ZÁKLADY DIGITÁLNÍ FORENZIKY

Co-funded by the
Erasmus+ Programme
of the European Union

Obsah

1. Úvod do digitální forenziky

Pojmy, definice

1. Úvod do digitální forenziky

Digitální forenzní analýza přímo souvisí s reakcí na incidenty, je dokonce jednou z jejích nejdůležitějších složek a je nezbytná k získání informací o událostech a akcích provedených v analyzovaném systému. Digitální forenzní analýza má také kriminalistickou úlohu, neboť zkoumá minulé akce na zařízeních ve snaze identifikovat a shromáždit důkazy o trestném činu, které by mohly pomoci při rozhodování u soudu.

"je nemožné, aby zločinec jednal, zejména s ohledem na intenzitu zločinu, aniž by zanechal stopy této přítomnosti". (Doktor Edmond Locard, s.d.)[1]

Digitální forenzní věda *Je chápána jako odvětví forenzní vědy, které studuje a uplatňuje proces získávání, analýzy a uchovávání digitálních důkazů tak, aby byly* právně přípustné a technicky nezpochybnitelné u soudu.

Digitální důkaz je jakýkoli údaj nebo digitální informace, která je právně přípustná (získání) a technicky nezpochybnitelná (původ, integrita a nepopiratelnost).

Digitální informace jsou všechna data uložená nebo přenášená digitálně, jako jsou protokoly, dokumenty, e-maily, databáze, síťový provoz a mnoho dalších.

Cíl digitální forenzní analýzy a reakce na incidenty:

- Identifikace, shromáždění a uchování důkazů o kybernetickém trestném činu;
- interpretovat, dokumentovat a předkládat důkazy tak, aby byly přípustné u soudu;
- Porozumět technikám a metodám používaným pachateli trestné činnosti;
- Reagovat na incidenty, aby se zabránilo ztrátám duševního a finančního vlastnictví a pověsti během útoku;
- Znát právní předpisy různých regionů;
- Seznamte se s procesy manipulace s digitálními platformami, typy dat a operačními systémy;
- Určit vhodné nástroje pro forenzní vyšetřování;
- Obnovení smazaných souborů, skrytých souborů a dočasných dat, která lze použít jako důkazní materiál;
- Podporovat trestní stíhání při vyšetřování kyberkriminality;
- Chránit organizaci před podobnými incidenty v budoucnu.

1.1. Povinnosti odborníka

Forenzní analytik, stejně jako počítačový znalec, je ze zákona odpovědný za analýzu digitálního obsahu zařízení, které mu bude svěřeno, a vypracuje zprávu nazvanou digitální forenzní znalecký posudek. Poté, co jste byli seznámeni se sankcemi za odmítnutí nebo nesplnění povinností, přečtěte před soudním orgánem nebo soudcem následující větu: "Zavazuji se na svou čest, že budu věrně plnit svěřené povinnosti" a podepište prohlášení o závazku. Tímto

[1] https://www.crimemuseum.org/crime-library/forensic-investigation/edmond-locard

způsobem se znalec zavazuje provést analýzu a digitální forenzní zprávu, přičemž znalci, kteří jsou státními úředníky a zasahují do výkonu svých povinností, jsou z doby závazku vyňati. Bude informován o postupu a o otázkách, které má zodpovědět. Sankce za odmítnutí nebo nesplnění povinnosti jsou přítomny v portugalském trestním řádu v článku 91, č. 1. 4. Pokud jde o doručení znaleckého posudku, článek 157 téhož trestního řádu stanoví, že posudek musí obsahovat řádně odůvodněné odpovědi a závěry a musí být předložen ve lhůtě nepřesahující 60 dnů.

Je nezbytné, aby zpráva obsahovala pouze pravdivé údaje, protože za nepravdivé údaje hrozí podle čl. 3 odst. 1 trest odnětí svobody na šest měsíců až tři roky nebo pokuta nejméně 60 dnů. 360.

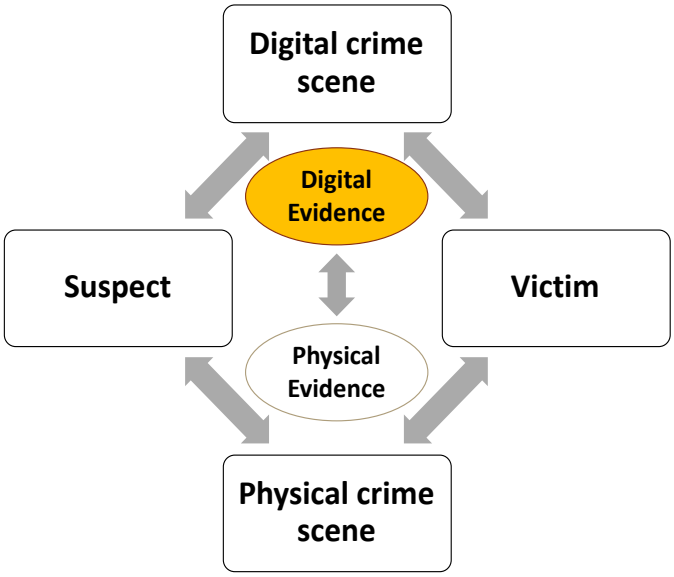
1.2. Aplikace digitální forenzní analýzy

Oblasti činnosti digitální forenziky jsou stále rozsáhlejší, zatímco dříve se analyzovaly pouze pevné disky a jiná média pro ukládání informací, nyní může být nutné shromažďovat a analyzovat data v nestálých pamětech (výkon v rámci forenziky živých dat) nebo dokonce data síťového provozu (síťová forenzika), data uložená v mobilních zařízeních (mobilní forenzika), data uložená v distribuovaných systémech v cloudech na internetu a mnoho dalších.

Edmond Locard (Obrázek 1) uvedl, že:

> *"je nemožné, aby zločinec jednal, zejména s ohledem na intenzitu trestného činu, aniž by zanechal stopy své přítomnosti".*

U trestných činů, které nějakým způsobem zahrnují digitální složku, kybernetické a kyberneticky závislé trestné činnosti (R. Bravo) a podle vyjádření Edmonga Locarda existuje větší možnost zanechání digitálních důkazů, které souvisejí s použitím digitálních prostředků.



Obrázek 1 - Schéma Edmonda Locarda

Zdroj: https://www.crimemuseum.org/crime-library/forensic-investigation/edmond-locard

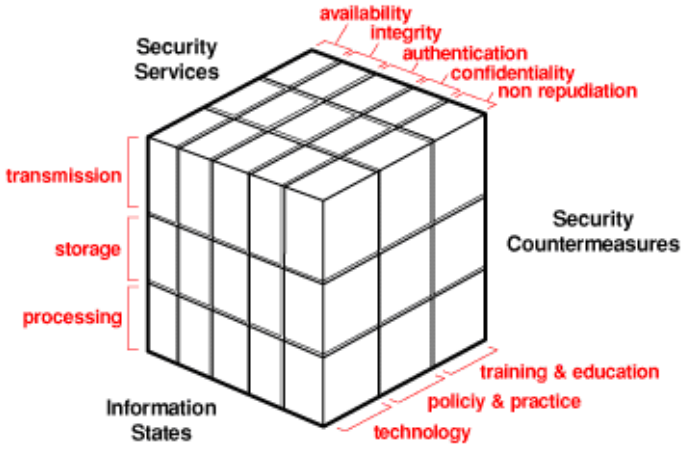
Digitální forenzní analýza není považována za exaktní vědu a je možné, že stejná digitální forenzní zpráva analyzovaná různými lidmi může být chápána různě, proto je nezbytné zajistit základní zásady bezpečnosti informací (obrázek 2), důvěrnost, integritu a nepopíratelnost. Tímto způsobem bude digitální forenzní analýza nutně:

PRÁVNĚ PŘÍPUSTNÉ A TECHNICKY NEZPOCHYBNITELNÉ.

Použití všeobecně uznávaných technik, dodržování ustanovení vnitrostátních právních předpisů ve snaze poskytnout na každou zkoumanou otázku co nejúplnější odpověď, přičemž 7 důvodů je nejúplnější formou odpovědi:

"Cože? Kde?, Kdy?, Jak?, Kdo?, Proč? a Kolik?"

Inspektor-koordinátor Rogério Bravo - soudní policie



Obrázek 2 - Bezpečnost informací

Zdroj: John McCumber

Důvěrnost

Do rozhodnutí soudu jsou a musí zůstat dotčené osoby nevinné a přístup k jejich údajům je zcela omezen na samotného znalce, který je nemůže poskytnout třetím osobám.

Autentičnost

Důkazy musí být autentické. Vypracované lidmi, kteří o nich mohou odpovědět. V opačném případě jsou důkazy u soudu považovány za irelevantní.

Integrita

Informace obsažené v zařízeních musí být za každou cenu zachovány v původním stavu. Odborník je odpovědný za použití technik, které mění integritu informací.

Žádné odmítnutí

Pokud jde o výkon znaleckých funkcí, "nepopírání" vyhovuje použití všeobecně uznávaných technik, které umožňují využít protiznalectví k dosažení stejných výsledků.

1.3. Výzvy digitální forenziky

Digitální forenzní metody a techniky čelí v současnosti velkým výzvám, které nutí forenzní vyšetřovatele k neustálému výzkumu a zdokonalování. Tradičně se digitální forenzní vyšetřovatelé systematicky snaží mnohem podrobněji zkoumat artefakty při hledání možné stopy, která by mohla být důkazem trestného činu. S vývojem technologií je však třeba zdokonalovat a přizpůsobovat postupy a přístupy k vyhledávání těchto důkazů trestné činnosti. Existuje spousta nových drobných výzev, které musí digitální kriminalistika překonat, nicméně předkládáme jejich stručný přehled ve třech kategoriích:

Technické údaje:

- Různé typy úložišť;
- Šifrování;
- Stegnografie;
- Antiforenzní techniky;
- Získávání a analýza dat v živé kriminalistice;
- Utajení a likvidace dat;
- Volatilita dat;
- Síťové akcie;
- ...

Právní předpisy:

- Ochrana osobních údajů;
- Ochrana údajů;
- Zpoždění při přizpůsobování zákonů technologické realitě;
- Jednání na místě činu;
- Analýza a zpracování dat;
- ...

Zdroje:

- Nárůst objemu dat;
- Složitost distribuovaných systémů pro ukládání dat;

- ...

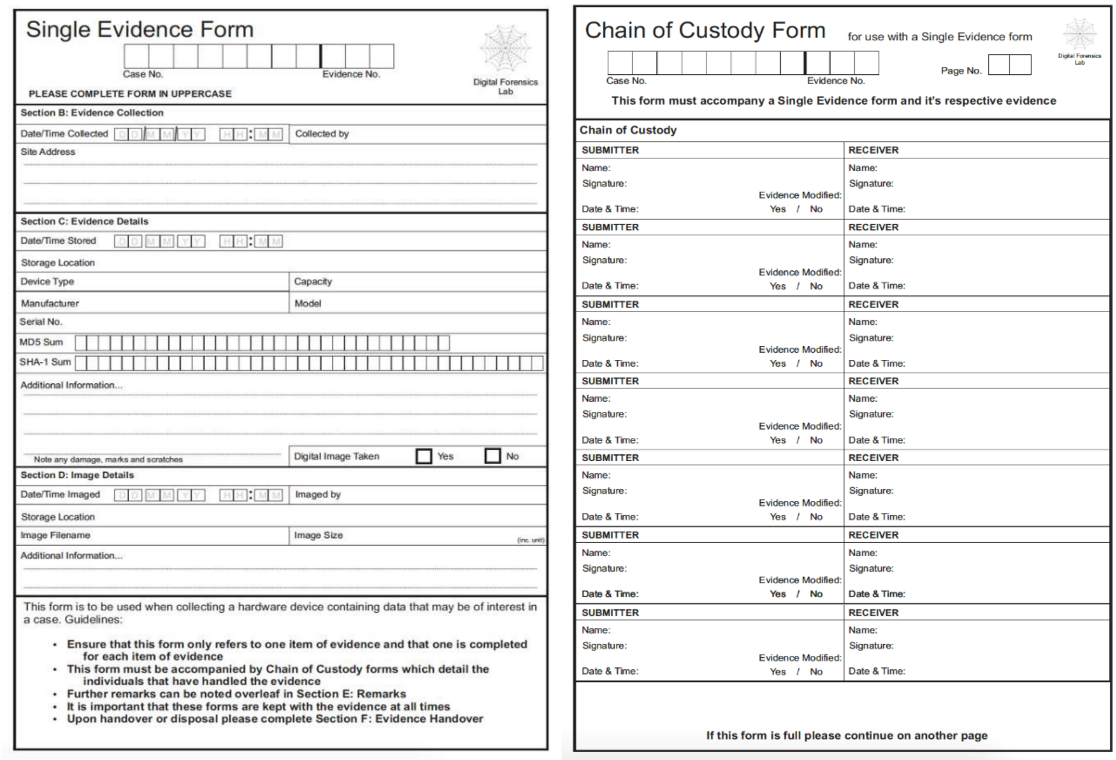
1.4. Mezinárodní standardy

Subjektů, které usilují o vypracování příruček správné praxe v oblasti digitální forenziky, je celá řada, a my se odvoláváme na ISO/IEC, NIST, ENISA, SANS a další, kteří se snaží šířit a rozvíjet znalosti v této oblasti. Existuje tedy několik důležitých dokumentů v oblasti rozvoje funkcí digitálního forenzního experta, a to např:

- **RFC 3227:2002** Příručka pro získávání a uchovávání digitálních důkazů
- **NIST 800-86** Příručka pro začlenění forenzních technik do reakce na incidenty
- **NIST 800-144** Průvodce bezpečností a ochranou soukromí v cloudu
- **NIST 800-101** Průvodce forenzní analýzou mobilních zařízení
- **ISO/IEC 20000-1:2018** Informační technologie - Řízení služeb
- **ISO/IEC 27001:2013** Definice systému řízení bezpečnosti informací (ISMS)
- **ISO/IEC 27002:2013** Průvodce správnou praxí v oblasti bezpečnosti informací
- **ISO/IEC 27005:2018** Řízení rizik bezpečnosti informací
- **ISO/IEC 27032:2012** Průvodce kybernetickou bezpečností
- **ISO/IEC 27037:2012** Průvodce identifikací, shromažďováním, získáváním a uchováváním digitálních důkazů

1.5. Kontrolní řetězec

Kontrolní řetězec je dokument/formulář, který musí vyplnit osoba, která zařízení zabavuje. Tento dokument musí být vždy přiložen k samotnému vybavení, přičemž se uchovává datovaný záznam o všech osobách, které měly vybavení v péči. Příklad řetězce úschovy je uveden (Obrázek 3 - Digitální forenzní laboratoř).



Single Evidence Form

Case No. Evidence No.

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected | Collected by

Site Address

Section C: Evidence Details

Date/Time Stored

Storage Location

Device Type | Capacity

Manufacturer | Model

Serial No.

MD5 Sum

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches | Digital Image Taken Yes No

Section D: Image Details

Date/Time Imaged | Imaged by

Storage Location

Image Filename | Image Size (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence
- This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence
- Further remarks can be noted overleaf in Section E: Remarks
- It is important that these forms are kept with the evidence at all times
- Upon handover or disposal please complete Section F: Evidence Handover

Chain of Custody Form for use with a Single Evidence form

Case No. Evidence No. Page No.

Digital Forensics Lab

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:

If this form is full please continue on another page

Obrázek 3 - Formulář kontrolního řetězce

Zdroj:
https://www.dfir.training/index.php?option=com_jreviews&format=ajax&url=media/download&m=wx99T&1661384494937

1.6.Procesní modely ve forenzní analýze

Každý forenzní vyšetřovatel má v průběhu forenzní analýzy vlastní pracovní metodu a metodiku a pro každý typ vyšetřování neexistuje standardní model, který se obvykle řídí dosavadními zkušenostmi každého vyšetřovatele.

V průběhu času se objevily různé metodiky, které definují potřebu posloupnosti obecných kroků při forenzním vyšetřování, obvykle definovaných jako "shromažďování, uchovávání nebo zkoumání důkazů, analýza".

