení s cílem najít dokument se stejným nebo podobným názvem, určit, kdy byl vytvořen, upraven nebo smazán. Důležitým aspektem bude také analýza času, který zaměstnanci s daným dokumentem strávili, a další podrobnosti, které mohou odhalit okolnosti toho, co se stalo.

Všechny názvy společností a osob byly smyšlené, jakákoli shoda se skutečností je náhodná shoda.

4.1.2 Druhá fáze: Vývoj souboru opatření pro sběr artefaktů v počítačové kriminalistice

V této fázi bude vypracován soubor opatření pro sběr artefaktů v počítačové forenzní analýze v operačním systému Microsoft Windows, přesněji řečeno pro proces provádění činností, které předcházejí přímému sběru artefaktů. V této části bude zohledněna nejen technická část opatření, ale také právní část vyšetřování incidentů, která ji upravuje.

V Policejním prezídiu České republiky se taková opatření nazývají kriminalistickotechnická (počítačová) expertíza. Podstata tohoto druhu expertízy spočívá v zodpovězení otázek vyšetřovatele odborníkem příslušného profilu. Účelem tohoto druhu expertízy může být (POŽÁR, 2023):

1. zjištění stavu elektronického počítačového stroje;
2. zjištění role každého konkrétního elektronického technického zařízení při vyšetřování trestného činu;
3. získání dalších důkazů o vyšetřované události (fyzické dokumenty, výpovědi obviněných nebo svědků, otisky prstů atd.);
4. získání přístupu k datům uloženým na elektronických digitálních médiích;
5. analýza a zkoumání specializovaných informací umístěných na elektronických digitálních médiích (sběr artefaktů a jejich analýza).

Soubor opatření pro ohledání místa činu a prohlídku

Prvním krokem je povrchní primární analýza cílového objektu počítačových informací, kterou může provést běžný forenzní specialista.

Druhou krokem je prohlídka. V této fázi musí specialista zdokumentovat všechny informace, které mohou napomoci vyšetřování, a zapečetit všechny možné cílové objekty počítačového forenzního zkoumání podle Zákona č. 141/1961 Sb. (Zákon o trestním řízení soudním (trestní řád)) (PARLAMENT ČESKÉ REPUBLIKY, 1961).

Znalci musí provést úkony s přihlédnutím k následujícím opatřením (RAK, 2013):

- Je nutné zajistit, aby do prostor, kde je instalováno potenciálně užitečné zařízení, měly přístup pouze osoby pověřené šetřením. Pokud to není možné, měla by být

zaznamenána pozice zařízení a zdokumentovány všechny činnosti, které byly s tímto zařízením provedeny;

- V této fázi v žádném případě nezapínejte vypnutá zařízení;
- Předat (prostřednictvím fotografií, videa, podrobné dokumentace) veškeré potenciálně užitečné vybavení pro výzkum, přítomnost všech kabelů a místa jejich připojení. Všechny periferní zařízení by měly být rovněž zachyceny a zdokumentovány;
- V případě, že je zařízení v pracovním stavu, je nutné přenášet to, co je na obrazovce jeho monitoru. Také počítač může být v režimu spánku. V takovém případě lze postupovat podle následujících pokynů: buď zařízení ihned vypnout, nebo počítač uvést ze stavu spánku do pracovního stavu (pohybem myši) a zaznamenat, co se děje na monitoru. Pokud se na monitoru objeví okno, které vyžaduje ověření uživatele, je třeba tuto skutečnost zdokumentovat a zařízení vypnout. Je však třeba mít na paměti, že před vypnutím je nutné uložit operační paměť do dlouhodobé paměti, protože v ní mohou být stopy užitečné pro vyšetřování;
- V blízkosti technických objektů šetření je nutno shromáždit také různé užitečné informace, jako jsou hesla, síťová rozhraní a další užitečné a relevantní informase;
- Je také nutné počítač správně vypnout. To se provádí vytažením napájecího kabelu ze skříně počítače, nikoli ze zásuvky. Vypnutí počítače ze zásuvky může vést k poškození důležitých systémových souborů a selhání operačního systému;
- Všechna zařízení jsou řádně utěsněna tak, aby do nich nebylo možné vniknout. Všechny úkony by měly být vyfotografovány a zdokumentovány;
- Technické prostředky zabavené při prohlídce se pečlivě zabalí, aby nedošlo k jejich poškození;
- Je nutné vyslechnout úřední osoby z místa činu, aby se dozvěděly užitečné údaje o technických zařízeních (hesla, síťová rozhraní, vlastnosti informační infrastruktury).

Soubor opatření pro vyjmutí technických a elektronických zařízení

V této části fáze probíhá vyšetřovací a operativní úkon zvaný vyjmutí. Zajištění zahrnuje odborné odebrání technických a elektronických zařízení za účelem jejich

následného dálkového zkoumání, neboť často není možné analyzovat informace na místě činu. Na základě výše uvedeného jsou tedy v této fázi technicky vyjmuty a následně zajištěny následující prvky: počítačové soubory, pevné disky, flash disky, polovodičové disky (SSD), SIM karty a paměťové karty mobilních zařízení. Při zabavování je třeba vzít v úvahu následující opatření (RAK, 2013):

- Při zabavování technických zařízení by neměly být upravovány, ukládány a měněny veškeré informace, které jsou na nich k dispozici, protože vyšetřovatel má povinnost prokázat, že informace nebyly nijak upravovány, protože pouze takové informace lze použít jako důkazní materiál. To znamená, že informace nesmí být změněny ani během zabavení, ani během jejich bezprostředního uložení;

- Každý úkon provedený technickou jednotkou by měl být zdokumentován, aby v případě potřeby mohl nezávislý odborník při opakovaném provádění stejných úkonů dosáhnout stejného výsledku.

4.1.3 Třetí fáze: Sběr artefaktů

Po povrchní prvotní analýze počítačového informačního objektu a jeho podrobné dokumentaci a po procesu odborného vytěžení technických a elektronických zařízení za účelem následné dálkové kontroly a analýzy přichází fáze sběru digitálních stop a jejich analýzy za účelem získání informací užitečných pro vyšetřování.

Podrobné zkoumání artefaktů, jako jsou digitální stopy, důkazy nebo data, vyžaduje důkladné vyhodnocení technologií a metod používaných k jejich sběru. Cílem této části výzkumu bude identifikovat a analyzovat účinnost různých nástrojů a přístupů používaných v současných postupech sběru dat v kontextu vyšetřování incidentů.

Podle scénáře modelové události se společnost John&Sons dostala do podezření vyšetřovatelů hospodářského a trestního práva ze spáchání podvodu. Byl nalezen dokument naznačující nezákonnou činnost vedoucího této společnosti. Ředitel společnosti zároveň popírá svou účast na nezákonných činnostech. Úkolem forenzního vyšetřovatele je incident prošetřit a poskytnout odpověď na hypotézu.

Nástroje pro sběr a analýzu:

- Aplikace Erica Zimmermana: MFTECmd.exe, PECmd.exe, AppCompatCacheParser.exe, SrumECmd.exe, LECmd.exe, ShellBagsExplorer.exe, WixTCmd.exe;

- Systémové aplikace: wevtutil, RegRipper;

- Aplikace třetích stran: ExtractUsnJrnl64.exe (Copyright 1999-2018 Jonathan Bennit & Autolt), UserAssistView.exe (Copyright 2008-2010 Nir Sofer);

- Asistent pro čtení souborů ve formátu SQLite: https://sqliteonline.com\ ;

- Asistent pro kontrolu odkazů ke stažení a aplikací na přítomnost virů: https://www.virustotal.com/gui/home/upload ;

Všechny aplikace musí být předem staženy a uloženy do adresáře "Downloads". Důležité je také zachovat důslednost při shromažďování digitálních stop.

Sběr artefaktů souborového systému

1. $MFT

K získání tohoto artefaktu souborového systému použijeme nástroj MFTECmd.

MFTECmd je nástroj s otevřeným zdrojovým kódem, který analyzuje, dekóduje a zapisuje informace z hlavní tabulky souborů ($MFT) do souboru vhodným způsobem pro další analýzu.

Ke shromáždění tohoto artefaktu souborového systému použijeme nástroj MFTECmd.exe.

Otevřeme příkazový řádek a provedeme požadovaný příkaz (obrázek 2):

C:\Windows\system32>cd..

C:\Windows>cd..

C:\>cd Users

C:\Users>cd <user>

C:\Users\<user>>cd Downloads

C:\Users\<user>\Downloads>dir

C:\Users\<user>\Downloads>cd MFTECmd

C:\Users\<user>\Downloads\MFTECmd>dir

C:\Users\<user>\Downloads\MFTECmd>MFTECmd.exe

C:\Users\<user>\Downloads\MFTECmd>MFTECmd.exe -f "C:\$MFT" --csv "c:\temp\out" --csvf MyOutputFile.csv

*“-f” – Umístění souboru, se kterým je potřeba pracovat

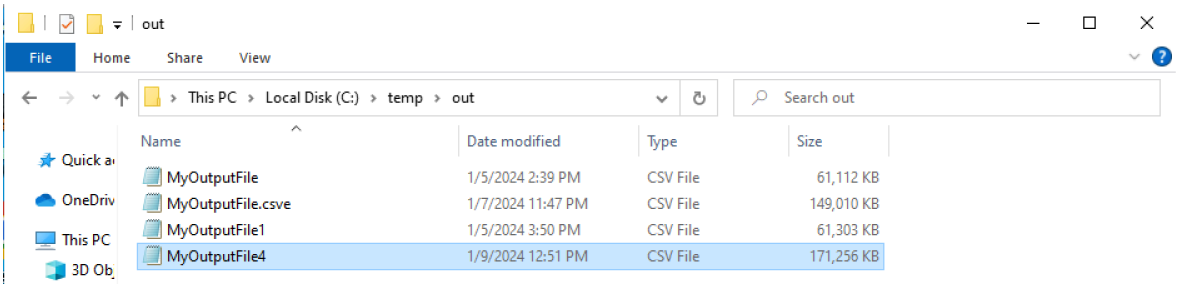
*“--csv” – Adresář pro uložení souboru s artefakty

*“--csvf” – Název souboru s artefakty

Obrázek 2 - Spuštění nástroje MFTECmd z příkazového řádku

Zdroj: Vlastní zpracování

Pomocí příkazového řádku vyjmeme artefakt (obrázek 3):