Bylo navrženo několik modelů vyšetřování, nazývaných také " Digital Forensics Investigation Frameworks "(Obrázek 4), přičemž tyto modely patří k nejoblíbenějším:

- Model DFRWS - Digital Forensic Research Workshop (Palmer et al. 2001)
- ADFM - Abstraktní digitální forenzní model (Reith et al. 2002)
- IDIP - Integrated Digital Investigation Process (Carrier et al. 2003)
- EIDIP - Enhanced Integrated Digital Investigation Process (Baryamureeba & Tushabe 2004)
- CFFTPM - Computer Forensics Field Triage Process Model (Rogers et al. 2006)
- SRDFIM - Systematický model digitálního forenzního vyšetřování (Agarwal et al. 2011)
- IDFPM - Integrovaný model digitálního forenzního procesu (Kohn et al. 2013)
- EDRM - Referenční model pro elektronické vyhledávání (https://edrm.net, 2014)

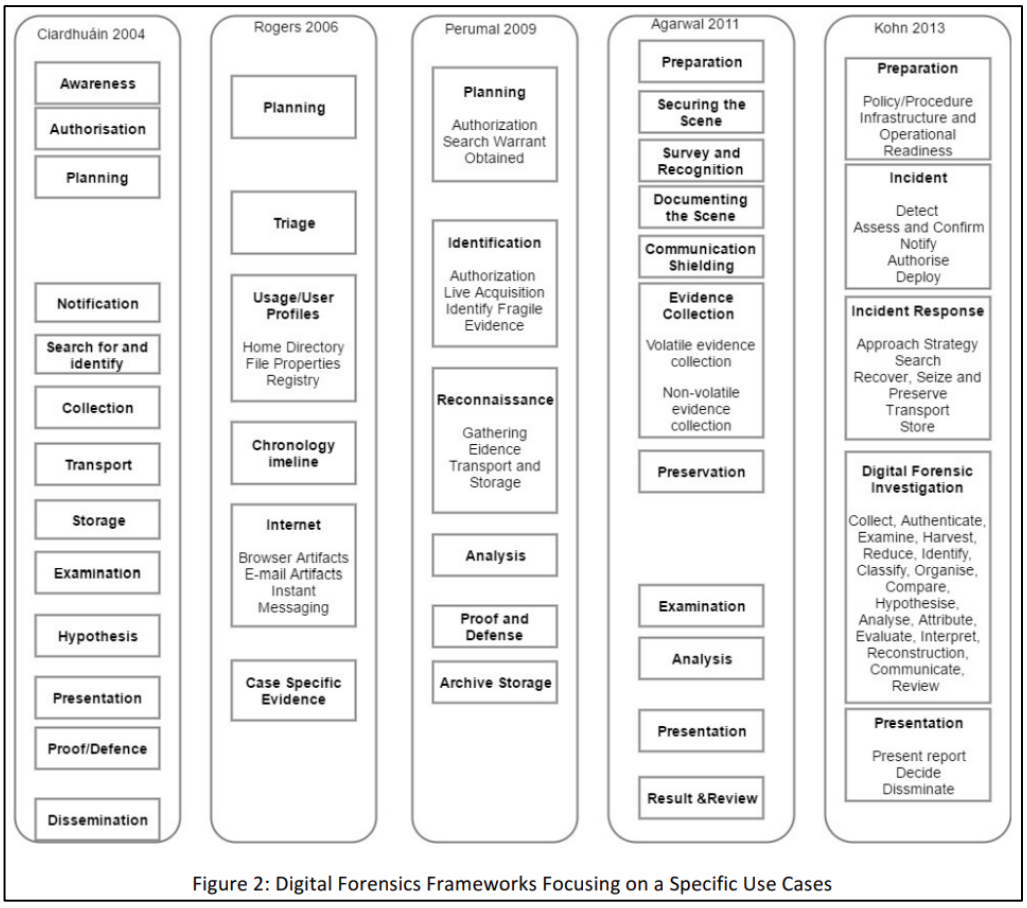
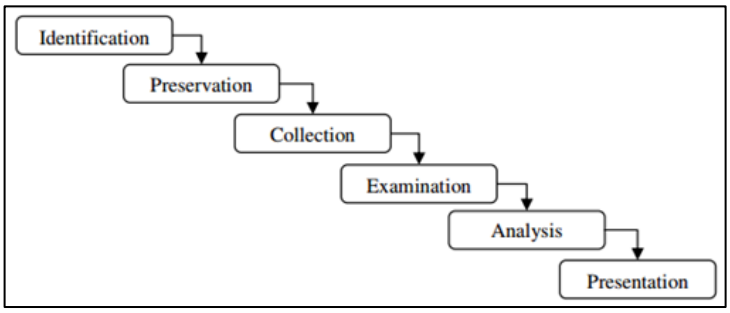


Figure 2: Digital Forensics Frameworks Focusing on a Specific Use Cases

Obrázek 4 - Rámce digitálního forenzního vyšetřování

Zdroj: Obrázek 2 v článku https://arxiv.org/ftp/arxiv/papers/1708/1708.01730.pdf

V roce 2001 byl v rámci výzkumu, který vzešel z digitálních výzkumných seminářů, navržen šestistupňový rámec, jak je znázorněno na obrázku 5.



Obrázek 5 - Rámec DFRWS

To je dodnes jedna z hlavních metodik digitálního forenzního vyšetřování, kterou se budeme řídit. Jednotlivé fáze jsou popsány níže:

Identifikace - kdy výzkumník musí identifikovat všechny relevantní informace a definovat strategii pro jejich získání. Výzkumník může mít co do činění s typickým paměťovým zařízením, jako je pevný disk, paměťová karta, nebo jinak může být třeba shromáždit digitální data z dat o

síťovém provozu, nestálých dat, jako jsou data z paměti, mobilních zařízení nebo zařízení internetu věcí, nebo jakéhokoli jiného zařízení pro ukládání digitálních dat. V této fázi je nesmírně důležitá příprava před použitím technik a nástrojů, aby byla zajištěna pravost, integrita a nezpochybnitelnost všech důkazů u soudu.

Uchovávání - Tato fáze zahrnuje úkoly, jako je nastavení řádného řízení případu a zajištění přijatelného řetězce úschovy u soudu. Tato fáze má zásadní význam pro zajištění toho, aby byly údaje shromážděny bez vnější kontaminace a správně analyzovány.

Shromáždění - Tento krok se týká získání digitálních důkazů a tradičně se provádí klonováním nebo forenzním zobrazením paměťového zařízení. Získání nestálých dat nebo jiných relevantních a nestálých dat může být pro fázi vyšetřování rozhodující, zejména pokud jsou data týkající se získaného úložiště zašifrována. Data získaná v této fázi jsou vstupními daty nebo zdrojem dat pro fázi analýzy.

Zkoumání - Jedná se o fázi vyhledávání požadovaných dat, která zahrnuje mimo jiné techniky vyhledávání, obnovu smazaných dat, dešifrování dat, prolomení hesla, analýzu škodlivého softwaru, analýzu vzorů. Tato fáze je propojena s fází analýzy, neboť například po identifikaci dokumentů bude nutné provést jejich analýzu s přihlédnutím k odpovědím na požadované otázky.

Analýza - analýza všech shromážděných údajů. Tato fáze je časově nejnáročnější, protože je třeba provést důkladnou rešerši a identifikovat všechny relevantní artefakty. Ve většině případů je běžné, že shromážděná data mají podobu nestrukturovaných dat, což vyžaduje specifické nástroje a časově náročnější analýzu k identifikaci potenciálních dat digitálních důkazů, kde jsou zahrnuta strukturovaná data, jako jsou záznamy, databáze, datové soubory, systémové soubory, webové stránky a další.

Prezentace - Jedná se o poslední fázi procesu digitální forenzní analýzy, kdy je soudci předložena závěrečná zpráva se všemi relevantními údaji. Tato zpráva by měla být předložena v tištěné podobě se všemi artefakty, které jsou považovány za důležité. V případě pochybností o informacích uvedených v předložené zprávě je nutné, aby znalec při výpovědi u soudu poskytl příslušná vysvětlení.

2.

Uchovávání a shromažďování digitálních důkazů na místě trestného činu/nehody

2. Uchovávání a shromažďování digitálních důkazů na místě trestného činu/nehody

Aby byla analýza provedena v co nejlepším stavu, je nutné, aby byla správně provedena i konzervace a sběr. V této části budeme k úkonům na místě incidentu přistupovat stejně jako k úkonům na místě činu, protože v obou případech jsou zřejmé podobnosti, ale každý z nich bude mít nutně svá specifika a specifické rysy, které zde nebudeme zobrazovat.

INCIDENT

"Počítačový incident je přerušení nebo porucha kvality služby informačních technologií" Zdroj: Příručka "ITIL V3 - Provoz služeb" (OGC, 2007)

Aby došlo k incidentu, musí nutně dojít k narušení dostupnosti, pravosti, integrity a/nebo důvěrnosti údajů.

Právě sítě CSIRT (Computer Security Incident Response Team) umožňují shromažďovat údaje o počítačových incidentech, k čemuž vyvinuly společnou taxonomii (zdroj: https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf) klasifikace incidentů, která je rozděluje podle dvou vektorů, podle typu incidentu a podle typu události.

Agentura ENISA rovněž rozvíjí a podporuje znalosti o osvědčených postupech při identifikaci a řízení incidentů a pravidelně na toto téma publikuje (viz https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection).

Agentura ENISA v roce 2010 zveřejnila dokument "Incident Management Guide" (https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management), v němž klasifikuje incidenty do kategorií podle stupně jejich závažnosti, jak je uvedeno na obrázku 6.

Group	Severity	Examples
RED	Very High	DDoS, phishing site
YELLOW	High	Trojan distribution, unauthorised modification of information
ORANGE	Normal	Spam, copyright issue

Obrázek 6 - Klasifikace událostí

Zdroj: Průvodce řízením incidentů (ENISA 2010)

2.1. Mezinárodní standardy pro reakci na incidenty

Subjektů, které se snaží vypracovat příručky správné praxe v oblasti reakce na incidenty, je celá řada, nicméně našimi referencemi jsou ISSO/IEC, NIST a ENISA. Existuje tedy několik důležitých dokumentů v oblasti vývoje funkcí digitálního forenzního experta, a to např:

- **Příručka pro řízení incidentů** (ENISA 2010)
- **ISO/IEC 27035:2016** Průvodce řízením incidentů v oblasti bezpečnosti informací pro střední a velké organizace
- **ISO/IEC 27037:2012** Průvodce identifikací, shromažďováním, získáváním a uchováváním digitálních důkazů
- **NIST 800-86** Příručka pro začlenění forenzních technik do reakce na incidenty
- **NIST IR 8796** Bezpečnostní analýza mobilních zařízení a nositelných zařízení pro první pomoc
- **ISO/IEC 27001:2013** Definice systému řízení bezpečnosti informací (ISMS)
- **ISO/IEC 27002:2013** Průvodce správnou praxí v oblasti bezpečnosti informací
- **ISO/IEC 27005:2018** Řízení rizik bezpečnosti informací
- **ISO/IEC 27032:2012** Průvodce kybernetickou bezpečností

Norma ISO/IEC 27002 - Řízení incidentů bezpečnosti informací definuje rozdíl mezi **událostí** a **incidentem,** kdy událost nemusí vždy vést k incidentu, ale incident vždy vede k události.

2.2.Řízení incidentů a zmírňování jejich následků

Norma ISO/IEC 27035 definuje 5 kroků při řízení a zmírňování incidentů, a to:

1. Příprava a plánování
2. Detekce a záznam
3. Posuzování a rozhodování
4. Reakce
5. Získané zkušenosti

1.Příprava a plánování je fáze identifikace všech kritických aktiv instituce, interních procesů pro přístup k informacím, vytvoření monitorovacích systémů, které umožňují identifikaci incidentů, a také všech odpovědností a postupů v případě incidentu.

Příprava

- Příprava digitální laboratoře
- Definice vedoucího týmu
- Definování členů týmu a odpovědností
- Příprava briefingu / intervenční strategie

Briefing

- Strategie zásahu?

- Potřebné vybavení na místo události?
- Jaký typ metod (nástrojů) sběru/získávání?
- Jaká je síťová aktivita?
- Volatilita shromážděných údajů?
- Mohlo být zařízení nastaveno tak, aby zničilo důkazy?
- Jak budeme digitální důkazy uchovávat/přepravovat?
- Související vybavení, příručky atd. ?
- Identifikovat možné střety zájmů?
- Hodnocení rizik

2. Detekce a záznam je nutně fází identifikace událostí a rozlišení události nebo po sobě jdoucích událostí a možného incidentu .

Podobně jako na jakémkoli jiném místě činu, protože incident mohl být záměrně vyprovokován interním zaměstnancem organizace. Takto bychom měli vzít v úvahu předchozí přípravu k jednání podle následujících bodů:

- Zajištění místa činu
- Shromažďování předběžných informací
- Dokumentace místa činu
- Shromažďování a uchovávání důkazů
- Balení a přeprava
- Kontrolní řetězec

Mělo by být provedeno maximální možné **shromáždění informací, které** odpovídají typu možné události, aby bylo možné účinně rozhodovat. Tímto způsobem bychom měli vzít v úvahu všechny typy informací, které lze získat, jako např:

- Typ připojení (Wi-Fi/Ethernet)
- Které počítače se používají k připojení k internetu?
- Umístění systémů a určení, kdo k nim má přístup
- Podrobnosti o vyměnitelných zařízeních a vlastnostech uživatele
- Získání podrobností o topologii sítě
- Získat podrobnosti o dalších periferních zařízeních připojených k počítači.
- Existují nějaké další otázky k tomuto tématu, které nebyly zodpovězeny?

Z těchto informací bychom měli vzít v úvahu okolní informace, jako např.:

- Jaké služby organizace nabízí?
- Koho se tyto události týkají? Byli informováni?
- Existují logická ochranná opatření (antivirus, firewall, IDS, IPS)? Alarmy?
- Jaká jsou zavedena opatření fyzické bezpečnosti?
- Existují záznamy z kamerového systému
- Určete počet počítačů a počítačů připojených k internetu.
- Zkontrolujte nejnovější výměny hardwaru
- Úroveň přístupu zaměstnanců? Nedávné propouštění?
- Úrovně přístupu pro správu/administrátora?
- Bezpečnostní zásady organizace?

- Postupy pro zvládnutí incidentu?
- Seznam podezřelých? Proč jsou podezřelí?
- Systémové protokoly? Síťové protokoly? Něco podezřelého?
- Používání systému po incidentu? Příkazy CMD/příkazy prostředí Shell? Skripty? Úlohy? Procesy?
- Postupy analýzy po nehodě?

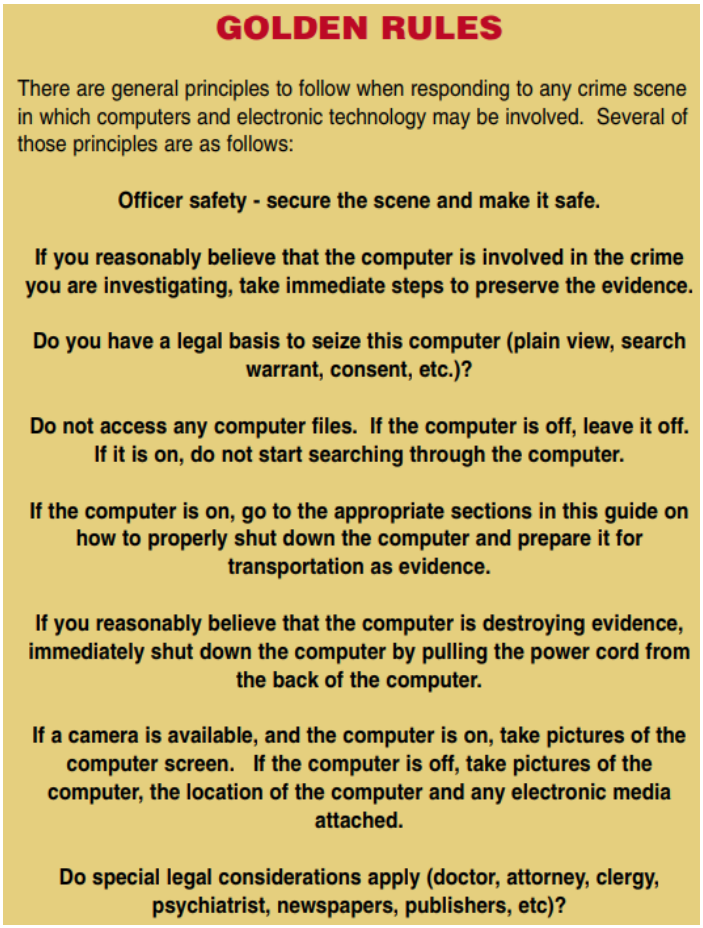
Tým pro reakci na incident by měl vzít v úvahu sběr nestálých dat, která jsou případně rozhodující pro rychlé rozhodování o všech minulých událostech. Proto je důležité jednat různými způsoby podle toho, zda je počítač zapnutý, nebo vypnutý (Obrázek 7).

Jak najít počítač?

Obrázek 7 - první akce

Osoba, která reaguje jako první, musí mít odpovídající oprávnění a odborné znalosti, aby mohla jednat.

Ministerstvo vnitřní bezpečnosti USA vydalo krátkou příručku pro první zásahové jednotky s názvem "Nejlepší postupy pro zajištění elektronických důkazů", která obsahuje tzv. zlatá pravidla, jež jsou uvedena v kapitole "Nejlepší postupy pro zajištění elektronických důkazů". Obrázek 8.

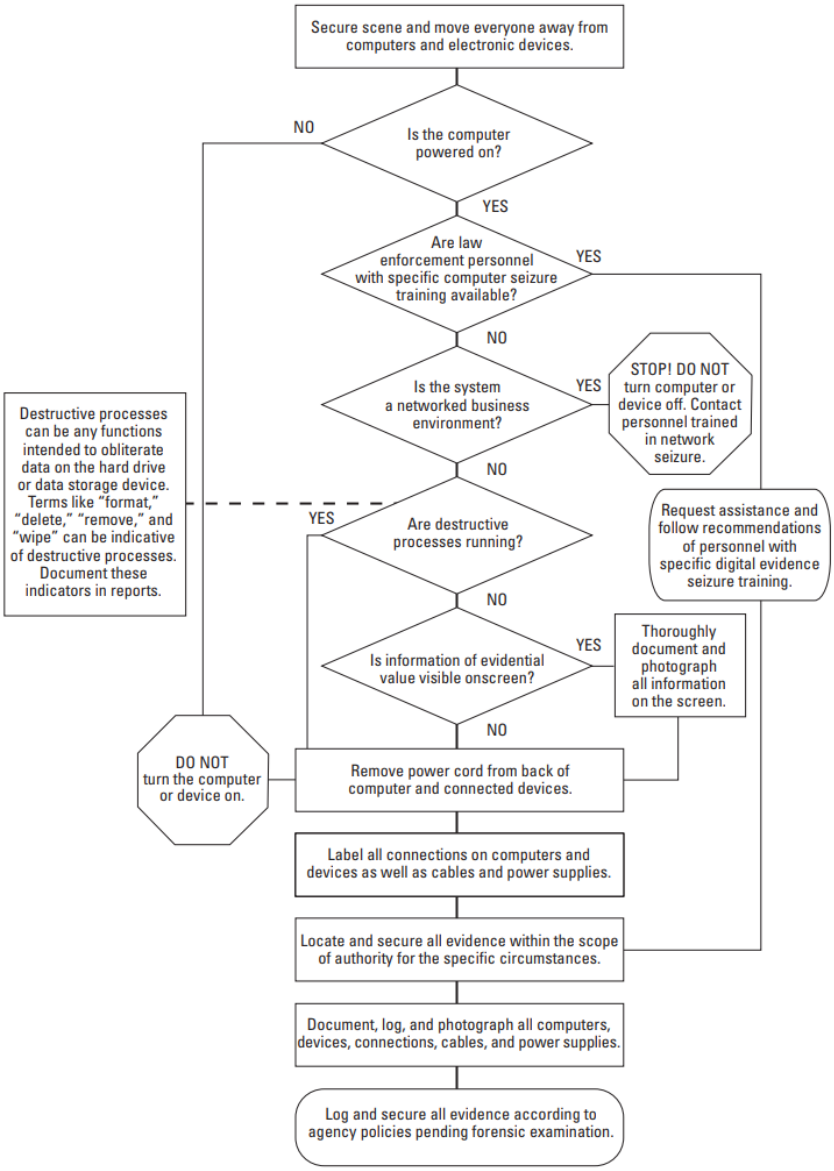


Obrázek 8 - Osvědčené postupy pro zajištění elektronických důkazů

Zdroj: https://www.crime-scene-investigator.net/SeizingElectronicEvidence.pdf

Tato pravidla jsou v současné době platná a měla by být dodržována při reakci na bezpečnostní incidenty.

Ministerstvo spravedlnosti USA - Národní institut spravedlnosti zase zveřejnil vývojový diagram shrnující proces přístupu k zařízením pod názvem "Collecting Digital Evidence Flow Chart" ("Vývojový diagram sběru digitálních důkazů").Obrázek 9).



Obrázek 9 - Vývojový diagram shromažďování digitálních důkazů

Zdroj: Zdroj: Vývojový diagram sběru digitálních důkazů. Ministerstvo spravedlnosti USA - Národní institut spravedlnosti (2010).

V tomto ohledu můžeme stanovit následující postupy:

1. Zajištění fyzické a elektronické bezpečnosti.
2. Pokud je počítač vypnutý:

- Ujistěte se, že se nezapíná (odpojte napájecí kabel/vyjměte baterii, pokud existuje).
- Označení/fotografie všech součástí a periferií
- Identifikace úložných zařízení
- Kontrola dat/času systému BIOS (bez pevného disku)

3. Pokud je počítač zapnutý:

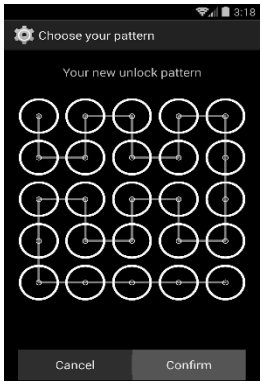
- Odpojení komunikace (odpojení síťového kabelu/vyjmutí karty SIM)

- Vyfotografujte obrazovku a veškerý její obsah (popište viditelný obsah).
- Pokud je potřeba shromažďovat těkavá a netěkavá data:
- Proveďte sběr dat v režimu Live (podle pořadí volatility).
- Zkontrolujte, zda jsou úložná zařízení zašifrována
- Odpojte počítač od zdroje napájení
- Označování/fotografování všech součástí a periferií
- Identifikace úložných zařízení
- Kontrola data/času systému BIOS (bez pevného disku)

4. Pokud se jedná o mobilní zařízení (smartphone/tablet):

- Pokud je přístroj vypnutý, nezapínejte jej.
- Pokud je zařízení zapnuté :
- Vyfotografujte displej (je-li k dispozici)
- Převedení do letového režimu
- Vždy se ujistěte, že zařízení připojené k baterii má dostatečné napájení, aby bylo aktivní až do analýzy.
- Použití Faradayova vaku (Obrázek 10)
- Označení/fotografie všech součástí
- Shromážděte všechna další paměťová zařízení (paměťové karty, karty SIM atd.).
- Zdokumentujte všechny kroky spojené se zabavením mobilního zařízení.
- Dotaz na přístupové kódy (PIN/vzor), PIN ke kartě SIM a kódy PUK (zkontrolujte pouzdra zařízení - obrázek 11).

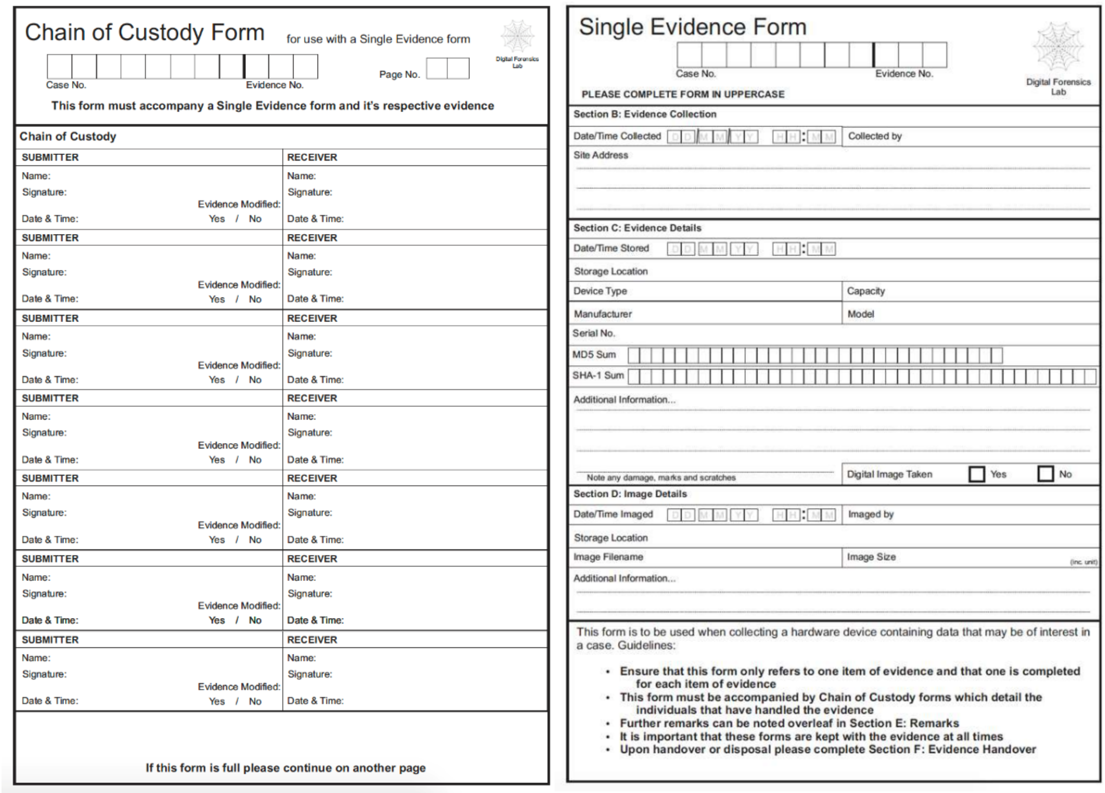
Obr. 10 - Faradayova vrouska



Obrázek 11 - Standardní kód

Jak skladovat a přepravovat?

- Používejte rukavice
- Nezakrývejte identifikační údaje
- Digitální důkazy s otvory a pohyblivými součástmi by měly být zapečetěny pečetěmi nebo páskou proti neoprávněné manipulaci.
- Zařízení by měla být uložena ve statickém rozptylovém a Faradayově vaku.
- Dokument
- Zdokumentujte v řádné zprávě a podepište ji všichni zúčastnění.
- Vyplňte řetězec kontroly zařízení ("Chain of Custody").Obrázek 12)



Chain of Custody Form — for use with a Single Evidence form

Case No. — Evidence No. — Page No.

Digital Forensics Lab

This form must accompany a Single Evidence form and it's respective evidence

Chain of Custody

SUBMITTER	RECEIVER
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:
Name: Signature: Evidence Modified: Date & Time: Yes / No	Name: Signature: Date & Time:

If this form is full please continue on another page

Single Evidence Form

Case No. — Evidence No.

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected DD MM YY HH:MM — Collected by

Site Address

Section C: Evidence Details

Date/Time Stored DD MM YY HH:MM

Storage Location

Device Type — Capacity

Manufacturer — Model

Serial No.

MD5 Sum

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches — Digital Image Taken ☐ Yes ☐ No

Section D: Image Details

Date/Time Imaged DD MM YY HH:MM — Imaged by

Storage Location

Image Filename — Image Size (inc. unit)

Additional Information...

This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines:

- **Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence**
- **This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence**
- **Further remarks can be noted overleaf in Section E: Remarks**
- **It is important that these forms are kept with the evidence at all times**
- **Upon handover or disposal please complete Section F: Evidence Handover**

Obrázek 12 - Kontrolní řetězec

Zdroj:
https://www.dfir.training/index.php?option=com_jreviews&format=ajax&url=media/download&m=wx99T&1661384494937

3. Vyhodnocení a rozhodnutí je fáze po zjištění existence možného incidentu, kdy se shromažďují všechny užitečné informace o tom, co se stalo, a která vede k rozhodnutí o potvrzení bezpečnostního incidentu IT. Po tomto potvrzení je třeba rychle reagovat, aby se zmírnil dopad incident a aby se vyřešil.

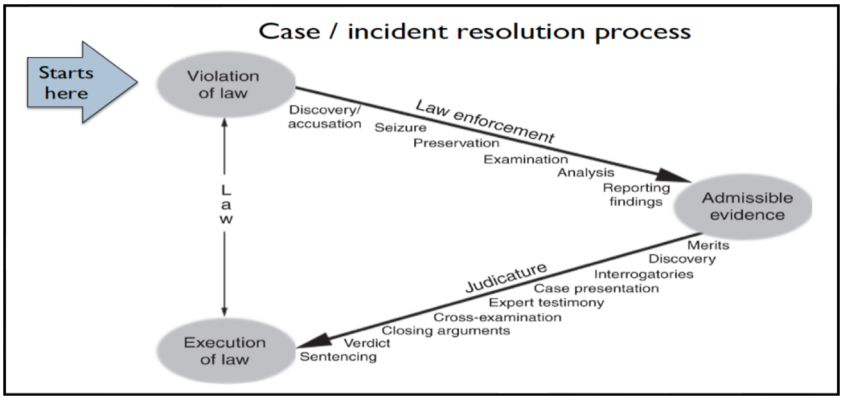
4. Reakce je fáze, kdy se incident klasifikuje v souladu s klasifikací definovanou ve fázi 1, kategorizuje se incident a klasifikuje se jeho závažnost, provádějí se nezbytné postupy pro jeho zmírnění a řešení, využívají se mechanismy krizového řízení a incident se hlásí příslušným orgánům, kterými jsou v portugalském případě soudní policie (PJ), Národní centrum kybernetické bezpečnosti (CNCS) a Národní komise pro ochranu údajů (CNPD).

5. Získané zkušenosti jsou jednou z nejpotřebnějších fází, protože umožňují zavést opatření, aby se podobný incident neopakoval, a také využít získané poznatky ke zlepšení bezpečnostního systému organizace.

Viz: https://www.cncs.gov.pt/certpt/coordenacao-da-resposta-a-incidents/

2.3. Vztah mezi procesem řešení incidentů a forenzní výpočetní technikou

Tyto postupy se týkají digitální forenzní analýzy (Obrázek 13) vždy, když je zjištěn incident a my se o něm chceme dozvědět více ve snaze postavit pachatele před soud. V procesu řízení incidentů tedy máme stejný postup vyšetřování, který je uveden v části 1.6, pokud jde o 6 kroků rámce analýzy.



Obrázek 13 - Proces řešení incidentu

Zdroj: http://www.c-jump.com/bcc/t155t/Week03a/W24_0030_overview_of_caseinci.htm

3.

Postupy získávání digitálních důkazů

3. Postupy pro získávání digitálních důkazů

Počítačová kriminalistika je proces získávání, analýzy a uchovávání digitálních důkazů za použití standardizovaných postupů, které umožňují zachování integrity obrazu důkazů.

Je proto nutné zajistit, aby forenzní pořízení paměťových zařízení probíhalo v souladu s mezinárodně uznávanými osvědčenými postupy, přičemž jedním z nich je předchozí sterilizace pevného disku, na který bude kopie dat uložena, jak je popsáno v následujícím bodě.

3.1.Sterilizační postup

Sterilizační postupy mají zajistit, aby naše cílové zařízení bylo připraveno přijímat původní informace. Cílem sterilizace je zapsat všechny bity našeho sběrného disku hodnotou 0 (nula), čímž se zajistí, že na něm nejsou žádné předchozí informace.

Po sterilizaci je vždy nutné provést validaci a zkontrolovat, zda sterilizace proběhla správným způsobem. Po této validaci můžeme přistoupit k formátování disku na vhodný souborový systém.

Existuje mnoho softwaru, který umožňuje provádět tyto postupy sterilizace disku a jeho formátování na požadovaný souborový systém. Zde si ukážeme postup pomocí nástrojů, které jsou přítomny ve většině linuxových distribucí, lsblk,fdisk a dc3dd.

Prvním krokem je identifikace sterilizovaného disku. Je velmi důležité, aby tato identifikace byla jednoznačná a byla potvrzena tolikrát, kolikrát je třeba. Sterilizovaný disk nelze obnovit.

3.1.1. Identifikace zařízení

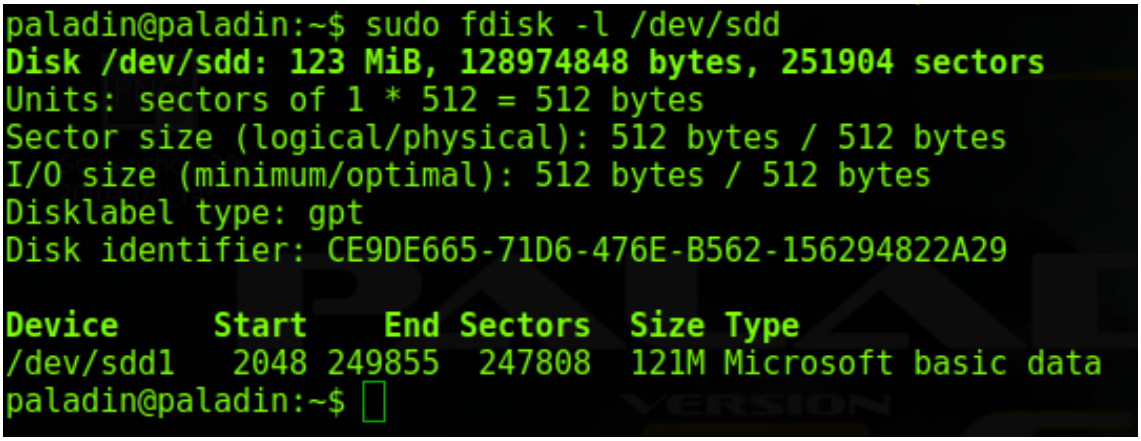
Identifikace zařízení se provádí pomocí řady příkazů. Nejprve je nutné určit, které svazky jsou v počítači nainstalovány a které se mají použít. Dobrou praxí je použít počítač s připojeným pouze sterilizovaným diskem a spustit operační systém z liveCD nebo USB flash disku. Tím se sníží možnost chyb při identifikaci disku:

```
$ lsblk | grep sd*
```

Tento příkaz zobrazí seznam všech úložných zařízení rozpoznaných operačním systémem. Zobrazí se všechny disky, jejich velikost a oddíly. Tento příkaz nám pouze pomůže zjistit, jak se jmenuje náš disk v počítači.

V případě pochybností můžeme ještě použít příkaz (Obrázek 14)

```
fdisk -l /dev/sd*
```



Obrázek 14 - identifikace zařízení

Tento příkaz nám poskytne více informací o požadovaném disku.

3.1.2. Sterilizace cílového disku

Proces sterilizace není nic jiného než zápis celého disku s hodnotou 0 (nula), tj. donutí všechny bity pevného disku nabýt hodnoty nula.