Obrázek 3 - Výsledek nástroje MFTECmd

Zdroj: Vlastní zpracování

2. USN Journal

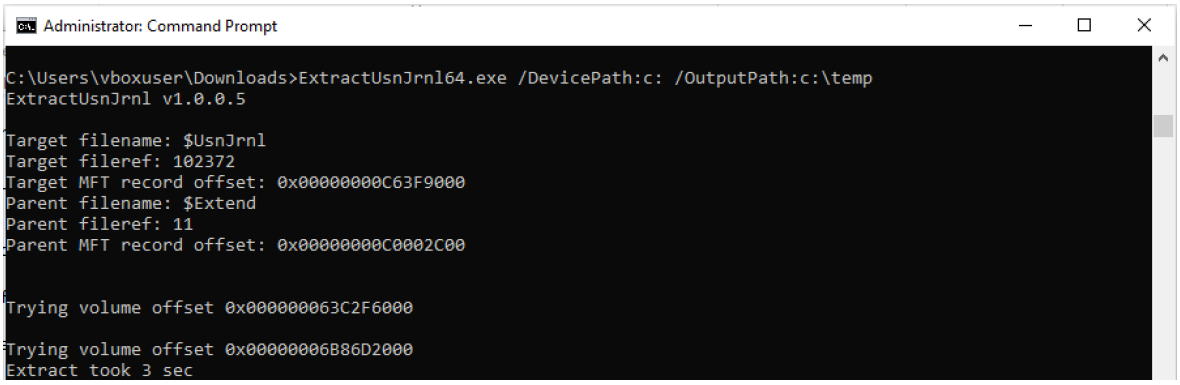
Ke shromáždění tohoto artefaktu souborového systému použijeme nástroj ExtractUsnJrnl64.exe

Otevřeme příkazový řádek a provedeme požadovaný příkaz (obrázek 4):

C:\Users\<user>\Downloads>ExtractUsnJrnl64.exe

C:\Users\<user>\Downloads>ExtractUsnJrnl64.exe /DevicePath:c: /OutputPath:c:\temp

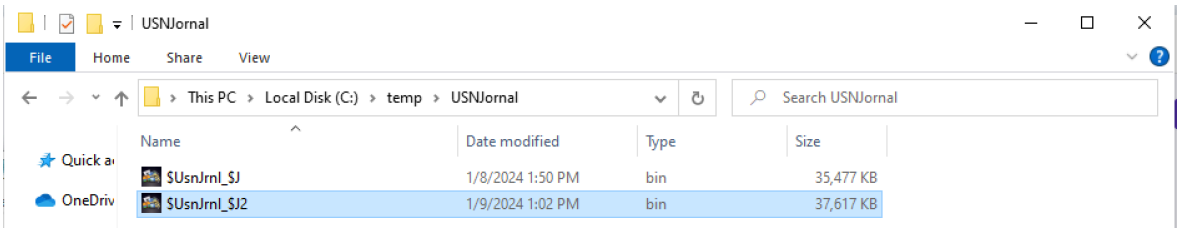
*“temp” – Adresář, do kterého se soubor uloží, lze vybrat jiný existující adresář.



Obrázek 4 - Spuštění příkazu USN Journal v cmd

Zdroj: Vlastní zpracování

Výsledkem je $UsnJrnl_$J2 soubor ve spustitelném adresáři (obrázek 5):



Obrázek 5 - Výsledek nástroje USN Journal

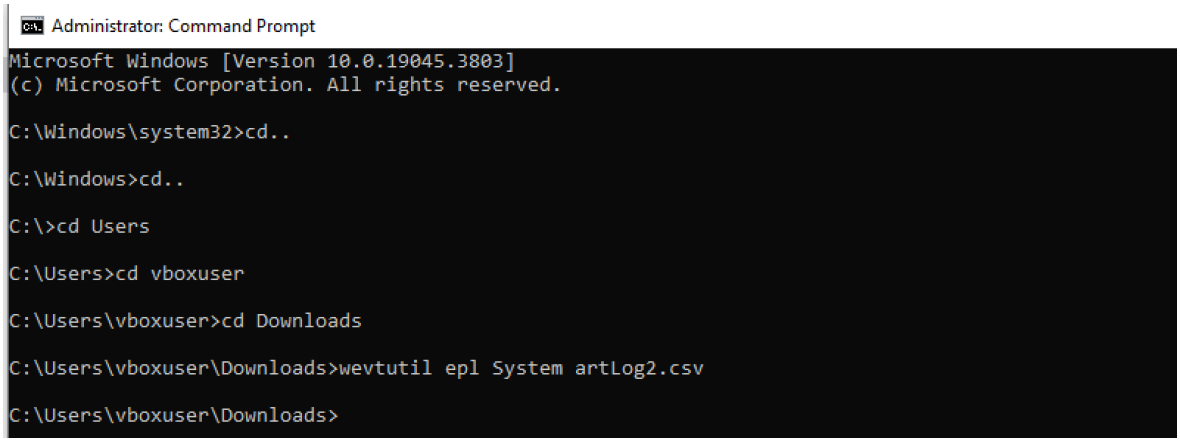
Zdroj: Vlastní zpracování

Systémové protokoly

Pro uložení protokolu událostí pomocí příkazového řádku musíme otevřít příkazový řádek a spustit příkaz nástroje wevtutil (obrázek 6):

C:\Users\<user>\Downloads>wevtutil epl System artLog.csv

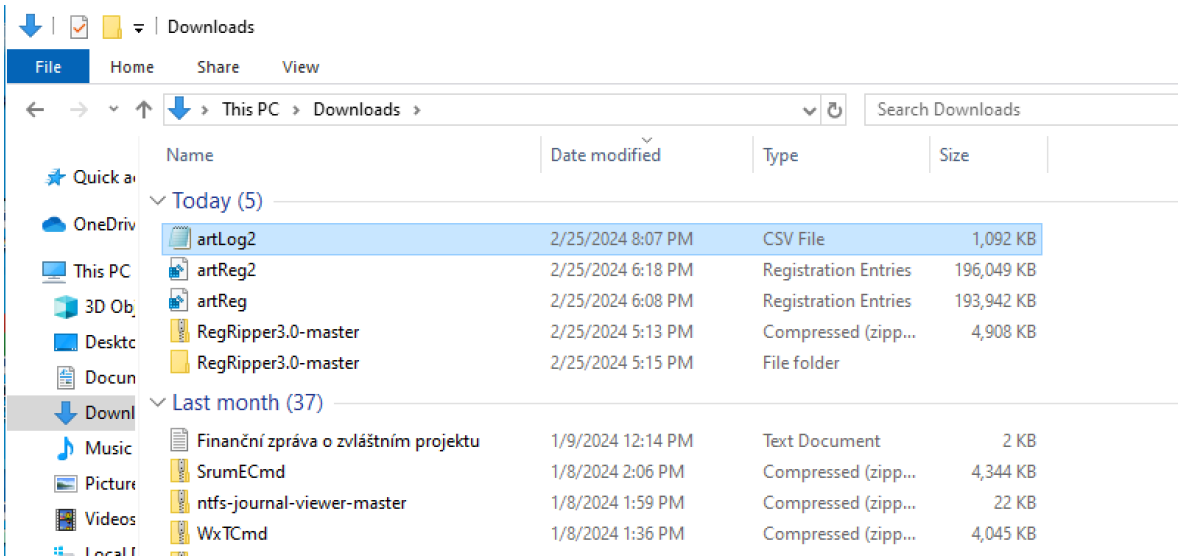
*“artLog.csv” - Název souboru; název lze změnit, přípona “csv” se nemění



Obrázek 6 - Spuštění příkazu wevtutil v cmd

Zdroj: Vlastní zpracování

Výsledkem je CSV soubor ve spustitelném adresáři (obrázek 7):



Obrázek 7 - Výsledek nástroje wevtutil

Zdroj: Vlastní zpracování

Systémový registr

Pro uložení systémového registru pomocí příkazového řádku je třeba otevřít příkazový řádek a spustit příkaz nástroje RegRipper integrovaného v operačním systému (obrázek 8):

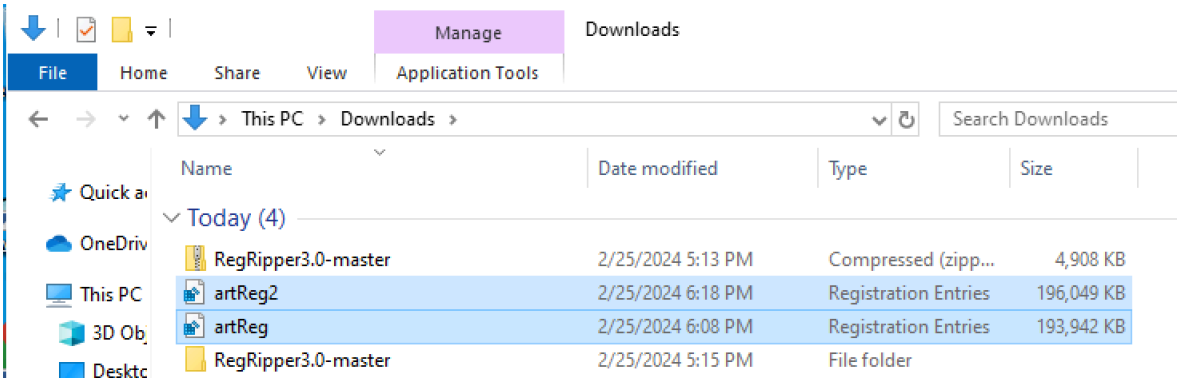
C:\Users\<user>\Downloads>REG EXPORT HKLM\SOFTWARE artReg3.reg

*“ artReg.reg” - Název souboru; název lze změnit, přípona “reg” se nemění

Obrázek 8 - Spuštění příkazu RegRipper v cmd

Zdroj: Vlastní zpracování

Výsledkem je soubor s příponou reg ve spustitelném adresáři (obrázek 9):



Obrázek 9 - Výsledek nástroje RegRipper

Zdroj: Vlastní zpracování

Stopy po spuštění programů

1. Prefetch

K uložení tohoto artefaktu pomocí příkazového řádku je třeba otevřít příkazový řádek a spustit příkaz nástroje PECmd.exe (obrázek 10):

C:\Users\<user>\Downloads>dir

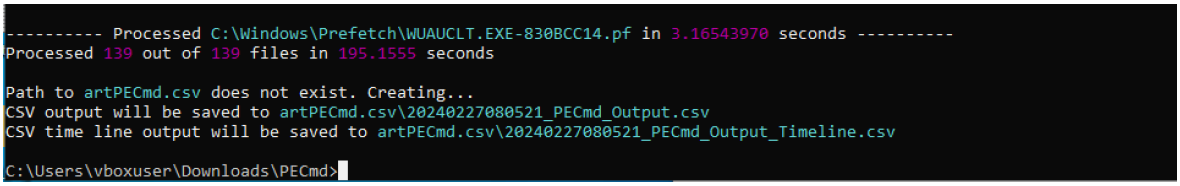
C:\Users\<user>\Downloads>cd PECmd

C:\Users\<user>\Downloads\PECmd>dir

C:\Users\<user>\Downloads\PECmd>PECmd.exe

C:\Users\<user>\Downloads\PECmd>PECmd.exe -d "C:\Windows\Prefetch" --csv "artPECmd.csv"