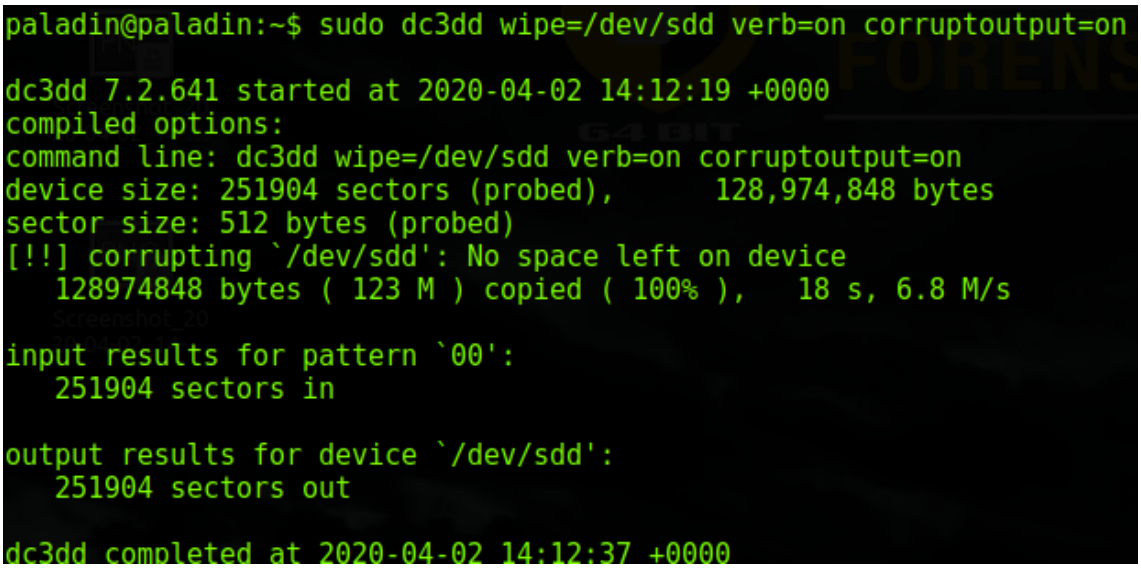
K tomuto úkolu můžete použít nástroje jako Live-CD DBAN (www.dban.org) nebo v systému Windows Eraser (eraser.heidi.ie).

V Linuxu můžete použít příkazy (Obrázek 15)

dc3dd wipe=/dev/sdd verb=on corruptoutput=on

nebo

dcfldd if=/dev/zero of=/dev/sdb bs=8k conv=noerror,sync



Obrázek 15 - Sterilizace cílového disku

Tento příkaz provede zápis všech bitů pevného disku, takže bude trvat tím déle, čím větší je pevný disk. V našem příkladu trval zápis na zařízení o velikosti pouhých 123 MB 18 sekund, avšak na pevný disk o velikosti 1 TB může zápis trvat i více než 8 hodin. Je také důležité poznamenat, že v závislosti na technologii pevného disku může být tato doba vyšší nebo nižší, v závislosti na jeho rychlosti zápisu.

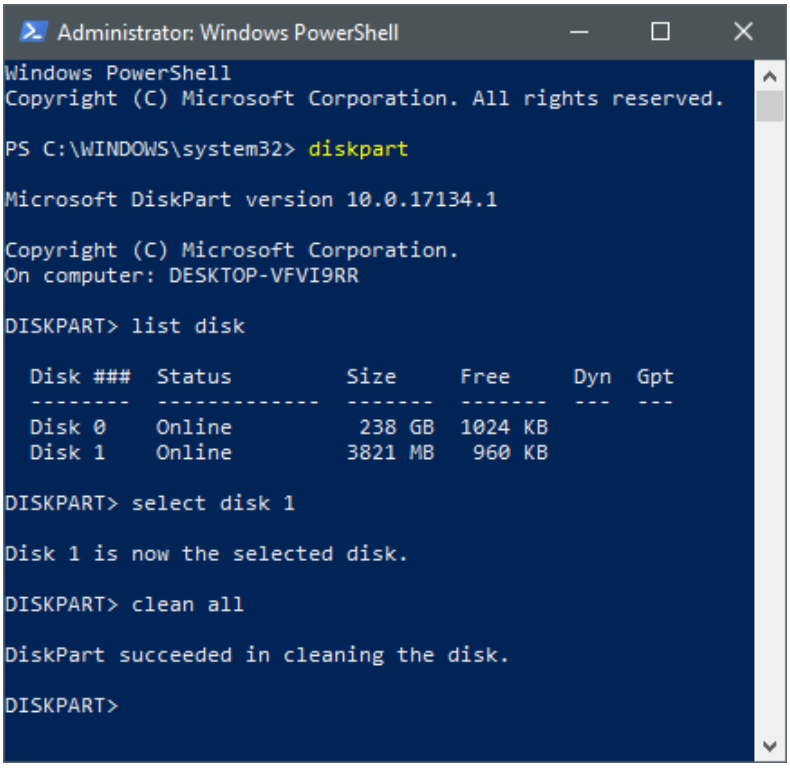
V systému Microsoft Windows lze sterilizaci cílového disku provést pomocí příkazu diskpart.

Provedení identifikace cílového disku pomocí:

LIST DISK (identifikace zařízení) **LIST VOLUME** (identifikace svazku) **SELECT DISK 1** (vyberte disk, který se má sterilizovat)

Provedení sterilizace (Obrázek 16)

ČIŠTĚNÍ VŠEHO



Obrázek 16 - Sterilizace cílového disku pod Windows

3.1.3. Ověření sterilizace

Nakonec je důležité ověřit, zda byl zápis na pevný disk úspěšný, k čemuž provedeme příkaz:

cat /dev/sdb |od

Pokud byl zápis úspěšný, bude výstupem příkazu 0000000, což znamená, že na pevný disk jsou zapsány pouze nuly (Obrázek 17).

```
paladin@paladin:~$ sudo cat /dev/sdd |od
0000000 000000 000000 000000 000000 000000 000000 000000 000000
*
754000000
```

Obrázek 17 - ověření sterilizace

Příkaz "cat" zobrazí obsah zařízení, zatímco argument "|od" převede tento obsah na osmičkovou bázi, takže v případě úspěšné sterilizace budou zobrazeny pouze nuly.

Kromě uvedených postupů lze použít i další metody a různé příkazy, například zobrazení v hexadecimálním formátu nebo jiné.

3.1.4. Formátování

Po sterilizaci je nutné disk naformátovat, aby mohl přijímat data.

Toto formátování lze stále provádět pomocí nástroje Diskpart, a to následujícím způsobem:

Vytvoření primárního oddílu (Obrázek 18)

```
DISKPART> create partition primary

DiskPart succeeded in creating the specified partition.
```

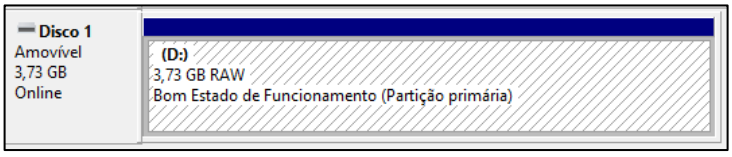
Obrázek 18 - Vytvoření primárního oddílu

Formátování NTFS (Obrázek 19)

```
DISKPART> select partition 1

Partition 1 is now the selected partition.

DISKPART> format fs=ntfs quick

  100 percent completed

DiskPart successfully formatted the volume.
```

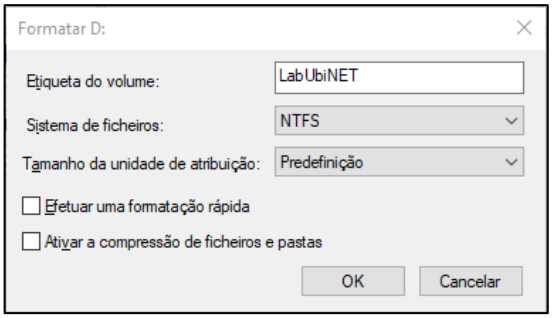
Obrázek 19 - Formátování

V grafickém prostředí lze aplikaci Správa disků používat prostřednictvím příkazu DISKMGMT.MSC (Obrázek 20).



Obrázek 20 - Správa disků

Klikněte pravým tlačítkem myši na požadovaný disk a vyberte možnost "Formátovat", poté zadejte název a požadovaný souborový systém. Lze zvolit rychlé formátování, protože disk byl předtím sterilizován (Obrázek 21).



Obrázek 21 - Formátování pomocí Správy disků

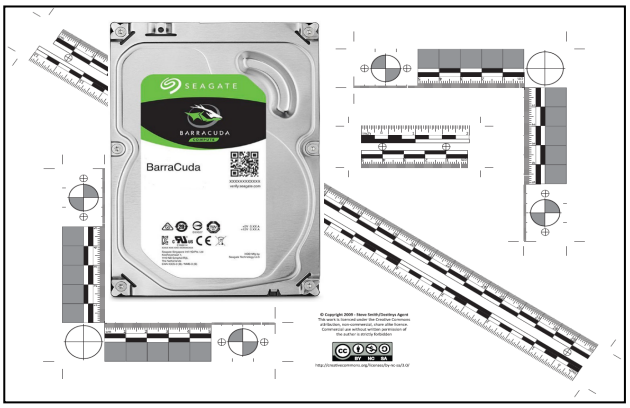
3.2. Identifikace zařízení pro ukládání dat

Paměťová zařízení prošla v posledních letech rychlým vývojem, což vyžaduje, aby forenzní analytik byl pozorný a zkoumal každé analyzované zařízení a snažil se získat informace o všech zařízeních pro ukládání dat, která dané zařízení podporuje. Tímto způsobem může analytik usilovat o identifikaci všech takových zařízení (obrázek 22).

Obrázek 22 - Identifikace úložných zařízení

3.3. Fotografická reportáž

Po identifikaci zařízení a příslušných zařízení pro ukládání dat je důležité zaznamenat jejich aktuální stav. Za tímto účelem přiřaďte každému zařízení interní označení a vyfoťte zařízení z různých úhlů (obrázek 23), použijte metrické měřítko a věnujte zvláštní pozornost jejich případnému poškození. Jedná se o informace, které mohou být důležité u soudu.



Obrázek 23 - fotografická reportáž

3.4. Forenzní distribuce rozsahu

S ohledem na techniky a postupy získávání a analýzy datových úložišť je důležité mít znalosti forenzních distribucí systému Linux. Ty disponují sadou nástrojů, které umožňují získávat a analyzovat informace s ohledem na osvědčené postupy. Jedná se zpravidla o Live distribuce, které není nutné instalovat do počítače, ale které umožňují připojit disky bez obav o blokování zápisu, protože jsou dodávány s nativní konfigurací bez automatického připojování do systému.

Rozdělení, která uvádíme, jsou následující:

- **CAINE (Computer Aided INvestigative Environment Live CD/DVD)**
- **DFF (Digital Forensics Framework)**
- **SANS SIFT (Sans Investigative Forensics Toolkit)**
- **Paladin Edge (Sumuri)**

3.5. Akviziční techniky

Postupy získávání jsou rozhodující pro zajištění integrity digitálních důkazů a usnadnění procesu jejich analýzy, neboť jsou jednou z technik používaných v rámci správné praxe v digitální forenzní technice, která zaručuje přípustnost získaných důkazů u soudu.

Pořízení bitové binární kopie zařízení pro ukládání dat nazýváme akvizice a existuje také tzv. forenzní kopie nebo duplikace (obrázek 24).

Obrázek 24 - Duplikátor úložných zařízení

Zdroj: https://security.opentext.com/tableau/hardware/details/td2u

U všech typů forenzních sběrů je důležité mít na paměti, že cílový disk by měl mít větší kapacitu než zdrojový.

3.5.1. Blokátor zápisu

Při akvizičních postupech je třeba použít hardwarové zařízení (obrázek 25), které blokuje zápis na zdrojový disk. Tímto způsobem je zaručena integrita dat na tomto disku, což chrání disk před neúmyslnými změnami, například ze strany operačního systému nebo antivirového programu, a také validace dat kopírovaných na cílový disk.

Obrázek 25 - Blokátor zápisu

Zdroj: www2.guidancesoftware.com

Pokud nemáte přístup k hardwarovému blokátoru zápisu, můžete použít softwarový blokátor zápisu. Ty vyžadují větší pozornost při ověřování jejich správné funkce, protože závisí na operačním systému, který používáme. Některé příklady jsou uvedeny v Obrázek 26.

Obrázek 26 - Forenzní software s blokováním zápisu

Blokování zápisu v operačním systému Microsoft Windows lze provést vytvořením klíče registru.

"HKLM\SYSTEM\ControlSet001\Control\StorageDevicePolicies\WriteProtect", jak je popsáno níže:

- "regedit" v režimu správce a přejděte na následující cestu: **"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control".**
- Vytvořte nový klíč v poli "Control" s názvem: **"StorageDevicePolicies".**
- Přidejte novou hodnotu typu "DWORD (32-bit)" s názvem: **"WriteProtect".**
- Změňte jeho údaje z "**0**" na **"1".**
- Otestujte zámek s několika úložnými zařízeními

3.5.2. Srovnání aplikací pro zadávání veřejných zakázek

Forenzní akviziční postupy je možné provádět v několika operačních systémech, protože existuje více aplikací, které jsou schopny tento úkol provádět, příkladem je aplikace Obrázek 27 porovnání stejných aplikací.

Tool	Platform			Input Sources				Encoding		Output Formats			
				Physical Disk	Logical Volume	Files	Folders	Compression	Encryption	Raw	E01	Ex01	Split
FTK Imager 3.2	✓			✓	✓		✓	✓	✓	✓	✓		✓
FTK Imager CLI 3.1.1	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓
EnCase Forensic Imager 7.0	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
dd		✓	✓	✓	✓	✓	✓			✓			
dcfldd		✓		✓	✓	✓	✓			✓			✓
dd_rescue		✓		✓	✓	✓	✓			✓			
dd.exe	✓			✓	✓	✓	✓	✓	✓	✓			
dc3dd	✓	✓		✓	✓	✓	✓			✓			✓
ewfacquire		✓	✓	✓	✓					✓	✓	✓	✓

Obrázek 27 - Srovnání aplikací pro zadávání veřejných zakázek

Zdroj: Vandeven, Sally, The SANS Institute, 2014

Přečtěte si: https://www.raedts.biz/forensics/forensic-imaging-tools-compared-tested/

3.5.3. Akvizice systému Linux

Akvizici prostřednictvím operačního systému Linux lze mimo jiné provádět pomocí dcfldd nebo dc3dd, aplikací odvozených od známého dd.

Zařízení a jeho tabulka oddílů musí být identifikovány.

```
mmls /dev/sdb
```

Akvizice prostřednictvím dclfdd:

```
dcfldd if=/dev/sdb hash=md5,sha256 hashwindow=10G md5log=md5.txt sha256log=sha256.txt hashconv=after bs=512 conv=noerror,sync split=10G of=diskimage.dd
```

Nebo pořízení prostřednictvím dc3dd:

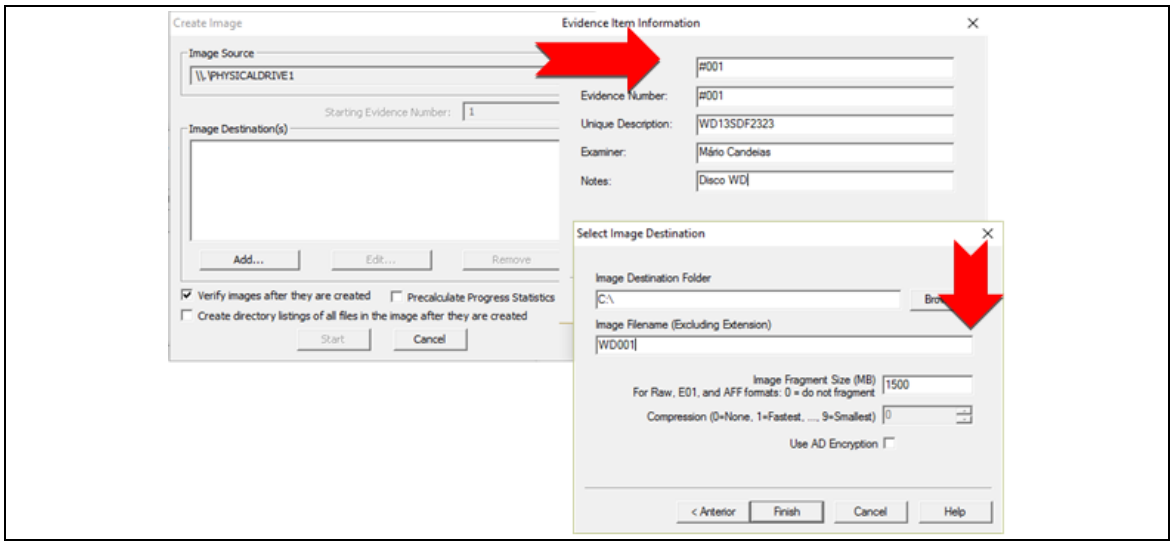
```
dc3dd if=/dev/sdb hash=md5,sha256 hlog=hash_log.log log= diskimage.log rec=off of=diskimage.dd
```

Je třeba zkontrolovat soubory protokolu a zjistit shodu hashů obsahu zdrojového disku s obsahem forenzního obrazu vytvořeného tímto postupem. Důležité je také ověřit nečitelný obsah neboli vadné sektory, které v obou postupech zůstanou bez zapsané hodnoty, takže tento prostor bude mít hodnotu 0 (nula).