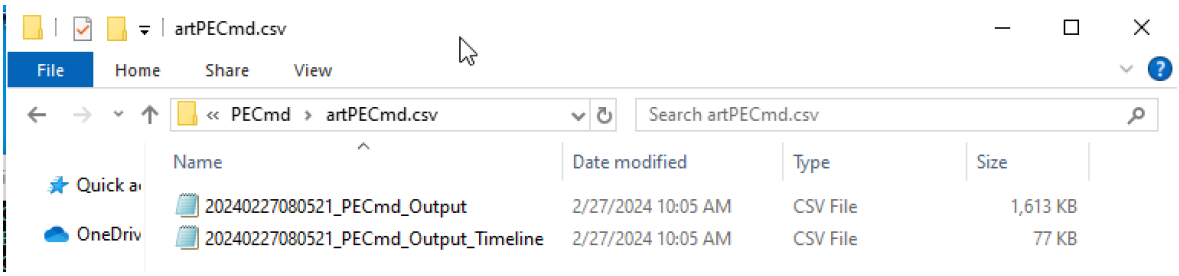
*“-d” – Umístění souboru, se kterým je potřeba pracovat



Obrázek 10 - Spuštění příkazu sběru Prefetch v cmd

Zdroj: Vlastní zpracování

Výsledkem jsou soubory ve spustitelném adresáři (obrázek 11):



Obrázek 11 - Získání dat Prefetch

Zdroj: Vlastní zpracování

2. AppCompatCache

K uložení tohoto artefaktu pomocí příkazového řádku je třeba otevřít příkazový řádek a spustit příkaz nástroje AppCompatCacheParser.exe (obrázek 12):

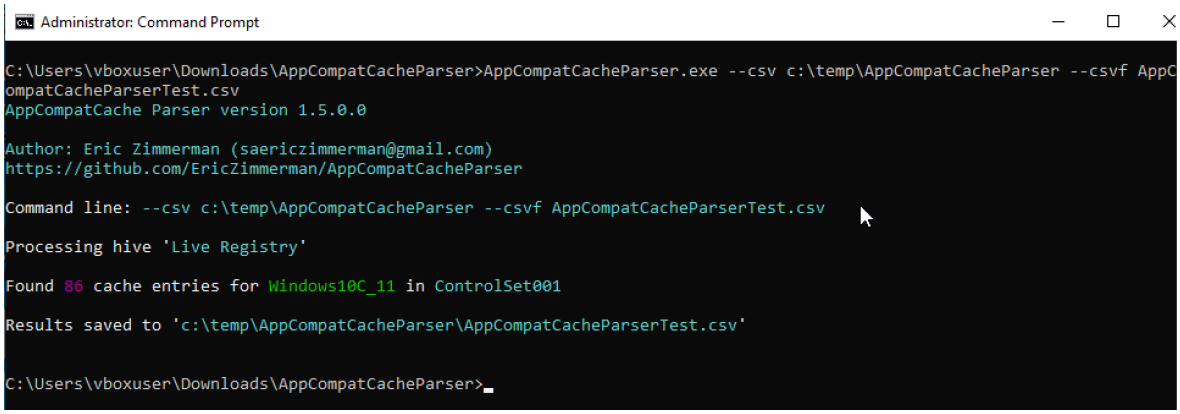
C:\Users\<user>\Downloads>dir

C:\Users\<user>\Downloads>cd AppCompatCacheParser

C:\Users\<user>\Downloads\AppCompatCacheParser>dir

C:\Users\<user>\Downloads\AppCompatCacheParser>AppCompatCacheParser.exe

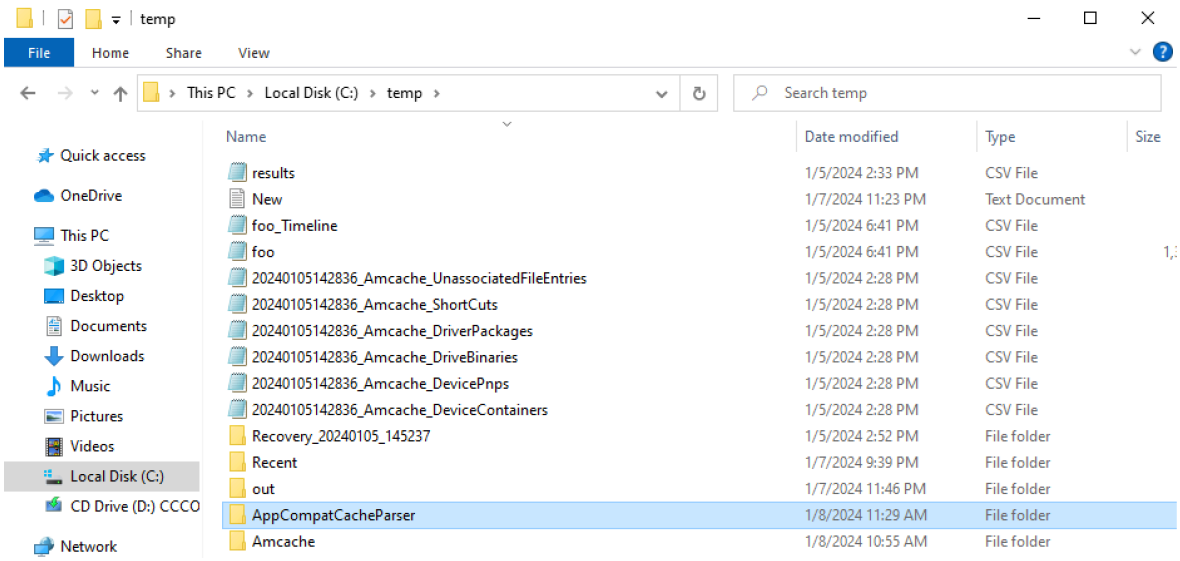
C:\Users\<user>\Downloads\AppCompatCacheParser>AppCompatCacheParser.exe --csv c:\temp\AppCompatCacheParser --csvf AppCompatCacheParserTest.csv



Obrázek 12 - Spuštění příkazu sběru AppCompatCache v cmd

Zdroj: Vlastní zpracování

Výsledkem je soubor ve spustitelném adresáři (obrázek 13):



Obrázek 13 - Získání dat AppCompatCache

Zdroj: Vlastní zpracování

ControlSet	CacheEntryPosition	Path	LastModifiedTimeUTC	Executed	Duplicate	SourceFile
1	0	C:\Windows\system32\SearchIndexer.exe	2023-05-05 12:21:06	No	FALSE	Live Registry
1	1	C:\Windows\system32\SgrmBroker.exe	2023-05-05 12:22:05	No	FALSE	Live Registry
1	2	C:\Windows\system32\wermgr.exe	2023-05-05 12:21:23	No	FALSE	Live Registry
1	3	C:\WINDOWS\SYSTEM32\RUNDLL32.EXE	2023-05-05 12:21:26	No	FALSE	Live Registry
1	4	C:\WINDOWS\SYSTEM32\veg.exe	2019-12-07 09:09:33	No	FALSE	Live Registry
1	5	C:\WINDOWS\SYSTEM32\SETUPUGC.EXE	2023-05-05 12:21:21	No	FALSE	Live Registry
1	6	C:\Windows\system32\provtool.exe	2023-05-05 12:20:40	No	FALSE	Live Registry
1	7	C:\Windows\system32\ByteCodeGenerator.exe	2023-05-05 12:21:10	No	FALSE	Live Registry
1	8	00000009 000a4a7f4a430000 000a000042ee0000 8664 Microsoft.ZuneVideo 8wekyb3d8bbwe		No	FALSE	Live Registry
1	9	00000009 000a4a7f4a430000 000a000042ee0000 8664 Microsoft.ZuneMusic 8wekyb3d8bbwe		No	FALSE	Live Registry
1	10	00000009 000c003217710000 000a000042ee0000 8664 Microsoft.XboxIdentityProvider 8wekyb3d8bbwe		No	FALSE	Live Registry
1	11	00000009 0001002e2af90000 000a000042ee0000 8664 Microsoft.XboxGameOverlay 8wekyb3d8bbwe		No	FALSE	Live Registry
1	12	00000009 0030003179190000 000a00003f810000 8664 Microsoft.XboxApp 8wekyb3d8bbwe		No	FALSE	Live Registry
1	13	00000009 2e8603ea00050000 000a000045550000 8664 Microsoft.WindowsStore 8wekyb3d8bbwe		No	FALSE	Live Registry
1	14	00000009 000a077207b40000 000a000045630000 8664 Microsoft.WindowsSoundRecorder 8wekyb3d8bbwe		No	FALSE	Live Registry
1	15	00000009 0005077207b40000 000a000045630000 8664 Microsoft.WindowsMaps 8wekyb3d8bbwe		No	FALSE	Live Registry
1	16	00000009 000107730c500000 000a000047ba0000 8664 Microsoft.WindowsFeedbackHub 8wekyb3d8bbwe		No	FALSE	Live Registry
1	17	00000009 3e852d6d4f5c0000 000a000045630000 8664 microsoft.windowscommunicationsapps 8wekyb3d8bbwe		No	FALSE	Live Registry
1	18	C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.181.5\MicrosoftEdgeUpdateComRegisterShell64.exe	2024-01-05 21:26:27	Yes	FALSE	Live Registry
1	19	00000009 07e2033a00620000 000a000045630000 8664 Microsoft.WindowsCamera 8wekyb3d8bbwe		No	FALSE	Live Registry

Obrázek 14 - Tabulka s údaji o artefaktu AppCompatCache

Zdroj: Vlastní zpracování

3. SRUM (System Resource Usage Monitor)

Pro uložení tohoto artefaktu pomocí příkazového řádku je třeba otevřít příkazový řádek a spustit příkaz nástroje SrumECmd.exe (obrázek 15):