3.5.4. Akvizice systému Windows

Snímání prostřednictvím operačního systému MS Windows lze mimo jiné provádět pomocí známé bezplatné aplikace FTK Imager od společnosti Acess Data.

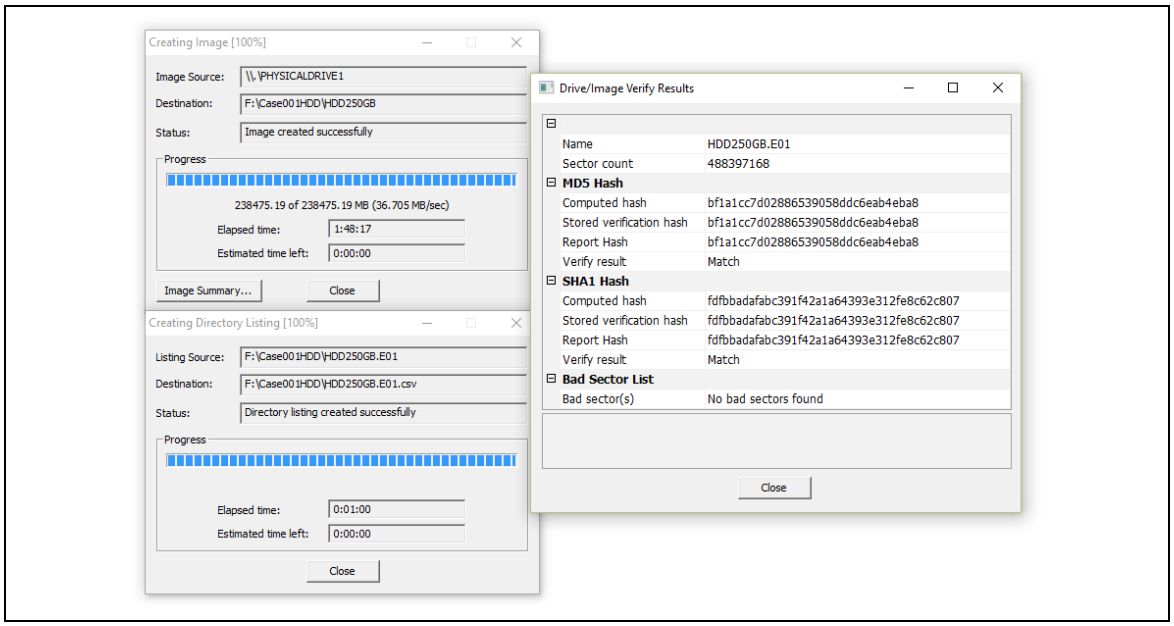
V programu FTK Imager byste měli vybrat možnost Vytvořit obraz disku / Fyzická jednotka, jak je znázorněno na obrázku 1. Obrázek 28.



Obrázek 28 - Postup pořizování snímků pomocí zobrazovací jednotky AccessData FTK

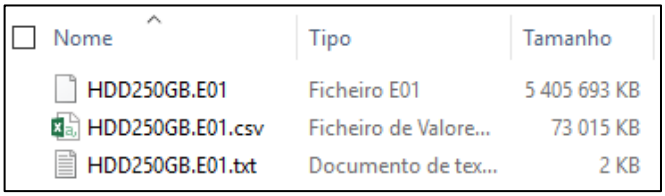
Před zahájením akvizičních postupů je možné zvolit možnost vytvoření seznamu všech souborů, které budou vytvořeny po akvizici a uloženy ve formátu ".csv".

Po spuštění akvizice se zobrazí validační okno s ověřením shody hash a také s informacemi o nepřečtených sektorech, nazývaných také vadné sektory (Obrázek 29).



Obrázek 29 - Výsledek snímání pomocí AccessData FTK Imager

Stejné informace budeme mít také v textovém souboru, který bude uložen na stejném místě jako forenzní obrazový soubor (Obrázek 30). Soubor ".csv" bude také ve stejném umístění, pokud jsme zvolili vytvoření seznamu souborů.



Obrázek 30 - Soubory vzniklé při akvizici pomocí nástroje AccessData FTKImager

4.

Získávání a analýza informací

4. Získávání a analýza efemérních informací

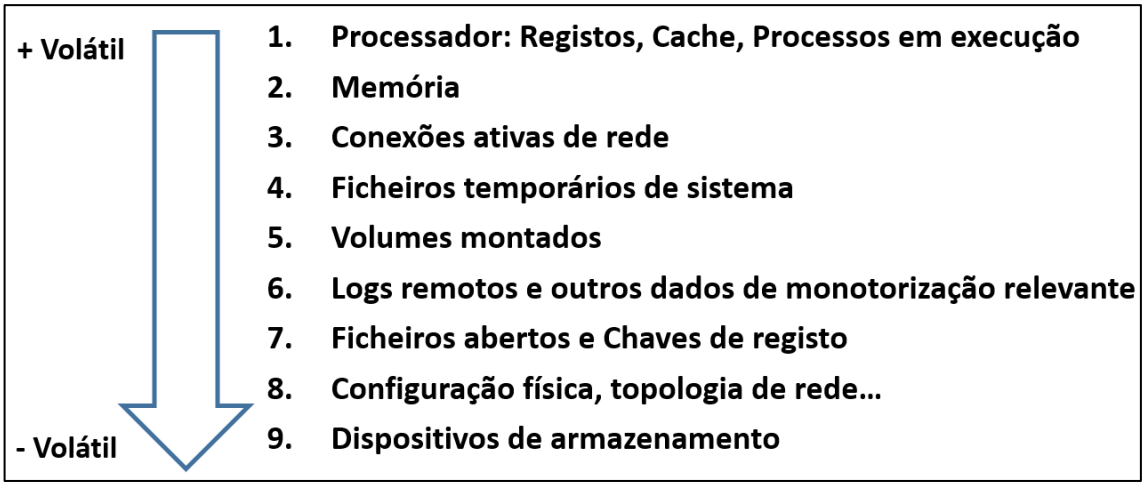
Nestálé informace jsou informace, které se ztratí při vypnutí systému nebo při ztrátě napájení. Těkavé informace se obvykle nacházejí ve fyzické paměti nebo v paměti RAM a skládají se z informací o procesech, síťových připojeních, otevřených souborech, schránce apod. Tyto informace popisují stav systému v daném okamžiku.

Při provádění forenzní analýzy živých dat by měl výzkumník jako jednu z prvních věcí shromáždit obsah paměti RAM. Tím, že se tyto informace shromažďují jako první, se minimalizuje dopad jejich sběru dat na obsah paměti RAM, nicméně toto zachycení může způsobit nestabilitu systému nebo dokonce vést k modré obrazovce smrti (BSoD), což vede některé autory k tomu, že uvádějí, že tyto postupy by se měly provádět až po shromáždění ostatních těkavých informací, přičemž by měly být upřednostňovány podle jednotlivých situací.

Některé konkrétní typy těkavých informací, které by měly být shromažďovány:

- Paměť RAM
- Systémové datum a čas
- Informace o síti
- Přihlášení uživatelé
- Otevřít soubory
- Síťová připojení
- Informace o spuštěných procesech
- Mapování mezi procesy a porty
- Stav sítě
- Obsah schránky
- Informace o službách a řidičích
- Historie provedených příkazů
- Mapované jednotky
- Akcie
- Hesla a kryptografické klíče

Z těchto informací je nutné pro každý konkrétní případ určit, které jsou proměnlivější a které bude důležitější získat jako první. Zde je uvedeno možné pořadí informací podle volatility (Obrázek 31).



Obrázek 31 - Možné pořadí informací podle volatility

4.1. Proces zachycení efemérních informací

V první řadě je nutné zajistit stabilitu našeho pracovního stroje. Jedním z problémů, se kterými se můžeme setkat, je automatické restartování počítače, způsobené automatickými aktualizacemi operačního systému. Proto je vhodné deaktivovat nikoli aktualizace operačního systému, ale jejich schopnost vynutit si restartování stroje. Tento restart by mohl například přerušit pořízení disku nebo analýzu obrazu.

Dalším osvědčeným postupem je zakázat přístup k vyměnitelným diskům pro zápis, čímž se zabrání změně zdrojových disků.

Nestálá data jsou jakákoli data, která mohou být ztracena při vypnutí systému, například záznam o připojení k webové stránce, který je stále přítomen v paměti RAM nebo v systémové schránce. Ke shromažďování těchto dat musí docházet za běhu systému.

Forenzní analýza živých dat je technika používaná ke shromažďování dat, která jsou nestálá a mohou být ztracena, pokud zařízení ztratí napájení.

Memory DUMP je postup ukládání všech dat, která se v daném okamžiku nacházejí ve fyzické paměti počítače, do souboru.

Při shromažďování tohoto typu údajů je nutné zohlednit pořadí nestálosti údajů a přizpůsobit shromažďování té kategorii údajů, která je nejzajímavější. Pokud je naším cílem identifikovat odeslání e-mailu na určitou adresu, nemělo by velký smysl upřednostňovat identifikaci procesů před sběrem hesel, resp. přístupových údajů, které umožňují přístup k e-mailové adrese.

Je velmi důležité, aby byl sběr dat v přímém přenosu řádně zdokumentován, nejlépe vytvořením týmu pro sběr dat složeného alespoň ze dvou osob, aby bylo zajištěno, že postupy sběru provádí jedna osoba a druhá dokumentuje použitý postup sběru.

Důležité je také zaručit minimální změny analyzovaného systému, a pokud je třeba nějakou změnu provést, měla by být zaznamenána ve zprávě pro budoucí paměť.

Doporučení k používání skriptů:

- Použití proměnných prostředí (např.: cmd: %COMPUTERNAME% / PS: $env:Computername)
- Spuštění v režimu správce

4.1.1. Nativní systémové nástroje

Vzhledem k minimální digitální stopě v zařízení bychom měli, kdykoli je to možné, používat forenzní nástroje ke shromažďování užitečných informací, které umožní efektivnější analýzu. Příkladem jsou informace týkající se šifrování celého disku. Operační systém MS Windows však umožňuje spouštění příkazů a skriptů pomocí nativních nástrojů, což je vynikající možnost, jak získat potřebné informace s minimální digitální stopou.

Příkazový řádek	Příkazový řádek systému MS Windows je přirozeně jedním z nejpoužívanějších při shromažďování systémových informací a umožňuje spouštění mnoha programů pro tento účel.	
Instrumentace správy systému Windows (WMI)	Nástroj Windows Management Instrumentation umožňuje přístup k operačnímu systému prostřednictvím příkazového řádku nástroje Windows Management Instrumentation a je vynikajícím způsobem získávání informací o operačním systému.	
Dávkový soubor systému Windows	Jedná se o soubor skriptu, který umožňuje seskupit sadu příkazů po řádcích. Umožňuje použití opakovacích struktur, podmíněných struktur, použití proměnných, typických pro skriptovací jazyk.	
Powershell	PowerShell je v současné době skriptovací jazyk, který byl původně vyvinut pro systémy MS Windows a v roce 2016 byl zpřístupněn jeho otevřený zdrojový kód a podpora různých platforem. Díky vlastnímu shellu byl PowerShell vyvinut tak, aby umožňoval spouštění rutin (cmdlets), přičemž umožňuje i spouštění jiných shellů.	

4.1.2. Externí nástroje

Vzhledem k tomu, že se využívají externí nástroje, je třeba dbát na důkladné otestování každého z těchto nástrojů, aby se přesně vědělo, co v systému dělají. U všech použitých externích nástrojů je třeba uvést datum/čas použití a popsat záměr použití.

Windows Sysinternals	Windows Sysinternals představuje sadu nástrojů původně vytvořenou Markem Russinovichem, která má správcům systému pomoci spravovat a monitorovat systémy Windows. https://docs.microsoft.com/en-us/sysinternals/	Windows Sysinternals
Nirsoft	NirSoft představuje sadu nástrojů vytvořených Nirem Soferem, z nichž vyzdvihujeme ty, které zařadil do kategorie forenzních. http://www.nirsoft.net/	NirSoft Tools and Utilities
Mitec	Společnost Mitec je také web, který nabízí řadu zajímavých nástrojů pro shromažďování a analýzu informací, například MiTeC System Information X a Windows Registry Recovery. https://www.mitec.cz/	MITEC
Zimmerman	Eric Zimmerman vyvinul sadu volně použitelných nástrojů, které mají pomoci při reakci na incidenty a forenzní analýze.	**Eric Zimmerman Nástroje**

4.1.3. Datum, čas a další systémové informace

Tento prvek by měl být při šetření shromažďován jako první. Datum systému umožňuje později shromážděné informace uvést do souvislostí a umožňuje výzkumníkovi sestavit časovou osu událostí, které se odehrály nejen v analyzovaném systému, ale i prostřednictvím korelace informací z jiných systémů. Dalším důležitým údajem je doba, která uplynula od posledního spuštění systému (uptime).

Některé nástroje mohou výzkumníkům v těchto úkolech pomoci, například MiTeC - System Information X[2] a WinAudit[3] .

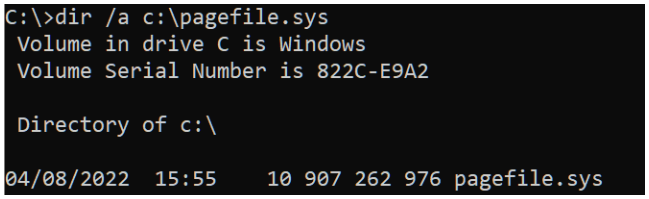
Sběr data/času obsluhovaného systému (Obrázek 32).

```
C:\>echo "the current time is: %date% - %time%" > currentTime.log

C:\>type currentTime.log
"the current time is: 21/03/2019 - 18:38:39,76"
```

Obrázek 32 - Zjištění data a času systému.

Shromažďování data/času posledního spuštění systému (Obrázek 33).

[2] www.mitec.cz/msi.html
[3] www.parmavex.co.uk



Obrázek 33 - Zjištění data a času posledního spuštění systému

Příkazy užitečné pro získávání dat ze systému:

- Verze pro Windows: **ver**
- Proměnné prostředí: **nastavit**
- Systémové informace: **systeminfo /fo list >> C:\tmp\info.txt**
- Přejděte do registru: **reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion" /v ProductName**
- Konzultace z WMI: **wmic os get name, version**
- Spuštění a vypnutí systému: (Fonte: Nirsoft.net)

Příkazy užitečné pro získávání údajů o uživatelích systému

- Uživatelé:
  - **Net User** [uživatelské jméno]
  - **Userprofilesview.exe /shtml "f:\temp\profiles.html" /sort "Jméno uživatele"** (Zdroj: Nirsoft.net)

- Přihlášení uživatelé:
  - **PSLoggedOn.exe** (Zdroj: SysInternals)
  - **LogonSessions.exe** (Zdroj: SysInternals)

4.1.4. Processos e Aplicações

Zásadní je výčet procesů spuštěných v potenciálně napadeném systému. Proces je část nebo instance spuštěné aplikace. Pohled na spuštěné procesy ve Správci úloh poskytuje určité informace, nicméně lze získat mnohem více informací, než je tam vidět.

Některé typy informací o spuštěných procesech, které lze získat:

- Absolutní cesta ke spustitelnému souboru
- Příkaz použitý ke spuštění procesu
- Doba, po kterou proces běží
- Který uživatel proces spustil a jaká je jeho úroveň oprávnění v systému.
- Moduly, které proces načetl
- Obsah paměti přidělené procesu

Příklady programů a příkazů pro získávání informací o **procesech běžících v** systému:

- **Psinfo.exe -h -s -d /accepteula** (Zdroj: SysInternals)
- ***PsList.exe*** (Zdroj: sysinternals)
- ***CurrProcess.exe*** (Zdroj: Nirsoft.net)
- ***tasklist /v***
- ***Wmic process get name, processid, priority, threadcount, privatepagecount***

Příklady programů a příkazů pro získávání informací o službách, naplánovaných úlohách a systémových událostech:

- [Služby] **PsService.exe** (SysInternals)
- [Služby] **net start**
- [naplánované úlohy] **schtasks**
- [události] **PsLogList.exe** (SysInternals)
- [události] **EventLogSourcesView.exe** (Nirsoft)
- [události] **wevtutil**

4.1.5. Paměť

Schránka je oblast v paměti, kam lze ukládat data pro budoucí použití. Většina aplikací systému Windows poskytuje tuto funkci prostřednictvím nabídky Úpravy a možností Kopírovat, Vložit nebo Vyjmout. Tato funkce je užitečná při přesouvání dat mezi aplikacemi nebo dokumenty. Data často zůstávají ve schránce několik dní, aniž by si to uživatel uvědomil.

Ke shromažďování dat uložených v této oblasti paměti lze použít následující aplikaci **InsideClipboard.exe** (Nirsoft.net).