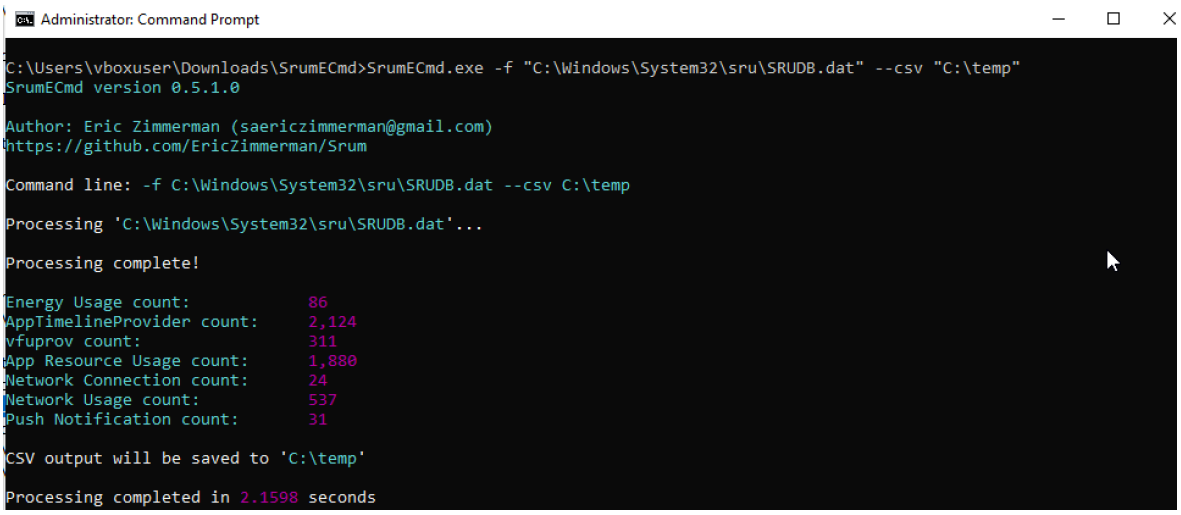
C:\Users\vboxuser\Downloads>dir

C:\Users\vboxuser\Downloads>cd SrumECmd

C:\Users\vboxuser\Downloads\SrumECmd>dir

C:\Users\vboxuser\Downloads\SrumECmd>SrumECmd.exe

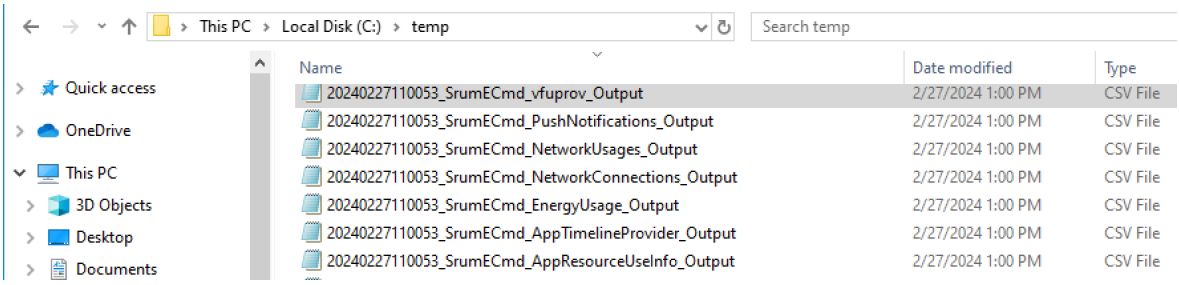
C:\Users\vboxuser\Downloads\SrumECmd>SrumECmd.exe - f "C:\Windows\System32\sru\SRUDB.dat" --csv "c:\temp"



Obrázek 15 - Spuštění příkazu sběru SRUM v cmd

Zdroj: Vlastní zpracování

Výsledkem jsou soubory ve spustitelném adresáři (obrázek 16):



Obrázek 16 - Získání dat SRUM

Zdroj: Vlastní zpracování

Stopy činnosti uživatele

1. Recent

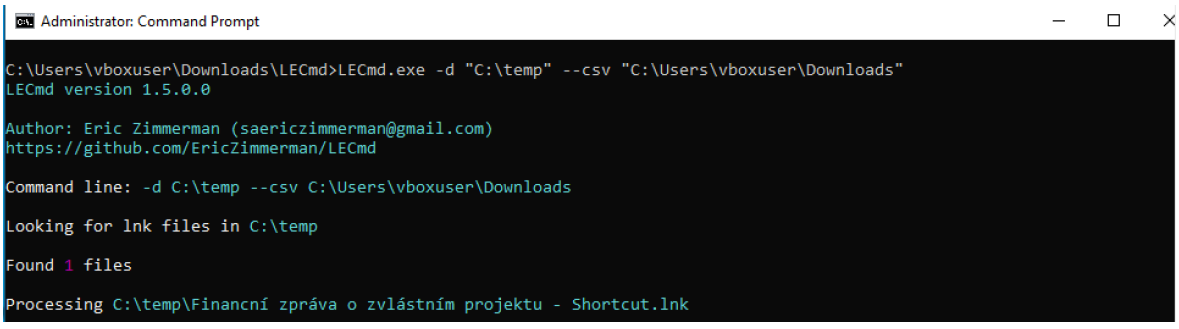
Pro uložení tohoto artefaktu pomocí příkazového řádku musíme otevřít příkazový řádek a spustit příkaz nástroje LECmd.exe (obrázek 17):

C:\Users\vboxuser\Downloads>cd LECmd

C:\Users\vboxuser\Downloads\LECmd>dir

C:\Users\vboxuser\Downloads\LECmd>LECmd.exe

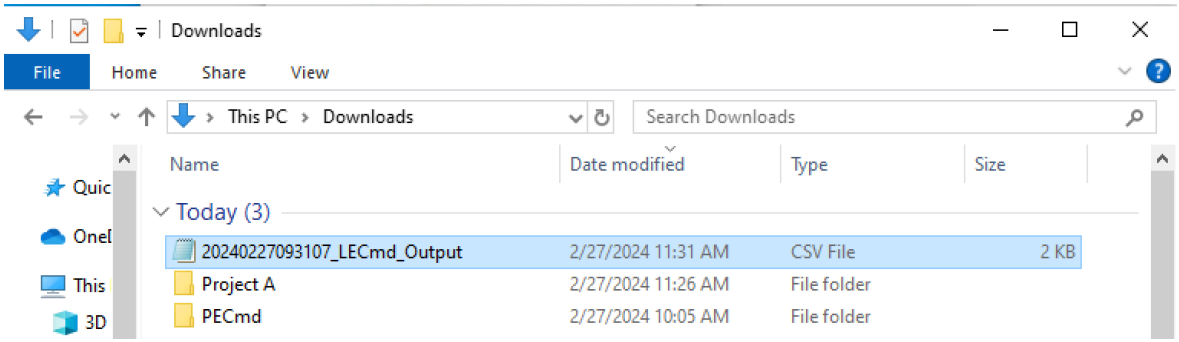
C:\Users\vboxuser\Downloads\LECmd>LECmd.exe - d "C:\Users\vboxuser\Dow nloads\Project A" --csv "C:\Users\vboxuser\Downloads"



Obrázek 17 - Spuštění příkazu sběru Recent v cmd

Zdroj: Vlastní zpracování

Výsledkem je soubor v adresáři uvedeném v příkazovém řádku (obrázek 18):

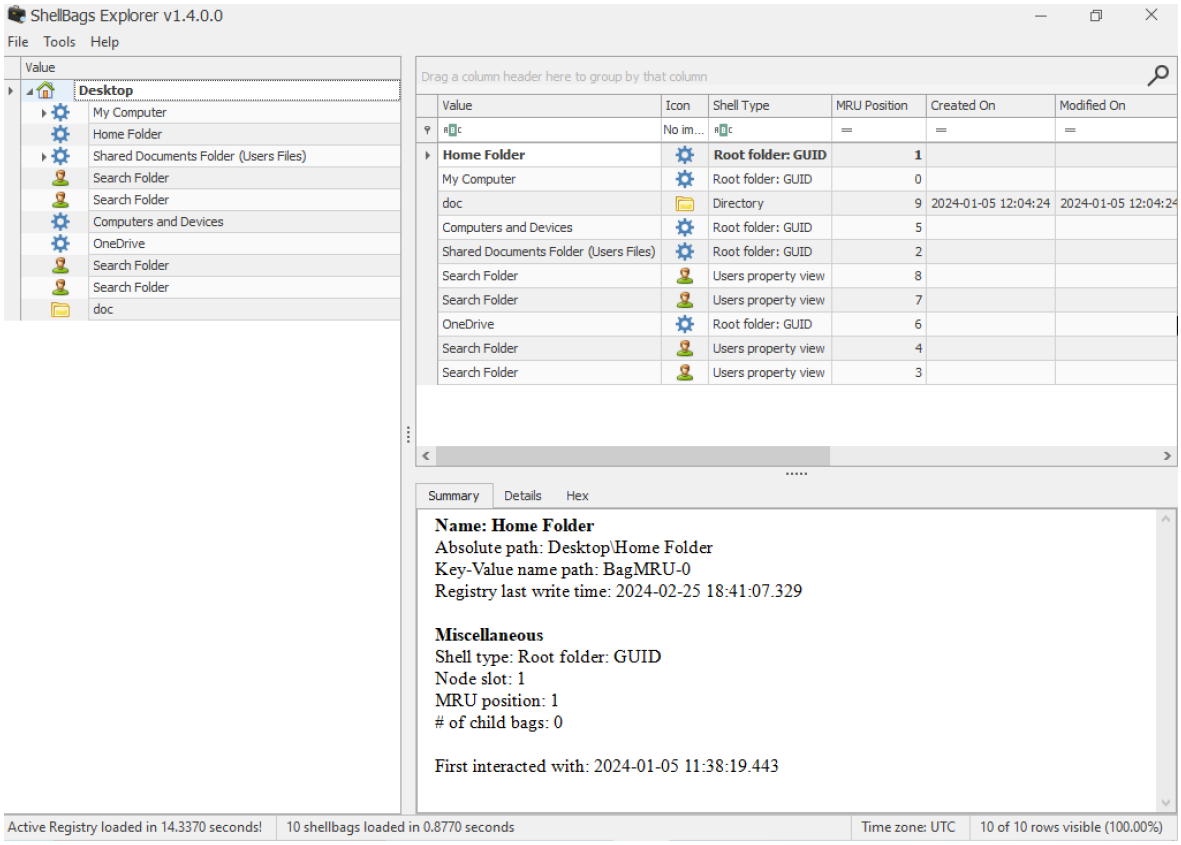


Obrázek 18 - Získání dat Recent

Zdroj: Vlastní zpracování

2. Shellbags

Tento artefakt zkoumáme v reálném čase pomocí nástroje ShellBagsExplorer.exe (obrázek 19):



Obrázek 19 - Výsledek nástroje ShellBagsExplorer.exe

Zdroj: Vlastní zpracování

3. Časová osa Win10

K uložení tohoto artefaktu pomocí příkazového řádku je třeba otevřít příkazový řádek a spustit příkaz nástroje WxTCmd.exe (obrázek 20):

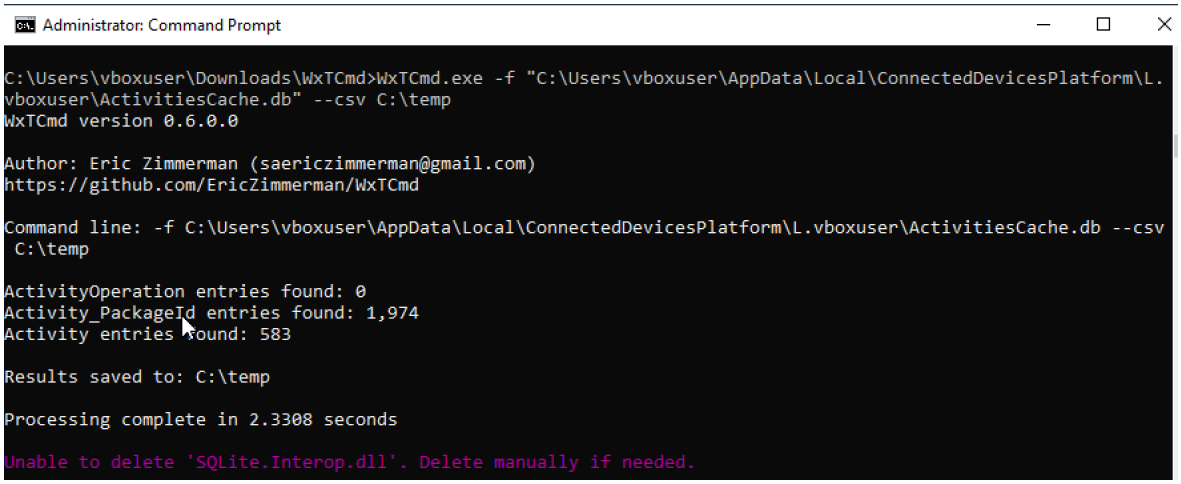
C:\Users\vboxuser\Downloads>dir

C:\Users\vboxuser\Downloads>cd WxTCmd

C:\Users\vboxuser\Downloads\WxTCmd>dir

C:\Users\vboxuser\Downloads\WxTCmd>WxTCmd.exe

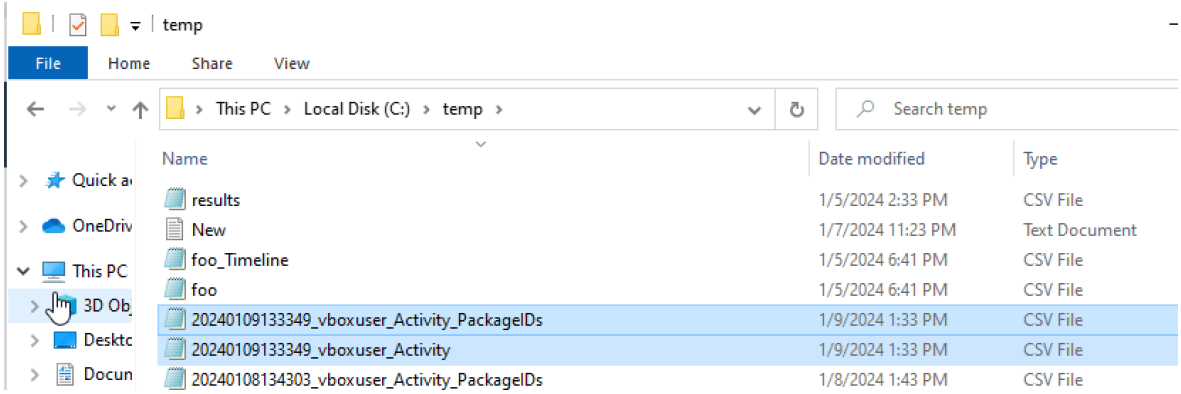
C:\Users\vboxuser\Downloads\WxTCmd>WxTCmd.exe - f "C:\Users\vboxuser\AppData\Local\ConnectedDevicesPlatform\L.vboxuser\ActivitiesCache.db" --csv C:\temp



Obrázek 20 - Spuštění příkazu Win10 Timeline v příkazovém řádku cmd

Zdroj: Vlastní zpracování

Výsledek se rovněž zobrazí v zadaném adresáři (obrázek 21).

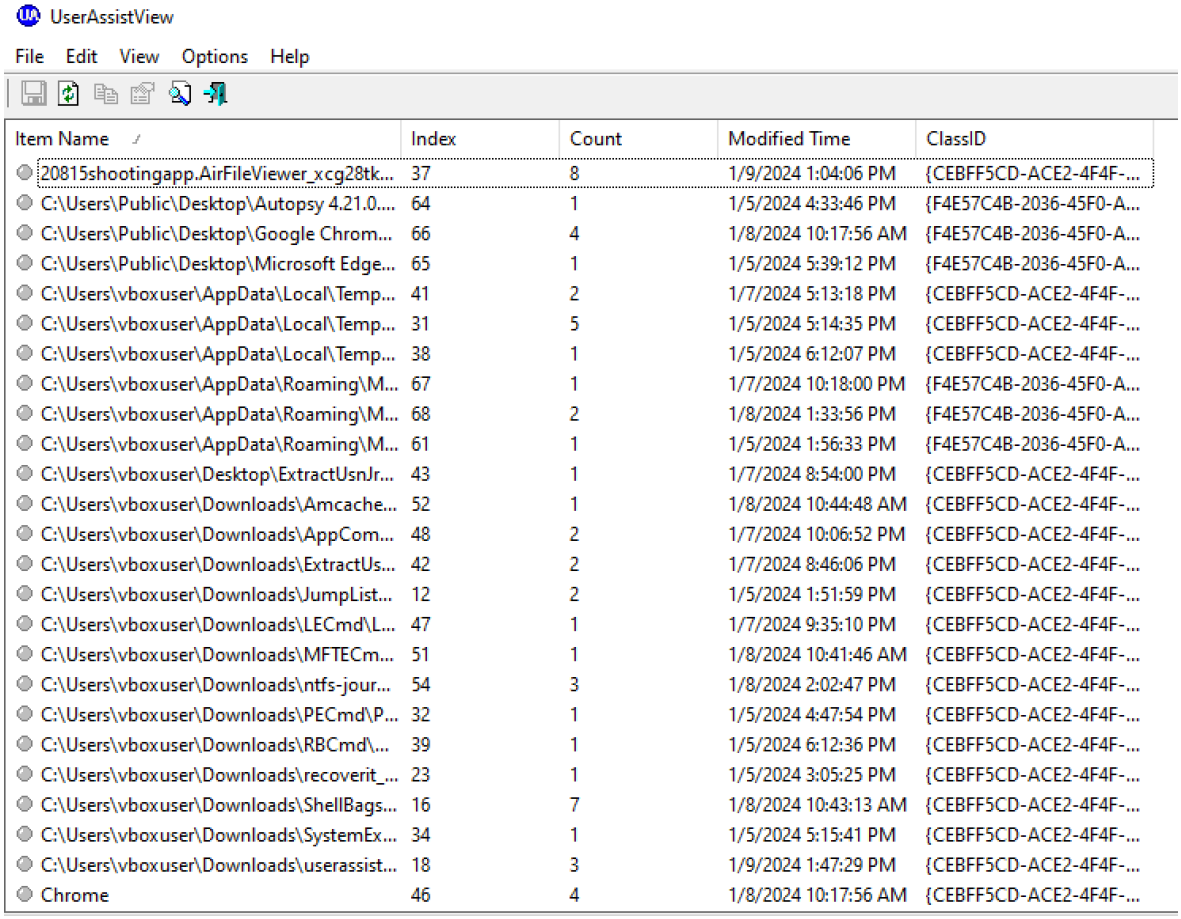


Obrázek 21 - Získání dat Win10 Timeline

Zdroj: Vlastní zpracování

4. Userassist

Tento artefakt zkoumáme v reálném čase pomocí nástroje UserAssistVeiw.exe (obrázek 22):



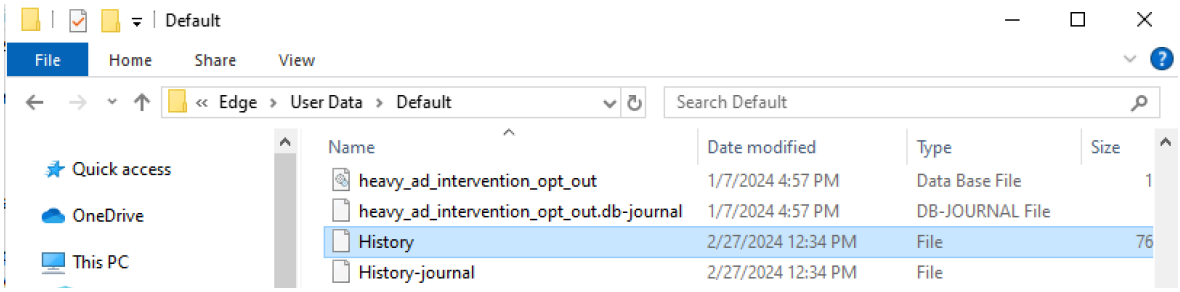
Item Name	Index	Count	Modified Time	ClassID
20815shootingapp.AirFileViewer_xcg28tk...	37	8	1/9/2024 1:04:06 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\Public\Desktop\Autopsy 4.21.0....	64	1	1/5/2024 4:33:46 PM	{F4E57C4B-2036-45F0-A...
C:\Users\Public\Desktop\Google Chrom...	66	4	1/8/2024 10:17:56 AM	{F4E57C4B-2036-45F0-A...
C:\Users\Public\Desktop\Microsoft Edge...	65	1	1/5/2024 5:39:12 PM	{F4E57C4B-2036-45F0-A...
C:\Users\vboxuser\AppData\Local\Temp...	41	2	1/7/2024 5:13:18 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\AppData\Local\Temp...	31	5	1/5/2024 5:14:35 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\AppData\Local\Temp...	38	1	1/5/2024 6:12:07 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\AppData\Roaming\M...	67	1	1/7/2024 10:18:00 PM	{F4E57C4B-2036-45F0-A...
C:\Users\vboxuser\AppData\Roaming\M...	68	2	1/8/2024 1:33:56 PM	{F4E57C4B-2036-45F0-A...
C:\Users\vboxuser\AppData\Roaming\M...	61	1	1/5/2024 1:56:33 PM	{F4E57C4B-2036-45F0-A...
C:\Users\vboxuser\Desktop\ExtractUsnJr...	43	1	1/7/2024 8:54:00 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\Amcache...	52	1	1/8/2024 10:44:48 AM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\AppCom...	48	2	1/7/2024 10:06:52 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\ExtractUs...	42	2	1/7/2024 8:46:06 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\JumpList...	12	2	1/5/2024 1:51:59 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\LECmd\L...	47	1	1/7/2024 9:35:10 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\MFTECm...	51	1	1/8/2024 10:41:46 AM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\ntfs-jour...	54	3	1/8/2024 2:02:47 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\PECmd\P...	32	1	1/5/2024 4:47:54 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\RBCmd\...	39	1	1/5/2024 6:12:36 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\recoverit_...	23	1	1/5/2024 3:05:25 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\ShellBags...	16	7	1/8/2024 10:43:13 AM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\SystemEx...	34	1	1/5/2024 5:15:41 PM	{CEBFF5CD-ACE2-4F4F-...
C:\Users\vboxuser\Downloads\userassist...	18	3	1/9/2024 1:47:29 PM	{CEBFF5CD-ACE2-4F4F-...
Chrome	46	4	1/8/2024 10:17:56 AM	{CEBFF5CD-ACE2-4F4F-...