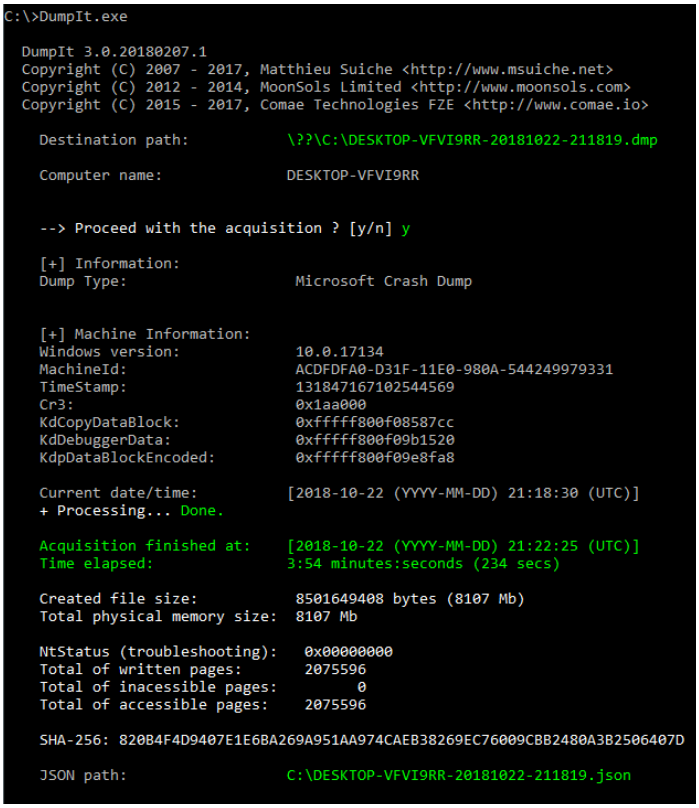
Analytici malwaru při práci s obfuskovaným malwarem hledají v paměti, protože při spuštění je dešifrován do stejné paměti. Rootkity navíc skrývají procesy, soubory, klíče registru a dokonce i síťová připojení. Analýzou paměti RAM je možné zkontrolovat, co je skryto před zraky uživatele. Tyto údaje jsou velmi užitečné pro kontextualizaci identifikovaných dat při budoucí analýze.

4.1.6. Získávání paměti

Proces výpisu paměti (Obrázek 34) se také hojně používá k diagnostice chyb v programech, protože tyto výpisy se obvykle vytvářejí, když dojde k chybě a programy neočekávaně přestanou fungovat.

Tyto výpisy paměti se provádějí v binárním, osmičkovém nebo šestnáctkovém formátu. Vyšetřování lze provádět pomocí programů, jako je např:

- DumpIT (moonsols)
- AccessData FTK Imager
- Belkasoft Live RAM Capturer



Obrázek 34 - Příklad fungování systému DumpIT

Existují další soubory[4] , které slouží k podpoře hlavní paměti a které je třeba shromáždit, například **pagefile.sys, který** systém Windows používá jako "virtuální paměť". Kdykoli systém potřebuje použít více paměti, než je k dispozici v operační paměti. Nebo **soubor hiberfil.sys** slouží k ukládání dat z paměti, když počítač přejde do režimu hibernace.

Pro sběr paměti v prostředí Linux *lze použít programy dcfldd* nebo *insmod*.

- dcfldd if=/dev/fmem of=memory.dump
- insmod lime-XX.ko "path="memory.dump" format=raw"

4.1.7. Informace o síti

Shromažďování nestálých informací o stavu sítě počítače: aktivní připojení, otevřené porty, informace o směrování a konfiguraci, mezipaměť, ARP.....

Jakmile je incident nahlášen, musí vyšetřovatel shromáždit informace o stavu síťových připojení k postiženému systému.

Platnost těchto připojení může vypršet a informace mohou časem zmizet. Pohled na tato data může pomoci zjistit, zda je útočník stále přihlášen do systému, zda existují připojení související se škodlivým softwarem, zda existuje proces, který se snaží najít další počítače v síti, aby tento škodlivý software rozšířil, nebo aby odeslal informace z protokolu na škodlivý server.

[4] https://www.hackingarticles.in/forensics-analysis-of-pagefile-and-hibersys-file-in-physical-memory/

Shromáždění těchto informací může poskytnout důležitá vodítka a doplnit kontext ostatních shromážděných informací.

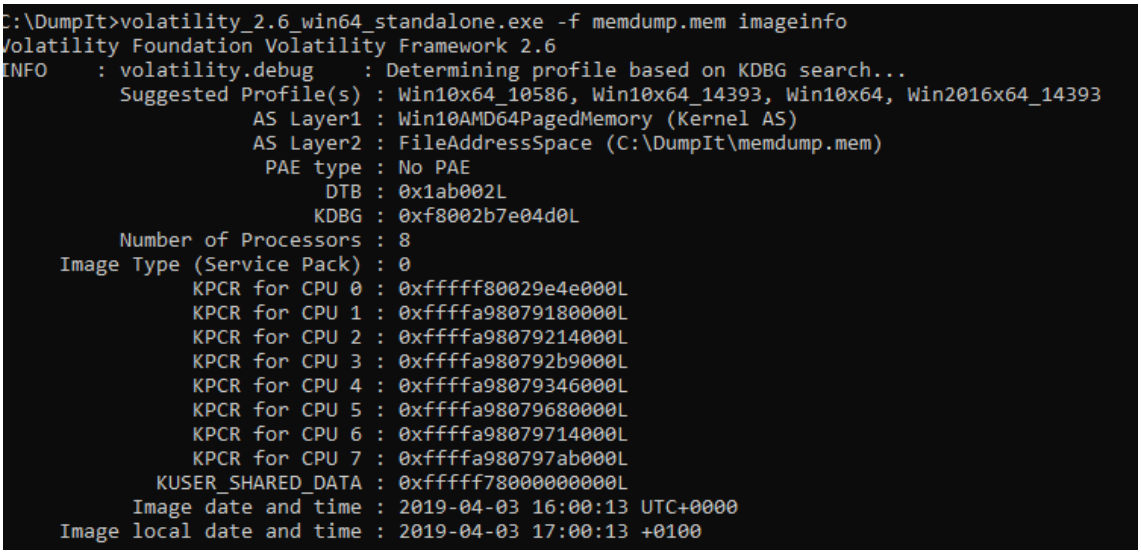
Příklady příkazů pro shromažďování informací o síti:

- Informace o síťové kartě: **ipconfig /all**
- Mezipaměť DNS: **ipconfig /displaydns**
- Aktivní síťová připojení: **Netstat -a**
- Mezipaměť ARP: **Arp -a**
- **Netsh int ipv6 show neigh**
- Události Wifi: **Netsh wlan show all**
- Bezdrátové sítě: (Zdroj: Nirsoft.net)
- Směrovací tabulka: **Tisk trasy**
- Připojení mezipaměti: **Netstat -c**
- Seznam relací mezipaměti: **Netstat -s**
- **Čisté účty**
- Sdílení zdrojů: **Čistý podíl**
- Dotazování serveru na službu DNS: **Nslookup -d**
- Seznam aktuálních připojení: **Rasdial**
- Seznam profilů: **Netsh wlan show profiles**

4.2. Analýza získávání paměti

Existují nástroje pro analýzu výpisů paměti, které jsou založeny pouze na obsahu paměti RAM. Tento obsah může být neúplný, protože části paměti jsou uloženy na disk, pokud nestačí k uložení všech dat. K překonání tohoto problému publikoval Nicholas Paul Maclean svou práci "Acquisition and Analysis of Windows Memory" (Získávání a analýza paměti systému Windows), jak funguje správa paměti v systémech Windows, a poskytl open-source nástroj vtop, který umožňuje kompletně rekonstruovat virtuální paměťový prostor procesu.

Pro analýzu výpisu paměti můžeme použít program Volatility, kde je možné provádět úkoly, jako je získání vysokoúrovňových informací o obraze, kde je identifikace operačního systému (Obrázek 35), servisního balíčku, hardwaru, architektury, adresy paměti a času, kdy byl Dump vytvořen.



Obrázek 35 - Získání informací o výpisu paměti

Příkazy užitečné pro provedení výpisu záznamů:

Export do textu:

```
C:\Regdmp.exe > e:\registryDump.txt
```

Najít výrazy v exportovaném souboru:

```
C:\Find/i "URL" registryDump.txt
```

Kopie používaných souborů registru:

```
C:\RawCopy.exe C:\WINDOWS\system32\config\SYSTEM E:\output -AllAttr
```

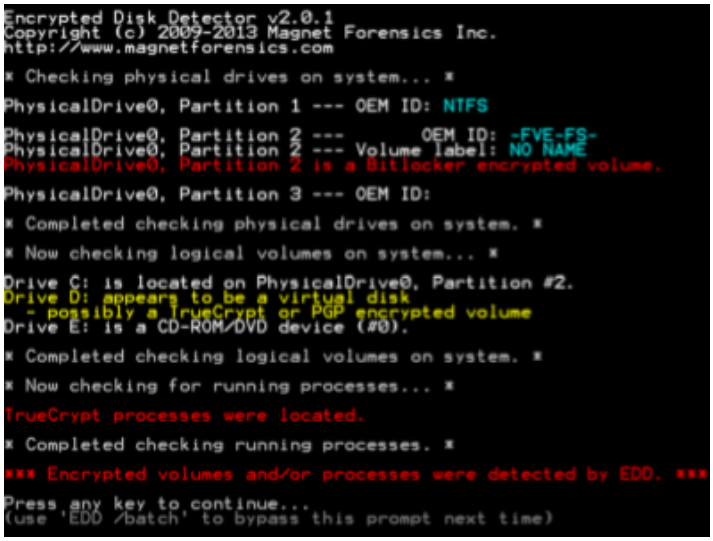
Další užitečné příkazy:

Pořiďte snímek obrazovky pracovní plochy:

```
C:\nircmd.exe savescreenshot screen1.png (Nirsoft.net)
```

Kontrola, zda je disk chráněn šifrováním (Obrázek 36)

```
C:\EDD.exe /accepteula /Batch > e:\EncryptedDiskDetector.txt

C:\Manage-bde -protectors c: -get
```



Obrázek 36 - Identifikace šifrovaného disku

4.2.1. Sintax programu Volatilita

První verze Volatility Framework byla zveřejněna na konferenci Black Hat. Software je založen na dlouholetém akademickém výzkumu v oblasti pokročilé analýzy paměti a forenzní analýzy. Volatility nyní umožňuje výzkumníkům analyzovat, v jakém stavu se stroj nacházel v době pořízení záznamu, a to na základě dat získaných z volatilní paměti.

Volatility Framework je založen na programovacím jazyce Python a je vyvinut v jeho nejvyspělejší verzi Python 2, kterou se budeme zabývat v tomto tématu. S příchodem Pythonu 3 vyvstala také potřeba aktualizovat verzi Volatility, využít výhod nové verze Pythonu a poskytnout jí více automatizace. Ve verzi 2 frameworku Volatility je prvním krokem při provádění analýzy paměti identifikace typu operačního systému. K tomu můžeme použít příkaz imageinfo programu Volatility (Obrázek 37). Tento příkaz je užitečný pro získání informací o obrazu na vysoké úrovni, uvádí pravděpodobnou identifikaci operačního systému (profil), service pack, hardwarovou architekturu, adresu paměti a čas výpisu.

```
C:\DumpIt>volatility_2.6_win64_standalone.exe -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_10586, Win10x64_14393, Win10x64, Win2016x64_14393
                     AS Layer1 : Win10AMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\DumpIt\memdump.mem)
                      PAE type : No PAE
                           DTB : 0x1ab002L
                          KDBG : 0xf8002b7e04d0L
          Number of Processors : 8
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff80029e4e000L
                KPCR for CPU 1 : 0xffffa98079180000L
                KPCR for CPU 2 : 0xffffa98079214000L
                KPCR for CPU 3 : 0xffffa980792b9000L
                KPCR for CPU 4 : 0xffffa98079346000L
                KPCR for CPU 5 : 0xffffa98079680000L
                KPCR for CPU 6 : 0xffffa98079714000L
                KPCR for CPU 7 : 0xffffa980797ab000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-04-03 16:00:13 UTC+0000
     Image local date and time : 2019-04-03 17:00:13 +0100
```

Obrázek 37 - Volatilita - Příklad výstupu příkazu imageinfo

Později musíme obsah paměti předat do textových souborů, aby bylo možné provést analýzu jejího obsahu. Volatility k tomuto účelu poskytuje řadu zásuvných modulů.

Sintax: **volatility -f <nome_da_imagem> -profile=< tipo_de_OS> <plugin> > <output>**

- **-f:** Soubor, který je výsledkem pořízení systému
- **-profile:** *pokyn k použití profilu operačního systému (dříve identifikovaného)*
- **plugin:** plugin, který se má spustit
- **výstup:** soubor pro export výsledků

4.2.2. Zásuvné moduly Volatility - Extrakce

Zásuvné moduly, které volatilita používá, jsou specifické pro identifikaci příslušných informací v obsahu výpisu paměti RAM. Některými z těchto zásuvných modulů se budeme zabývat zde.

Pslist Seznam spuštěných procesů

Pstree Zobrazení procesů, které se liší svým původem (Obrázek 38)

```
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x852854b0:csrss.exe                                316    300      9    449 2018-03-22 14:39:39 UTC+0000
 0x852b4b18:wininit.exe                              360    300      3     81 2018-03-22 14:39:39 UTC+0000
. 0x852e8d28:services.exe                            448    360     10    247 2018-03-22 14:39:39 UTC+0000
.. 0x84d21d28:vmicsvc.exe                           1408    448      4    102 2018-03-22 14:39:50 UTC+0000
.. 0x84d52d28:vmicsvc.exe                           1536    448      4     88 2018-03-22 14:39:50 UTC+0000
.. 0x846d5ca8:AdskNetSrv.exe                        3696    448     10    136 2018-03-22 14:42:18 UTC+0000
.. 0x845e4528:taskhost.exe                          1416    448     10    231 2018-03-22 14:41:59 UTC+0000
.. 0x8484a918:TrustedInstall                         128    448      5    119 2018-03-22 14:42:41 UTC+0000
.. 0x84923b40:svchost.exe                            268    448      8    114 2018-03-22 14:46:36 UTC+0000
.. 0x84687d28:AdskScSrv.exe                         3544    448      6     45 2018-03-22 14:42:17 UTC+0000
.. 0x853a4c60:svchost.exe                            792    448     20    479 2018-03-22 14:39:47 UTC+0000
... 0x853ce030:audiodg.exe                           944    792      7    136 2018-03-22 14:39:48 UTC+0000
```

Obrázek 38 - volatilita pluginu pstree

Psxview Porovnání procesů (Obrázek 39)

```
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x5c826300 WmiPrvSE.exe           3124 True   False  True     True   True  True    False
0x5cb9b8c0 dwm.exe                2296 True   False  True     True   True  True    True
0x5c84e7e0 svchost.exe            3776 True   False  True     True   True  True    True
0x5d7e9030 acad.exe               3312 True   False  True     True   True  True    False
0x5d1f0608 WSCommCntr1.ex         4036 True   False  True     True   True  True    False
0x5cc90a68 lsass.exe               456 True   False  True     True   True  True    False
0x5da1e030 mstsc.exe              3848 True   False  True     True   True  True    False
0x5cceb390 svchost.exe             560 True   False  True     True   True  True    False
0x5d5e9918 TrustedInstall          128 True   False  True     True   True  True    False
0x5d9bca68 explorer.exe           4072 True   False  True     True   True  True    True
0x5cc53b18 wininit.exe             360 True   False  True     True   True  True    True
0x5c5c6558 winlogon.exe           3644 True   False  True     True   True  True    True
```

Obrázek 39 - Zásuvný modul Volatility psxview

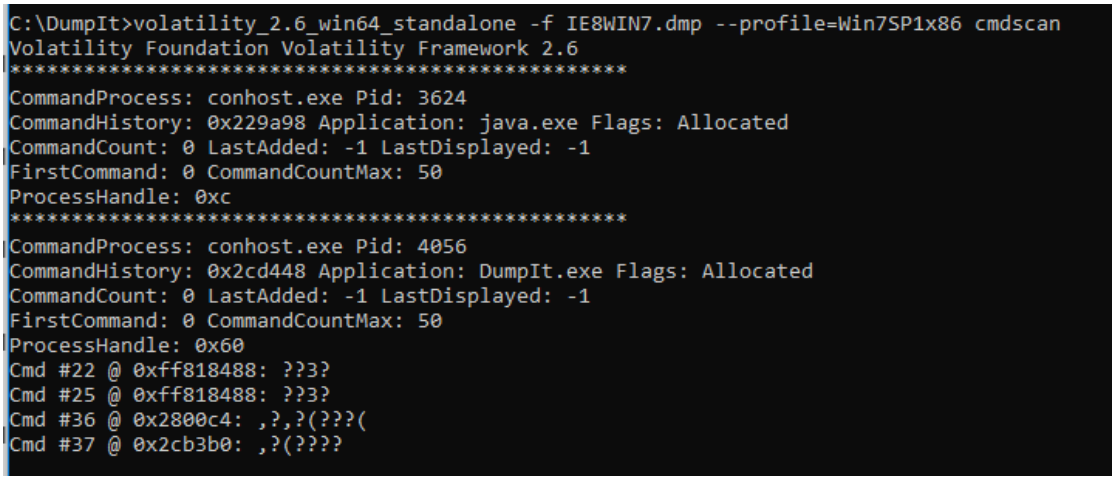
Netscan Zobrazení síťových připojení

Cmdline Cmdline Porovnání procesů (Obrázek 40)

```
Volatility Foundation Volatility Framework 2.6
**************************************************************************
System pid:      4
**************************************************************************
smss.exe pid:    240
Command line : \SystemRoot\System32\smss.exe
**************************************************************************
csrss.exe pid:    316
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows S
erServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2
**************************************************************************
csrss.exe pid:    352
Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows S
erServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2
**************************************************************************
wininit.exe pid:    360
Command line : wininit.exe
**************************************************************************
winlogon.exe pid:    400
Command line : winlogon.exe
**************************************************************************
services.exe pid:    448
Command line : C:\Windows\system32\services.exe
**************************************************************************
```