Obrázek 22 - Výsledek nástroje UserAssistVeiw.exe

Zdroj: Vlastní zpracování

5. Historie prohlížeče (Browser History)

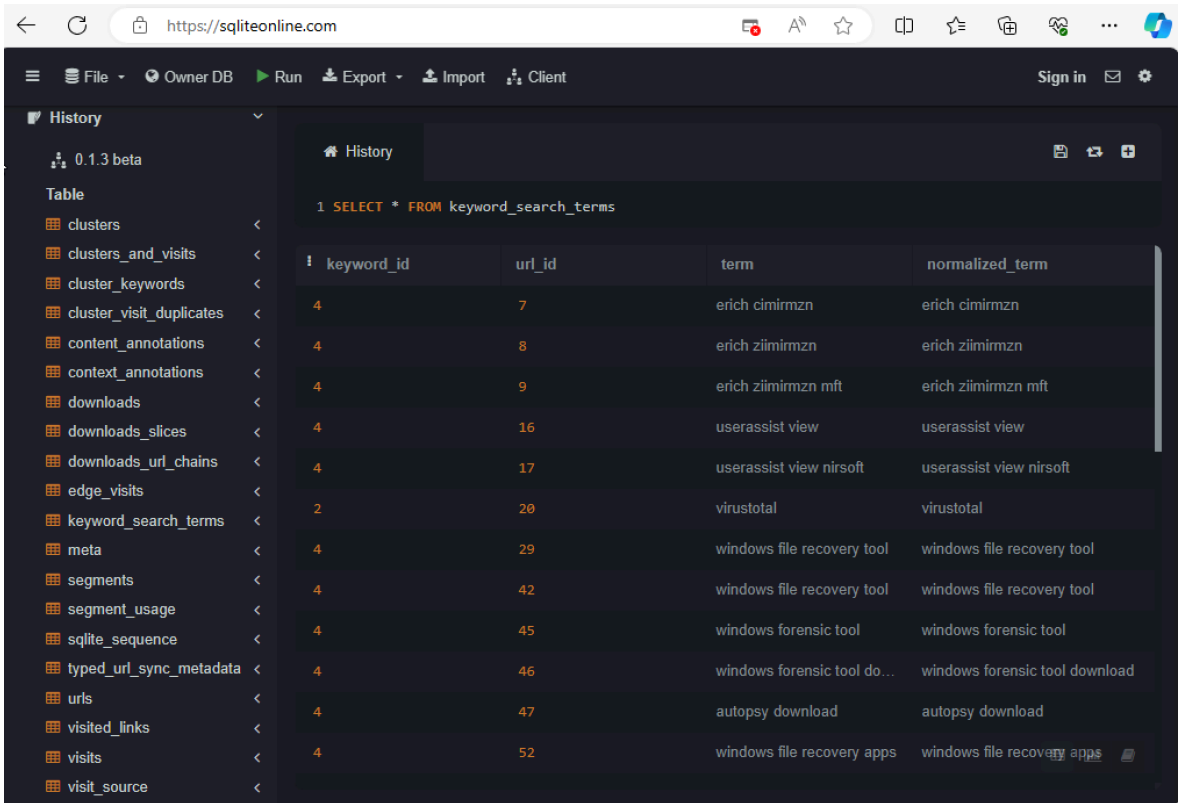
Umístění tohoto artefaktu je C: \Users\<user>\AppData\Local\Microsoft\Edge\User Data\Default (obrázek 23):



Obrázek 23 - Umístění dat historie prohlížeče

Zdroj: Vlastní zpracování

Soubor s názvem History s informacemi o historii prohlížeče Edge (jako příklad) je ve formátu SQLite. Pro otevření tohoto souboru je třeba použít odkaz https://sqliteonline.com/, tento online program je určen pro práci s databázemi, které jsou uloženy ve formátu SQLite (obrázek 24).

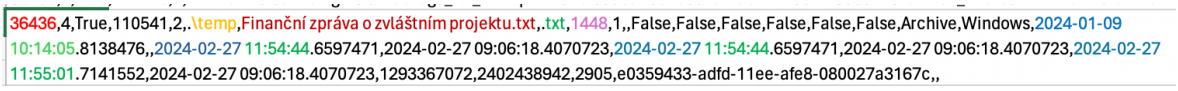


Obrázek 24 - Výsledek otevření souboru s historií prohlížeče pomocí SQLite online

Zdroj: Vlastní zpracování

4.1.4 Čtvrtá fáze: Analýza získaných informací

Analýza dat souborového systému, konkrétně artefaktu $MFT (obrázek 25), odhalila zajímavé informace ohledně dokumentu s názvem "Finanční zpráva o zvláštním projektu". Tento dokument byl poprvé vytvořen dne 9. ledna 2024 v 10:14 hodin. Zároveň bylo zjištěno, že tento projekt byl uložen do složky \temp. Dále se ukázalo, že soubor byl upraven 27. února 2024 v 11:54 hodin. Poslední přístup byl zaznamenán 27. února 2024 v 11:55 hodin. Velikost tohoto souboru je: 1448 kilobajtů. Přípona souboru: .txt.

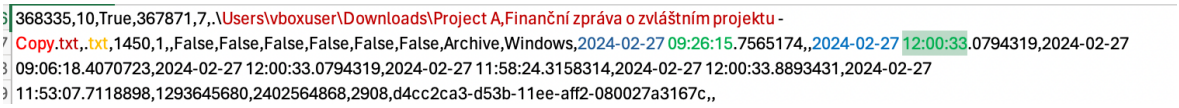


Obrázek 25 - Vybrané informace o artefaktu $MFT (1)

Zdroj: Vlastní zpracování

Další analýza artefaktu $MFT (obrázek 26) odhalila další důležité informace ohledně dokumentu. Zjistilo se, že uživatel počítače vytvořil kopii tohoto dokumentu dne 27. února 2024. Tuto kopii uložil do složky "Projekt A", která se nachází ve složce se staženými soubory.

Kromě toho bylo zjištěno, že došlo ke změně velikosti dokumentu. Velikost dokumentu se zvětšila, což naznačuje, že došlo k úpravám nebo doplněním v dokumentu.



Obrázek 26 - Vybrané informace o artefaktu $MFT (2)

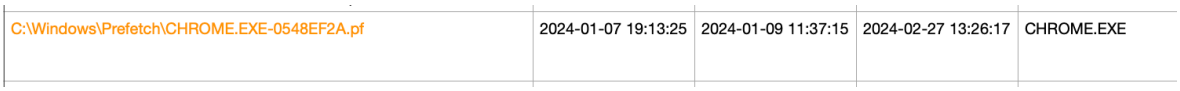
Zdroj: Vlastní zpracování

Byly nalezeny také informace o vytvoření zástupce tohoto dokumentu (obrázek 27).

Obrázek 27 - Vybrané informace o artefaktu $MFT (3)

Zdroj: Vlastní zpracování

Analýza mechanismu Windows Prefetch poskytla další důležité informace ohledně sledovaného dokumentu. Zjistilo se, že tento dokument byl otevřen pomocí aplikací Chrome.exe (obrázek 28), Notepad.exe (obrázek 29) a Wordpad.exe (obrázek 30). Zvláště poslední zmíněná aplikace, Chrome.exe, může naznačovat, že dokument byl stažen z internetu. Tato informace poukazuje na to, že dokument mohl být sdílen mezi několika uživateli prostřednictvím internetového prohlížeče Chrome. Tato zjištění jsou klíčová pro pochopení cesty, kterou dokument prošel od svého vytvoření až po jeho použití uživateli (obrázek 24).



Obrázek 28 - Vybrané informace o artefaktu Prefetch (1)

Zdroj: Vlastní zpracování

C:\Windows\Prefetch\NOTEPAD.EXE-EB1B961A.pf	2024-01-05 11:45:21	2024-02-27 12:57:47	2024-02-27 13:28:35	NOTEPAD.EXE

Obrázek 29 - Vybrané informace o artefaktu Prefetch (2)

Zdroj: Vlastní zpracování

C:\Windows\Prefetch\WORDPAD.EXE-1BCC3DB7.pf	2024-01-05 15:53:26	2024-02-27 12:00:10	2024-02-27 13:31:28	WORDPAD.EXE

Obrázek 30 - Vybrané informace o artefaktu Prefetch (3)

Zdroj: Vlastní zpracování

4.1.5 Pátá fáze: Shrnutí a závěr

V průběhu této práce byla vyvinuta a aplikována metoda sběru a analýzy artefaktů, která zahrnuje nejen pořadí a objasnění sběru artefaktů a pravidla pro ohledání místa události, ale také následnou dokumentaci získaných informací. Tato metoda odhalila cenné údaje o činnosti uživatele počítače a jeho interakci s konkrétním dokumentem.Na základě získaných údajů byly zjištěny následující informace:

- Uživatel počítače má na svém pevném disku konkrétní dokument;
- Byla zjištěna časová razítka, jako je datum vytvoření, poslední změny a otevření dokumentu, což pomáhá určit chronologii činností uživatele;
- Zkoumala se také velikost a přípona dokumentu, což může naznačovat typ a obsah dokumentu;
- Identifikováno bylo také umístění dokumentu, jeho kopie a označení;
- Bylo zjištěno, že tento dokument byl otevřen pomocí aplikace Chrome.exe, což může naznačovat, že byl stažen a sdílen mezi uživateli;
- Nebylo zjištěno žádné přihlášení k tomuto počítači jinými uživateli.

Na základě těchto údajů byl učiněn závěr, že uživatel, který měl přístup k dokumentu, s ním aktivně pracoval, otevíral ho, upravoval a případně stahoval. To ukazuje na jeho zapojení do trestného činu nebo události, k níž se dokument vztahuje.

Toto zjištění poskytuje cenné informace pro další vyšetřování a může být použito v soudním řízení nebo při správních žalobách. Vyvinutá metoda sběru a analýzy artefaktů se tedy ukázala jako účinná a praktická při vyšetřování digitálních incidentů.

5 Výsledky a diskuse

5.1 Výsledky a diskuse o použití vyvinuté metody

V současné době, v době rychlého rozvoje informačních technologií, zaujímá počítačová kriminalistika významné místo v systému občanského a trestního práva. Jejím úkolem je poskytovat objektivní a ucelené digitální důkazy v soudním řízení. Rychlý nárůst počtu počítačů a dalších digitálních informačních zařízení v každodenním životě činí z digitálních důkazů nedílnou součást forenzního vyšetřování.

Počítačová kriminalistika se zabývá digitálními zařízeními a daty v nich uloženými. Tato data, známá také jako artefakty, se mohou při správném shromáždění a analýze stát klíčovými důkazy. Mohou pomoci rekonstruovat řetězec událostí, najít pachatele nebo spolupachatele a vyřešit případ jako celek.

Hlavním cílem bakalářské práce bylo vyvinout metodu pro správné a důsledné vyhledávání a shromažďování digitálních stop v operačním systému Microsoft Windows. Toho bylo dosaženo vytvořením virtuálního prostředí systému Windows 10 a použitím nástrojů vyvinutých Ericem Zimmermanem i nástrojů zabudovaných do systému. Dílčím cílem bylo sběr a zkoumání artefakty za účelem získání užitečných informací, které by mohly být použity při vyšetřování incidentů. Za tímto účelem byl modelován případ podnikového podvodu a vytvořen dokument, který byl umístěn do virtuálního prostředí pro další analýzu.

Práce odhalila, že operační systém Windows uchovává rozsáhlé informace o činnostech uživatele, jako je vytváření, úprava a mazání souborů, má dočasné informace atd. Tyto údaje lze použít ke zjištění časového průběhu událostí a k identifikaci činností konkrétních uživatelů. Další analýza ukázala, že artefakty systému Windows mohou být cenným doplňkem jiných typů důkazů, například hmotných důkazů. Mohou pomoci vytvořit úplný obraz incidentu a poskytnout přesnější a komplexnější vyšetřování. Vyvinutá metoda se ukázala jako použitelná a užitečná pro sběr artefaktů.

5.2 Výsledky vypracovaného souboru opatření před zahájením sběru artefaktů

Než se přistoupí k praktickému vyjmutí artefaktů z elektroniky, nastává důležitá přípravná fáze, která zahrnuje technické i právní aspekty. Digitální artefakty získané

forenzním specialistou z technických a elektronických zařízení budou právně relevantní pouze tehdy, pokud byl proces sběru proveden v souladu se všemi nezbytnými pravidly a postupy. Kromě toho je důležité zajistit, aby data v zařízeních zůstala neporušená a nebyla během sběru zařízení z místa události změněna.

Důležitým aspektem je také dokumentace informací. To je nezbytné pro zajištění integrity a platnosti shromážděných údajů. Dokumentace procesu sběru artefaktů pomůže při dalším výzkumu a analýze a může být také použita jako důkaz v soudním řízení.

Výsledky vypracovaného souboru opatření před sběrem artefaktů ukazují, že řádná příprava a přísné dodržování všech postupů jsou klíčem k úspěšnému a efektivnímu procesu sběru dat. Tím je zajištěna integrita a validita shromážděných artefaktů, což následně zvyšuje jejich právní relevanci a užitečnost pro vyšetřování incidentů. Vypracovaný soubor bezpečnostních opatření před sběrem artefaktů je tedy nedílnou součástí procesu digitálního vyšetřování a zajišťuje spolehlivost a kvalitu shromážděných údajů.

6 Závěr

Přestože vláda i soukromé společnosti vynakládají značné úsilí a investují obrovské částky do rozvoje počítačové forenzní a informační bezpečnosti obecně, podvodů a kyberzločinců přibývá. Zároveň se také s bleskovým rozvojem technologií vyvíjejí nové typy hrozeb, proti kterým je třeba se chránit, takže nedostatečný rozvoj počítačové forenziky jsou vážnou hrozbou nejen pro každý podnik, ale i pro informační bezpečnost celé země.

V práci byly zvažovány oblasti ekonomické činnosti, typy podvodů, které mohou podnik postihnout, a také motivy, které lidi k páchání protiprávního jednání tlačí. Dále byly analyzovány trestné činy v digitálním prostředí, forenzní věda jako věda, která se zabývá vyšetřováním digitálních incidentů. Byly probrány její oblasti a metody, jakož i fáze vyšetřování kybernetických trestných činů.

Dále byla zkoumána počítačová kriminalistika jako obor kriminalistiky. V této části byly probrány základní vyšetřovací techniky a analyzovány artefakty potřebné v počítačové kriminalistice. Na základě technik, artefaktů a existujících řešení pro jejich sběr byl vytvořen soubor opatření a metoda pro sběr artefaktů v operačním systému Microsoft Windows, které byly následně použity ve virtuálním prostředí.

Vyvinutá metoda a její praktická implementace pro sběr artefaktů, pokud jsou správně a bezpodmínečně splněny všechny body, umožňuje získat informace o počítačovém incidentu co nejrychleji. Aplikace této metody oddělením IT ve firmě přinese zvýšení efektivity při vyšetřování ekonomických podvodů, skrytých machinací a falšování dat. Je třeba poznamenat, že praktickou implementaci, provedenou v této práci, lze vylepšit, například je možné sběr artefaktů automatizovat pomocí programovacího jazyka Python. Takový vývoj zjednoduší proces sběru artefaktů a také tento proces urychlí, což umožní poskytnout artefakt k vyšetřování operativně a v co nejkratší době.

7 Bibliografie

—. 2018b. Forensics Windows Free tools in Web Browser Artifacts (history, cookie, cache). *Codeby.net.* [Online] Codeby.net, 07 23, 2018b. [Cited: 11 25, 2023.] https://codeby.net/threads/forensics-windows-free-tools-in-web-browser-artifacts-history-cookie-cache.64181/.

—. 2020. The Windows USN Journal. *Velociraptor.* [Online] Velociraptor, 12. 11 2020. [Citace: 02. 09 2023.] https://velociraptor.velocidex.com/the-windows-usn-journal-f0c55c9010e.

—. 2022. JumpList Class. *Microsoft.* [Online] Microsoft, 2022. [Cited: 12 25, 2023.] https://learn.microsoft.com/en-us/uwp/api/windows.ui.startscreen.jumplist?view=winrt-22000.

ADMIN. 2022. Prefetch: chto ehto za papka i mozhno li ee udalit? *Blog molodogo admina.* [Online] Blog molodogo admina, 2022. [Citace: 20. 12 2023.] https://fulltienich.com/chto-za-papka-prefetch-i-kak-ee-udalit/.

ALBRECHT, W. S., ALBRECHT, C. O., ALBRECHT, C. C., ZIMBELMAN, M. F. 2012. *Fraud Examination Fourth Edition.* South-Western : Cengage Learning, 2012. 0-538-47084-4.

BABU, M., PARISHAT, M. G. 2004. What Is Cybercrime? *Computer Crime Research Center.* [Online] 10 11, 2004. [Cited: 09 12, 2023.] https://www.crime-research.org/analytics/702.

BARBOŘÍK, M., KOSOVÁ, L. 2023. Fenomén zvyšující se kybernetické kriminality byl hlavním tématem aktivit ke Dni bezpečnějšího internetu 2023. *Prevence kriminality.* [Online] 10. 02 2023. [Citace: 23. 09 2023.] https://prevencekriminality.cz/fenomen-zvysujici-se-kyberneticke-kriminality-byl-hlavnim-tematem-aktivit-ke-dni-bezpecnejsiho-internetu-2023/#:~:text=Kybernetická%20kriminalita%20patř%C3%AD%20v%20České,%25%20(94%2C9%20%25)..

BERTOVSKIJJ, L. 2016. *Rassledovanie prestuplenijj ehkonomicheskojj napravlennosti. Nauchno-prakticheskoe posobie.* Moskva : Prospekt, 2016. 978-5-392-20119-8.

BRODOWSKI, D., FREILING, F. 2011. *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft.* Berlin : s.n., 2011. 978-3-929619-66-9.

BROOKS, C. J., GROW, C. ,CRAIG, P. A., SHORT, D. 2018. *Cybersecurity Essentials.* Alameda : Sybex, 2018. 9781119362456.

CASEY, E. 2011. *Digital Evidence and Computer Crime, Forensic Science, Computers and Internet.* USA : Academic Press, 2011. 9780123742681.

CLOUDIAN. 2023. Understanding Digital Forensics: Process, Techniques, and Tools. *BlueVoyant.* [Online] BlueVoyant, 2023. [Cited: 10 15, 2023.] https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools.

COHEN, M. 2022. Digging Into The System Resource Usage Monitor (SRUM). *Velociraptor.* [Online] Velociraptor, 2022. [Cited: 12 21, 2023.] https://docs.velociraptor.app/blog/2019/2019-12-31_digging-into-the-system-resource-usage-monitor-srum-afbadb1a375/.

EADRES. 2021. Fraza dnja: kompjuternaja kriminalistika (kiber-kriminalistika). *eAdres.* [Online] eAdres, 11. 05 2021. [Citace: 25. 08 2023.] https://eadres.ru/blog/--609a5862b46ab.html.

EMBROKER. 2023. What is the Fraud Triangle? (Three Components Explained). *Embroker.* [Online] Embroker Insurance Services LLC, 09 21, 2023. [Cited: 02 10, 2024.] https://www.embroker.com/blog/fraud-triangle/.

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION. 2022. Economic Crime. *Europol.* [Online] Europol, 2022. [Cited: 06 20, 2023.] https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/economic-crime.

EVENT LOG EXPLORER. 2023. ZHurnaly sobytijj Windows. *Event Log Explorer.* [Online] Event Log Explorer, 18. 10 2023. [Citace: 20. 11 2023.] https://eventlogxp.com/rus/essentials/windowseventlog.html.

FORENCSIC CERTIFIED PUBLIC ACCOUNTANT. 2018. What is a Forensic Accountant? *Forensic CPA Society.* [Online] Forensic Certified Public Accountant Society, 2018. [Cited: 10 5, 2023.] https://www.fcpas.org/about-us/what-is-a-forensic-accountant/.

FORENSICS. 2020. The Amcache registry and how to access it. *LITIGATION SUPPORT TIP OF THE NIGHT.* [Online] 01 04, 2020. [Cited: 12 15, 2023.] https://www.litigationsupporttipofthenight.com/single-post/2020/06/03/the-amcache-registry-and-how-to-access-it#:~:text=Amcache%20is%20a%20database%20on,hve%20on%20Windows%2010..