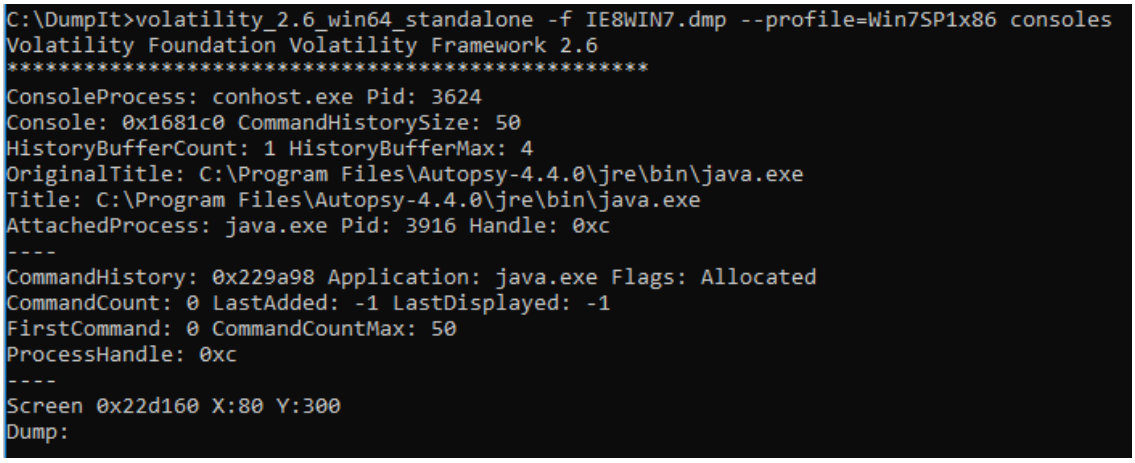
Obrázek 40 - Zásuvný modul cmdline Volatility

Cmdscan Porovnání procesů (Obrázek 41)



Obrázek 41 - Zásuvný modul cmdscan Volatility

Konzoly. Porovnání procesů (Obrázek 42)

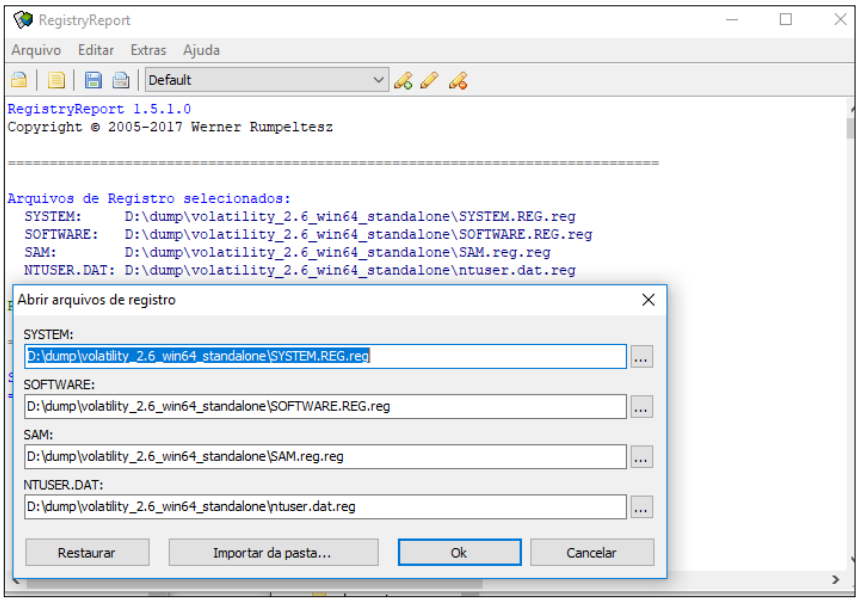


Obrázek 42 - Zásuvný modul konzol Volatility

DumpregistryExtrahovat soubory protokolu

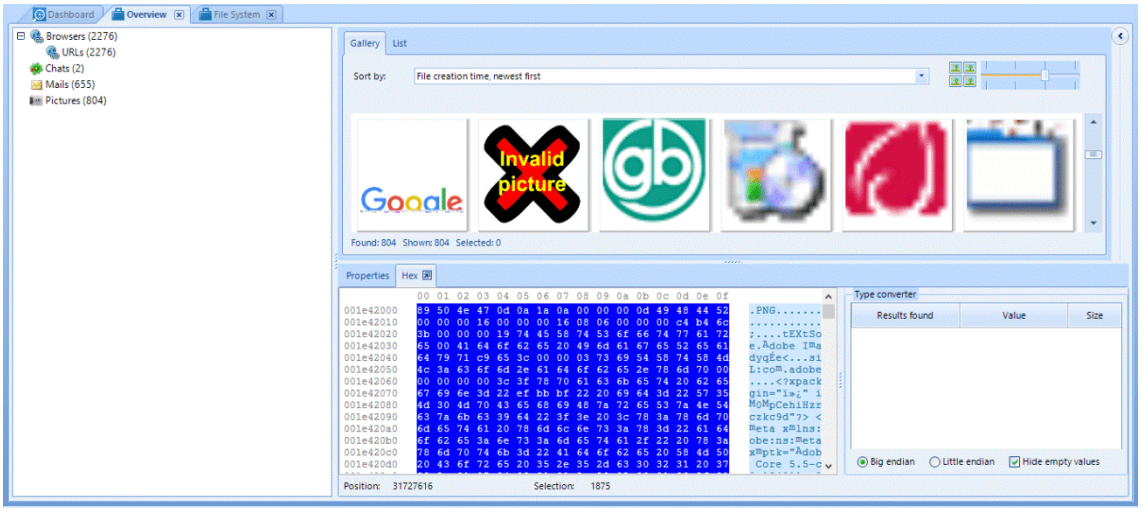
4.2.3. Volatilita zásuvných modulů - analýza

Soubory protokolu extrahované z paměti je možné analyzovat stejnými nástroji jako soubory protokolu extrahované z operačního systému. Příkladem je RegRipper, volatilita sama nebo RegistryReport, zobrazený na obrázku Obrázek 43.



Obrázek 43 - Analýza souboru RegistryReport

Při analýze paměti je také možné získat soubory, které byly zpracovány. Existují programy s možností identifikace a extrakce souborů z paměti, jak ukazuje následující obrázek se softwarem Belkasoft, kde je možné ověřit, že identifikoval adresy procházení v prohlížečích, údaje o konverzaci v chatu, soubory elektronické pošty a obrazové soubory (Obrázek 44).



Obrázek 44 - Analýza souborů pomocí Belkasoft

SANS zveřejnila plakát (Obrázek 45) s odkazem na analýzu paměti pomocí Volatility, který shrnuje mnoho zásuvných modulů užitečných pro tento typ analýzy.

Obrázek 45 - Plakát SANS - Cheat Sheet pro forenzní analýzu paměti v2.0

Vytvoření časové řady událostí v paměti

Z dat získaných z volatilní paměti je užitečné vytvořit časovou osu, která umožní datovat a třídit údaje v systému. Jedná se o proces zahrnující níže popsané postupy:

Timeliner vytvořit časovou osu

```
C:\> volatility_2.6_win64_standalone.exe -f IE8WIN7.dmp --profile=Win7SP1x86_23418 timeliner -- output=body > timeliner.body
```

Více informací na: https://volatility-labs.blogspot.com/2013/05/movp-ii-23-creating-timelines-with.html

Mftparser Obt (tabulka hlavních souborů).

```
C:\> volatility_2.6_win64_standalone.exe -f IE8WIN7.dmp --profile=Win7SP1x86_23418
mftparser -- output=body > mftparser.body
```

Spojte soubory týkající se zásuvných modulů **timeliner** a **mftparser.**

```
# cat timeliner.body mftparser.body >> timeline.log
```

Mactime[5] Generování časové osy z kombinace souborů

```
# mactime -d -b timeline.log > timeline.csv
```

Konečný výsledek postupů TimeLine (Obrázek 46)

Date	Size	Type	Mode	UID	GID	Meta	File Name
Fri Jan 25 2008 00:02:43	0	...b	---a-------|---	0	0	68267	[MFT FILE_NAME] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\CONTEN~1.CUI (Offset: 0xf352c00)
Fri Jan 25 2008 00:02:43	0	...b	---a-------|---	0	0	68267	[MFT FILE_NAME] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\contentsearch.cui (Offset: 0xf352c00)
Fri Jan 25 2008 00:02:43	0	m..b	---a-------|---	0	0	68267	[MFT STD_INFO] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\CONTEN~1.CUI (Offset: 0xf352c00)
Fri Jan 25 2008 00:57:05	0	...b	---a-------|---	0	0	68199	[MFT FILE_NAME] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\ACIMPR~1.CUI (Offset: 0xe84ec00)
Fri Jan 25 2008 00:57:05	0	...b	---a-------|---	0	0	68199	[MFT FILE_NAME] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\AcImpression.cui (Offset: 0xe84ec00)
Fri Jan 25 2008 00:57:05	0	m..b	---a-------|---	0	0	68199	[MFT STD_INFO] Users\mesi\AppData\Roaming\Autodesk\AUTOCA~1\R17.2\enu\Support\ACIMPR~1.CUI (Offset: 0xe84ec00)
Sat Jan 26 2008 16:24:32	0	m..b	---a----------	0	0	18486	[MFT STD_INFO] PROGRA~1\AUTOCA~1\PPCLIE~1.MAN (Offset: 0x4a15d800)

Obrázek 46 - Obsah souboru timeline.csv

Pomocí této tabulky lze snadno identifikovat akce provedené v paměti zařízení, které doplní informace získané při analýze zařízení v rámci forenzní analýzy mrtvých schránek.

Příklad identifikace přístupu do sítě TOR

Jako příklad analýzy paměťových dat můžeme uvést použití prohlížeče Tor Browser, který neukládá navigační informace na pevný disk, ačkoli je možné je identifikovat a analyzovat prostřednictvím paměti.

Začneme potvrzením **profilu systému** (Obrázek 47).

```
     Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                AS Layer2 : FileAddressSpace (D:\dump\tor\memdump.mem)
                 PAE type : PAE
                      DTB : 0x185000L
                     KDBG : 0x8293ac30L
     Number of Processors : 2
Image Type (Service Pack) : 1
           KPCR for CPU 0 : 0x8293bc00L
           KPCR for CPU 1 : 0x807c1000L
       KUSER_SHARED_DATA : 0xffdf0000L
     Image date and time : 2019-04-04 20:24:26 UTC+0000
Image local date and time : 2019-04-04 13:24:26 -0700
```

Obrázek 47 - Zásuvný modul Volatility imageinfo

Ke kontrole spuštěných procesů jsme použili zásuvný modul **pstree, který** filtruje procesy podle názvu "firefox.exe" (Obrázek 48), protože tento proces používá prohlížeč Tor Browser, nebo přímo podle názvu "tor.exe". Pro získání dalších informací o procesech v analyzovaném zařízení máme ještě možnost použít pluginy **pslist**, **psscan**.

[5] https://wiki.sleuthkit.org/index.php?title=Mactime

```
D:\dump\tor>volatility_2.6_win64.exe -f memdump.mem --profile=Win7SP1x86_23418 pstree | find "firefox.exe"
Volatility Foundation Volatility Framework 2.6
. 0x84cd67c8:firefox.exe                          1736   1604     45    715 2019-04-04 20:58:21 UTC+0000
.. 0x85f484c8:firefox.exe                         2428   1736     21    340 2019-04-04 20:59:08 UTC+0000
.. 0x844d8b20:firefox.exe                         2484   1736     19    328 2019-04-04 20:59:47 UTC+0000

D:\dump\tor>volatility_2.6_win64.exe -f memdump.mem --profile=Win7SP1x86_23418 pstree | find "tor.exe"
Volatility Foundation Volatility Framework 2.6
.. 0x85c15380:tor.exe                             2064   1736      4     65 2019-04-04 20:58:49 UTC+0000
```

Obrázek 48 - Využití volatility ve výzkumu procesů

Getsidy Informace o zahájení procesu, které se vztahují k uživateli (Obrázek 49).

```
G:\tor\Tor Browser>volatility.exe -f memdump.mem --profile=Win7SP1x86 getsids | find "tor.exe"
Volatility Foundation Volatility Framework 2.6
tor.exe (3868): S-1-5-21-3463664321-2923530833-3546627382-1000
tor.exe (3868): S-1-5-21-3463664321-2923530833-3546627382-513 (Domain Users)
tor.exe (3868): S-1-1-0 (Everyone)
tor.exe (3868): S-1-5-114 (Local Account (Member of Administrators))
tor.exe (3868): S-1-5-32-544 (Administrators)
tor.exe (3868): S-1-5-32-545 (Users)
tor.exe (3868): S-1-5-4 (Interactive)
tor.exe (3868): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
tor.exe (3868): S-1-5-11 (Authenticated Users)
tor.exe (3868): S-1-5-15 (This Organization)
tor.exe (3868): S-1-5-113 (Local Account)
tor.exe (3868): S-1-5-5-0-66052 (Logon Session)
tor.exe (3868): S-1-2-0 (Local (Users with the ability to log in locally))
tor.exe (3868): S-1-5-64-10 (NTLM Authentication)
tor.exe (3868): S-1-16-8192 (Medium Mandatory Level)
```

Obrázek 49 - Využití volatility při identifikaci procesu

netscan zobrazí síťová připojení

V tomto případě proces "tor.exe" indikuje dokončené připojení k cílové IP "54.37.17.235" na portu 9001 (Obrázek 50).

```
dfir@LAPTOP:/mnt/c/BoH$ vol.py -f Win10_14393_Tor_Closed.vmem --profile=Win10x64_14393 netscan | egrep "firefox.exe|tor.exe"
Volatility Foundation Volatility Framework 2.6
0x80814c899ab0     TCPv4    127.0.0.1:9150                127.0.0.1:51014      CLOSED          3552     tor.exe         2018-03-18
11:26:53 UTC+0000
0x80814c8cb8b0     TCPv4    192.168.241.133:50630         54.37.17.235:9001    CLOSED          3552     tor.exe         2018-03-18
11:18:59 UTC+0000
0x80814cafb470     TCPv4    127.0.0.1:51099               127.0.0.1:9150       CLOSED          7960     firefox.exe     2018-03-18
```

Obrázek 50 - Použití volatility při identifikaci sítě

Firefoxhistorie Seznam dotazovaných adres (URL) (Obrázek 51).

```
dfir@LAPTOP:/mnt/c/BoH$ vol.py --plugins=/usr/lib/python2.7/dist-packages/volatility/plugins -f Win10_14393
_Tor_Closed.vmem firefoxhistory | awk '{print $1, $2}'
Volatility Foundation Volatility Framework 2.6
ID URL
------ --------------------------------------------------------------------------------
4 place:type=6&sort=14&maxResults=1
3 place:sort=8&maxResults=1
2 https://blog.torproject.org
1 https://www.torproject.org
```

Obrázek 51 - Použití volatility k načtení adres URL z paměti

Zdroj: https://blog.superponible.com/2014/08/31/volatility-plugin-firefox-history/

5.

Identifikace a analýza informací v operačních systémech

5. Identifikace a analýza informačních bodů zájmu v operačních systémech

Podle serveru "https://gs.statcounter.com/os-market-share/desktop/worldwide" má operační systém Microsoft Windows podíl na trhu přibližně 75 %, následuje Apple OS X se 14,5 %. Forenzní analytik najde podstatně více zařízení s operačními systémy Micrososft než s jinými. To odůvodňuje větší pozornost věnovanou analýze tohoto operačního systému.

SANS provádí vynikající výzkumnou a vzdělávací činnost v oblasti digitální forenziky, přičemž jedním ze zajímavých faktorů je pravidelné zveřejňování takzvaného Posteru, na adrese: https://www.sans.org/posters/, s výsledky tohoto výzkumu. Tyto Postery jsou také důležitým zdrojem informací o umístění artefaktů forenzního zájmu, neboť operační systémy MS Windows ukládají při každodenních činnostech svých uživatelů četné artefakty.