GITHIB. 2022. Recent file cache. *GitHib.* [Online] GitHib, 11 21, 2022. [Cited: 11 17, 2023.] https://github.com/ForensicArtifacts/artifacts-kb/blob/main/docs/sources/windows/RecentFileCache.md.

GONZÁLEZ, A. G. 2022. The importance of RAM in computer forensic analysis. *Atalayar.* [Online] Atalayar, 01 26, 2022. [Cited: 09 01, 2023.] https://www.atalayar.com/en/articulo/new-technologies-innovation/importance-ram-computer-forensic-analysis/20220124160303154780.html.

GROSS, H., KALLEN, H.M. 2017. *Criminal Psychology: A Manual for Judges, Practitioners, and Students.* s.l. : USA: Legare Street Press, 2017. 978-1015521926.

CHANDEL, R. 2020. Forensic Investigation: Shellbags. *Hacking Articles.* [Online] Hacking Articles, 10 26, 2020. [Cited: 12 22, 2023.] https://www.hackingarticles.in/forensic-investigation-shellbags/.

INTERNATIONAL BUSINESS MACHINES. 2022. What is digital forensics and incident response (DFIR)? *IBM.* [Online] 2022. [Cited: 12 10, 2023.] https://www.ibm.com/topics/dfir.

KASPERSKI, K. 2020. NTFS iznutri. Kak ustroena fajjlovaja tablica MFT v Windows. *Khaker.* [Online] Khaker, 29. 01 2020. [Citace: 2023. 09 02.] https://xakep.ru/2020/01/29/ntfs-inside/.

KOZHUKHOV, D. 2021. Kak sozdat damp operativnojj pamjati Windows. *SPY-SOFT.NET.* [Online] SPY-SOFT.NET, 17. 06 2021. [Citace: 01. 09 2023.] https://spy-soft.net/how-to-create-memory-dump-windows/.

MAGNET FORENSICS . 2022. What is MRU (Most Recently Used)? *Magnet Forensics.* [Online] Magnet Forensics, 09 09, 2022. [Cited: 11 29, 23.] https://www.magnetforensics.com/blog/what-is-mru-most-recently-used/.

MICROSOFT OFFICE. 2023. Co je to kybernetická bezpečnost? *Microsoft Office.* [Online] Microsoft Office, 2023. [Citace: 25. 09 2023.] https://support.microsoft.com/cs-cz/topic/co-je-to-kybernetická-bezpečnost-8b6efd59-41ff-4743-87c8-0850a352a390.

MICROSOFT. 2023. about_PSReadLine. *Microsoft.* [Online] Microsoft, 11 14, 2023. [Cited: 12 29, 2023.] https://learn.microsoft.com/en-us/powershell/module/psreadline/about/about_psreadline?view=powershell-7.4.

MIROSHINA, E. 2016. Ponimanie ehkonomicheskojj svobody v sovremennom obshhestve. *Cyberleninka.* [Online] 2016. [Citace: 11. 07 2023.] https://cyberleninka.ru/article/n/ponimanie-ekonomicheskoy-svobody-v-sovremennom-obschestve.

MUSIL, J., SUCHÁNEK, J., KONRÁD, Z. 2004. *Kriminalistika (2. přepracované a doplněné vydání).* Praha : C. H. Beck, 2004. 80-7179-878-9.

NEMCHENKO, G., TOKAREV, JU., IGNATOV, E. 2016. *Institucionalnoe oformlenie ehkonomicheskojj svobody.* Moskva : MGJUA, 2016. No 10 (119).

PARLAMENT ČESKÉ REPUBLIKY. 1961. Zákon č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád). *Zákony pro lidi.* [Online] Parlament České republiky, 09. 12 1961. [Citace: 15. 02 2024.] https://www.zakonyprolidi.cz/cs/1961-141#cast1.

PAYNE, B. K. 2016. *White-Collar Crime: The Essentials.* New York : SAGE Publications, Inc, 2016. 1506344771.

POLICIE ČR. 2023. Odbor hospodářské kriminality. *Policie ČR.* [Online] Policie ČR, 2023. [Citace: 09. 02 2023.] https://www.policie.cz/clanek/uskpv-ohk-odbor-hospodarske-kriminality.aspx.

POŽÁR, J., HNÍK, V. 2023. Charakteristika vyšetřování kybernetické kriminality. *Ministerstvo vnitra.* [Online] 2023. [Citace: 14. 02 2024.] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjs5P25ovOEAxVq7QIHHcjyB7sQFnoECBsQAQ&url=https%3A%2F%2Fwww.mvcr.cz%2Fsoubor%2Fpolicejni-akademie.aspx&usg=AOvVaw3VSpuFl2HyOeXcR8WSWkHH&opi=89978449.

PŘEDSEDNICTVO ČESKÉ NÁRODNÍ RADY. 1992. LISTINY ZÁKLADNÍCH PRÁV A SVOBOD. *Poslanecká sněmovna Parlamentu České republiky.* [Online] Poslanecká sněmovna Parlamentu České republiky, 16. 12 1992. [Citace: 10. 08 2023.] https://www.psp.cz/docs/laws/listina.html.

RAK, R., PORADA, V. 2013. *Kybernetická kriminalita.* Praha [i.e. Karlovy Vary] : Vysoká škola Karlovy Vary, 2013. 978-80-87236-16-1.

SAFONOV, L. 2017. Kompjuternaja kriminalistika (forenzika) — obzor instrumentarija i trenirovochnykh ploshhadok. *Habr.* [Online] Habr, 02. 05 2017. [Citace: 07. 11 2023.] https://habr.com/ru/articles/327740/.

SCULLY, M. 2021. Outlook data file. *Microsoft.* [Online] Microsoft, 09 15, 2021. [Cited: 11 30, 2023.] https://answers.microsoft.com/en-us/outlook_com/forum/all/outlook-data-file/7b5bca8b-dcc5-4e09-a996-a8e5a38bf087.

SHKOLA WINDOWS. 2021. Dlja chego Windows nuzhen sistemnyjj reestr – osnovy ispolzovanija i upravlenija. *Shkola Windows.* [Online] Shkola Windows, 10. 07 2021. [Citace: 20. 11 2023.] https://windows-school.ru/blog/sistemnyj_reestr/2021-07-10-781.

STALLINGS, W., BROWN, L. 2017. *Computer Security: Principles and Practice.* s.l. : Pearson, 2017. 9780134794105.

STRAUS, J. 2008. *Kriminalistická metodika.* Plzeň : Aleš Čeněk s.r.o., 2008. 978-80-7380-124-3.

SUNNYCH. 2018a. Codeby.net. *Forensics Windows Registry - rasshifrovka i otobrazhenie vsekh zapisejj UserAssist.* [Online] Codeby.net, 04. 08 2018a. [Citace: 21. 12 2023.] https://codeby.net/threads/forensics-windows-registry-rasshifrovka-i-otobrazhenie-vsex-zapisej-userassist.64342/.

SUPERUSER. 2023. Where does Windows 10 store the last visited files, recent folders, and frequent folders? *SuperUser.* [Online] SuperUser, 12 01, 2023. [Cited: 12 29, 2023.] https://superuser.com/questions/1508457/where-does-windows-10-store-the-last-visited-files-recent-folders-and-frequent.

THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. 2023. Digital security. *The Organisation for Economic Co-operation and Development (OECD).* [Online] The Organisation for Economic Co-operation and Development, 2023. [Cited: 09 14, 2023.] https://www.oecd.org.

VARGOVA, Z. 2021. How to trace the user: Windows 10 Timeline. *IstroSec.* [Online] IstroSec, 11 30, 2021. [Cited: 12 21, 2023.] https://istrosec.com/blog/windows-10-timeline/.

VICHLENDA, M. 2011. Kriminalistika. *sosoom-zlin.* [Online] 2011. [Citace: 21. 07 2023.] https://www.sosoom-zlin.cz/media/skripta/kriminalistika.pdf.

VIRUSNET. 2019. Amcache i Shimcache v kriminalisticheskom analize. *VirusNet.* [Online] VirusNet, 26. 07 2019. [Citace: 21. 12 2023.] https://virusnet.info/amcache-i-shimcache-v-kriminalisticheskom-analize/.

8 Seznam obrázků a tabulek

8.1 Seznam obrázků

Obrázek 1 Schéma trojúhelníku podvodu 18
Obrázek 2 - Spuštění nástroje MFTECmd z příkazového řádku 42
Obrázek 3 - Výsledek nástroje MFTECmd 42
Obrázek 4 - Spuštění příkazu USN Journal v cmd 43
Obrázek 5 - Výsledek nástroje USN Journal 43
Obrázek 6 - Spuštění příkazu wevtutil v cmd 44
Obrázek 7 - Výsledek nástroje wevtutil 44
Obrázek 8 - Spuštění příkazu RegRipper v cmd 45
Obrázek 9 - Výsledek nástroje RegRipper 45
Obrázek 10 - Spuštění příkazu sběru Prefetch v cmd 46
Obrázek 11 - Získání dat Prefetch 46
Obrázek 12 - Spuštění příkazu sběru AppCompatCache v cmd 47
Obrázek 13 - Získání dat AppCompatCache 47
Obrázek 14 - Tabulka s údaji o artefaktu AppCompatCache 48
Obrázek 15 - Spuštění příkazu sběru SRUM v cmd 48
Obrázek 16 - Získání dat SRUM 49
Obrázek 17 - Spuštění příkazu sběru Recent v cmd 49
Obrázek 18 - Získání dat Recent 50
Obrázek 19 - Výsledek nástroje ShellBagsExplorer.exe 50
Obrázek 20 - Spuštění příkazu Win10 Timeline v příkazovém řádku cmd 51
Obrázek 21 - Získání dat Win10 Timeline 51
Obrázek 22 - Výsledek nástroje UserAssistVeiw.exe 52
Obrázek 23 - Umístění dat historie prohlížeče 52
Obrázek 24 - Výsledek otevření souboru s historií prohlížeče pomocí SQLite online 53
Obrázek 25 - Vybrané informace o artefaktu $MFT (1) 54
Obrázek 26 - Vybrané informace o artefaktu $MFT (2) 54
Obrázek 27 - Vybrané informace o artefaktu $MFT (3) 54
Obrázek 28 - Vybrané informace o artefaktu Prefetch (1) 54
Obrázek 29 - Vybrané informace o artefaktu Prefetch (2) 55
Obrázek 30 - Vybrané informace o artefaktu Prefetch (3) 55

8.2 Seznam tabulek

Tabulka 1 - Oblasti výzkumu forenzní vědy 27
Tabulka 2 - Fáze forenzního procesu 28
Tabulka 3 - Forenzní metody 29
Tabulka 4 - Základní vyšetřovací techniky 31