5.1. Registr systému MS Windows

"*Centrální hierarchická databáze v systému Windows ... slouží k ukládání informací potřebných ke konfiguraci systému pro jednoho nebo více uživatelů, aplikací a hardwarových zařízení. Registr obsahuje informace, na které se systém Windows během provozu neustále odvolává, například profily jednotlivých uživatelů, aplikace nainstalované v počítači a typy dokumentů, které mohou jednotlivé aplikace vytvářet, nastavení vlastností složek a ikon aplikací, jaký hardware v systému existuje a jaké porty jsou používány.* "

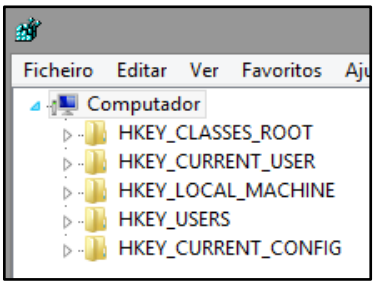
Zdroj: Redmond, Washington, Microsoft Press, 2002, s. 445.

Lze tedy konstatovat, že registr systému Windows obsahuje navzdory svým strukturovaným souborům logickou strukturu, kterou operační systém neustále používá a která uchovává soubor informací nezbytných pro jeho fungování.

Logická struktura registru systému Windows obsahuje:

1. **Klíče registru**, klíče s názvy "Software" a "System", patřící do *koše* "HKEY_CURRENT_CONFIG".
2. **Dílčí klíče registru**, ve kterých jsou uloženy informace registru (např.: dílčí klíč "Fonts").
3. **Hodnoty registru,** které obsahují informace zadáním jejich typu v příslušném sloupci (např.: REG_DWORD - 32bitová binární hodnota, REG_QWORD - 64bitová binární hodnota).

Pět hlavních úlů v logické struktuře operačního systému MS Windows je vidět na obrázku Obrázek 52.



Obrázek 52 - Kořenový úl

Hive registru (kořenové klíče) jsou charakterizovány předponou "HKEY_", což je zkratka pro "Handle to a KEY".

V různých souborech tvořících registr je uloženo 5 hlavních úložišť, přičemž za skutečná úložiště se považují pouze HKEY_USERS a HKEY_LOCAL_MACHINE, ostatní jsou zástupci nebo aliasy pro jejich větve.

Hive	Zkratka	Popis	*Odkaz*
HKEY_CURRENT_USER	**HKCU**	Ukazuje na uživatelský profil aktuálně přihlášeného uživatele.	Podklíč pod HKEY_USERS odpovídající aktuálně přihlášenému uživateli
HKEY_USERS	**HKU**	Obsahuje dílčí klíče pro všechny načtené uživatelské profily.	Nejedná se o odkaz
HKEY_CLASSES_ROOT	**HKCR**	Obsahuje informace o asociaci souborů a registraci COM	Nejedná se o přímý odkaz, ale o sloučené zobrazení HKLM\SOFTWARE\Classes a HKEY_CURRENT_USER\SOFTWARE\Classes.
HKEY_LOCAL_MACHINE	**HKLM**	Globální nastavení stroje.	Nejedná se o odkaz
HKEY_CURRENT_CONFIG	**HKCC**	Aktuální profil hardwaru	HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current
HKEY_PERFORMANCE_DATA	**HKPD**	Počítadla výkonu	Nejedná se o odkaz

Zdroj:
Redmond, Washington, Microsoft Press, 2012, str. 281.

Soubory protokolu jsou umístěny v následujících složkách:

Soubory protokolu operačního systému

C:\Windows\System32\Config\

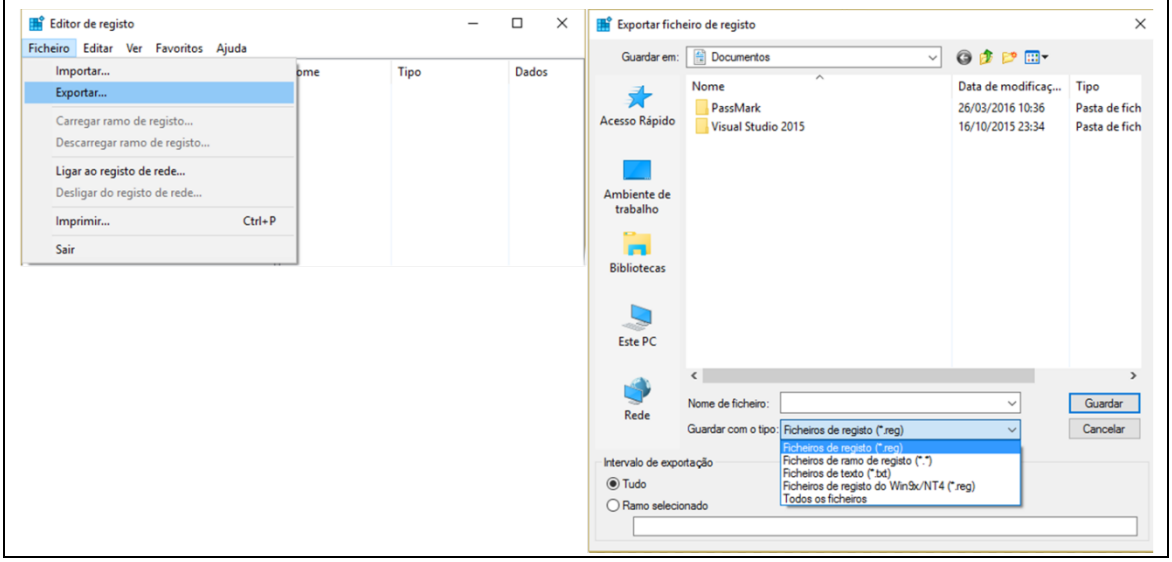
Soubory registru pro každého uživatele

C:\Users\<uživatelské jméno>\ntuser.dat

5.1.1. Editor registru (RegEdit)

Editor registru ve své grafické verzi umožňuje exportovat jeden nebo více klíčů registru (Obrázek 53).

RegEdit, Soubor > Exportovat



Obrázek 53 - Export registru prostřednictvím nástroje RegEdit

Prostřednictvím příkazového řádku:

regedit /e c:\output.reg "HKEY_LOCAL_MACHINE\System\..."

5.1.2. ERUNTgui

Aplikace ERUNTgui (Obrázek 54) umožňuje zálohování, obnovu a optimalizaci registru, přičemž pro forenzní analýzu je zajímavá možnost provést zálohu registru a umožnit tak jeho následnou analýzu.

Obrázek 54 - Export registru prostřednictvím ERUNTgui

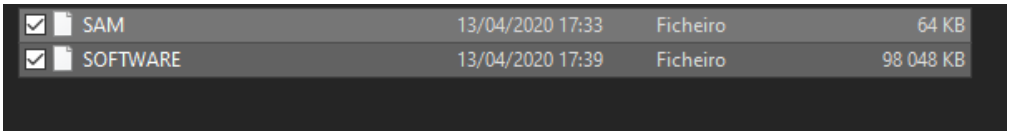
5.1.3. RAWCopy

Aplikace RAWCopy (Obrázek 55) umožňuje kopírovat sektory disku, ve kterých se nacházejí používané soubory, a překonat tak omezení kopírování souborů otevřených systémem.

```
C:\ForensicsSoftware\VArios\RawCopy>RawCopy64.exe C:\WINDOWS\system32\config\SAM C:\
RawCopy v1.0.0.9

Error: NtOpenFile returned: 0xC0000043
Opening target file failed, now re-trying with INDX method from parent folder
Record number: 128277 found at disk offset: 3352581120 -> 0x41E8FA8A80000000
Record number: 219734 found at disk offset: 63105103872 -> 0x422D62B6F0000000
Writing: SAM

Job took 1.07 seconds

C:\ForensicsSoftware\VArios\RawCopy>RawCopy64.exe C:\WINDOWS\system32\config\SOFTWARE C:\
RawCopy v1.0.0.9

Error: NtOpenFile returned: 0xC0000043
Opening target file failed, now re-trying with INDX method from parent folder
Record number: 128277 found at disk offset: 3352581120 -> 0x41E8FA8A80000000
Record number: 220159 found at disk offset: 63105539072 -> 0x422D62C438000000
Writing: SOFTWARE

Job took 1.31 seconds

C:\ForensicsSoftware\VArios\RawCopy>
```

Obrázek 55 - Export registru prostřednictvím RAWCopy

Prostřednictvím RAWCopy bylo možné získat kopii souboru SAM a SOFTWARE se spuštěným systémem (Obrázek 56).



Obrázek 56 - Soubory exportované programem RAWCopy

Zdroj: https://github.com/jschicht/RawCopy

5.2. Analýza registru systému Windows

Analýzu registru systému Windows lze provést pomocí forenzního softwaru, jako je AccessData Registry Viewer, nástroje Erica Zimmermana, RegRipper nebo i jakýkoli jiný software schopný extrahovat data z těchto souborů registru.

Vzhledem ke složitosti registru systému Windows může být určení umístění jednotlivých důležitých informací náročným úkolem, nicméně jsme si vyžádali pomoc společnosti SANS FOR500 (https://digital-forensics.sans.org/docs/DFPS_FOR500_v4.11_0121.pdf), která určila mnoho důležitých míst, kde lze nalézt příslušné informace.

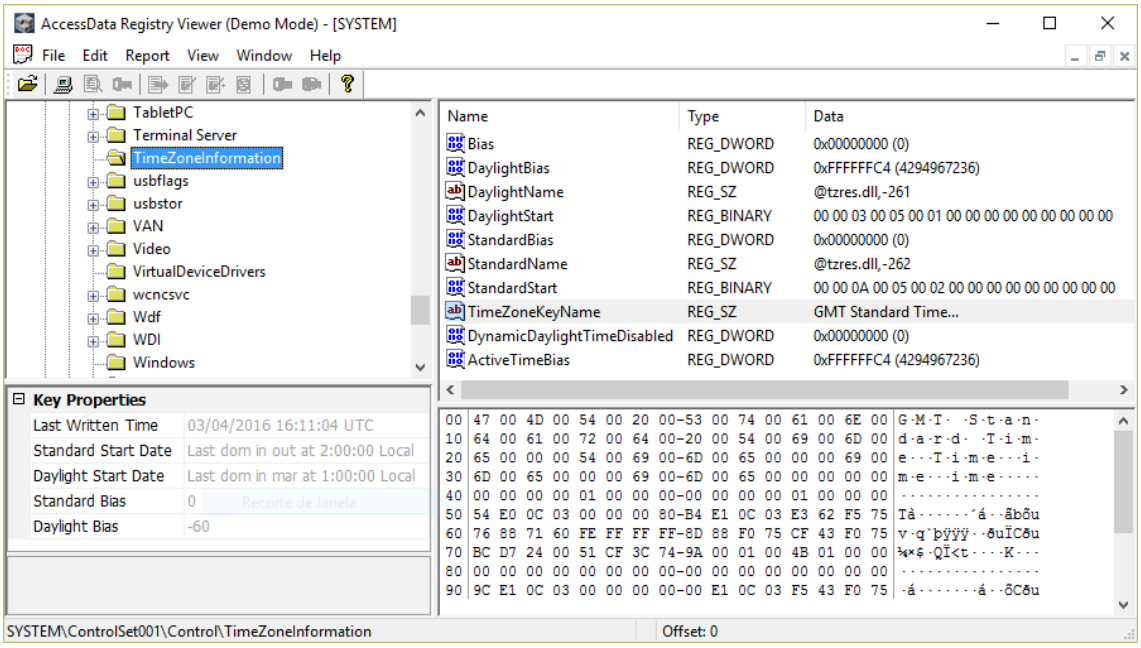
Může být potřeba získat protokol z připojeného počítače, který je obrovským zdrojem forenzně relevantních informací, a proto bude nezbytné získat všechny tyto informace. (Čtěte: https://resources.infosecinstitute.com/windows-registry-analysis-regripper-hands-case-study-2/). Existuje několik způsobů, jak provést výpis registru, zde se zaměříme na některé různé způsoby.

5.2.1. Časové pásmo

Mezi první analyzované informace by mělo patřit časové pásmo (Obrázek 57), protože to nás může vést k chybám, když se setkáme s akcemi, které uvádějí jiné datum/čas, než je skutečný, jednoduše proto, že systém je nakonfigurován s jiným časovým pásmem, než které používá forenzní analytik.

Tyto informace lze zjistit v systému *hive* SYSTEM na následujícím místě:

SYSTEM\ControlSet001\Control\TimeZoneInformation



Obrázek 57 - Časová zóna v zobrazení registru AccessData Viewerr

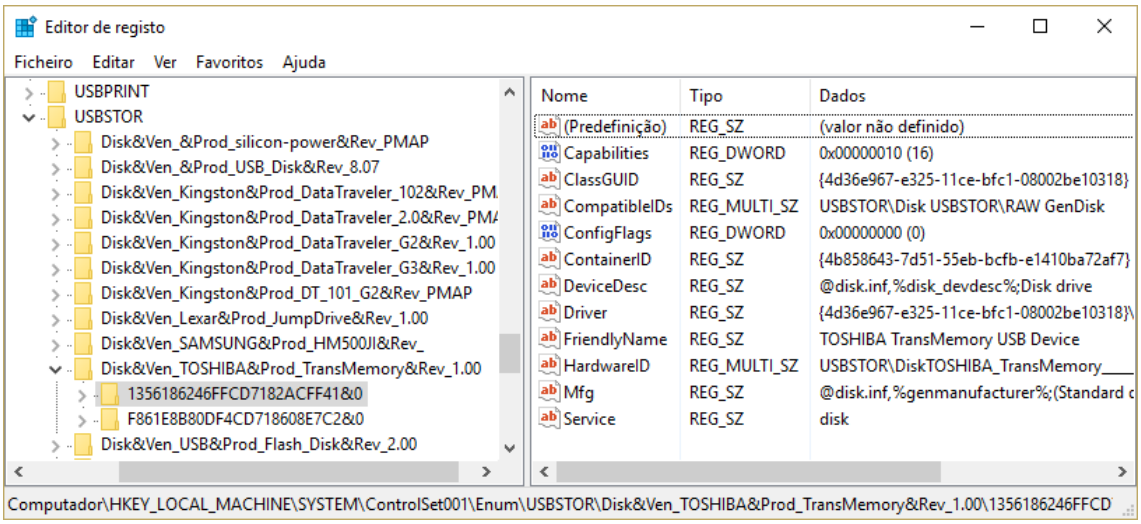
5.2.2. Zařízení USB

V registru je také možné získat informace ze zařízení USB, která byla připojena k systému v *koši* SYSTEM:

Získat: Výrobce / značka / sériové č. / datum / čas prvního a posledního připojení k systému

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR HKLM\SYSTEM\CurrentControlSet\Enum\USB

Zobrazením (Obrázek 58).



Obrázek 58 - Zobrazení zařízení USB v Editoru registru

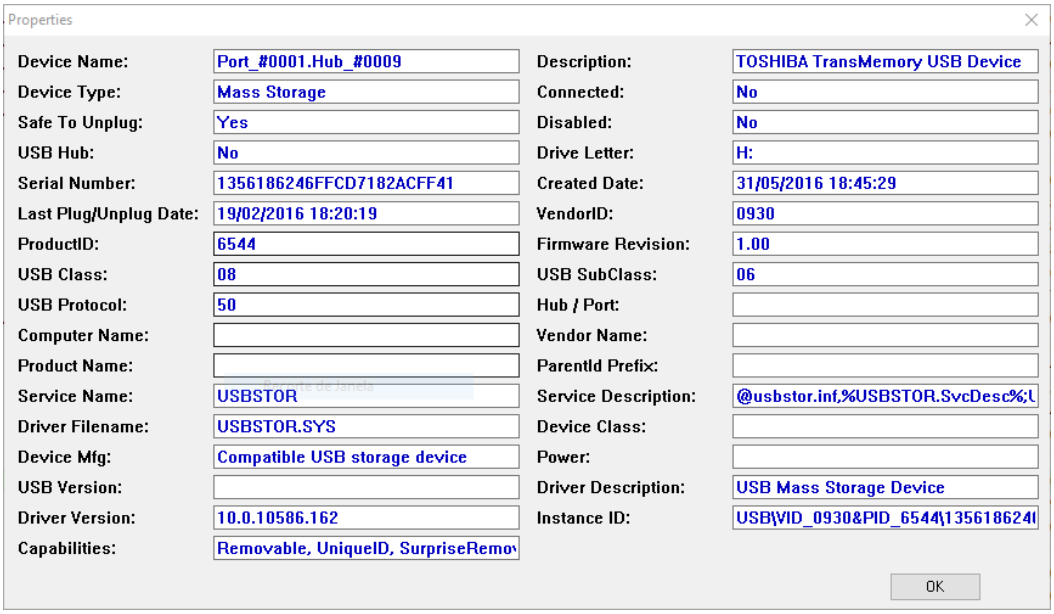
Získání písmene přiřazeného zařízení USB

HKLM\SYSTEM\MountedDevices

Zjištění uživatele, který připojil zařízení k systému.

NTUSER.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

Stejné informace lze získat pomocí specifických nástrojů pro získávání informací ze zařízení USB, jako jsou nástroje 4Discovery nebo USBDeview(Obrázek 59).



Obrázek 59 - Zobrazení zařízení USB v aplikaci USBDeview

Přečtěte si:https://www.researchgate.net/publication/318514858_USB_Storage_Device_Forensics_for_Windows_10

5.2.3. Uživatelé

Informace o uživatelích systému jsou uloženy v registru systému Windows v koši SAM, ale pro každého uživatele existuje také soubor registru NTUSER.DAT, který uchovává údaje specifické pro daného uživatele:

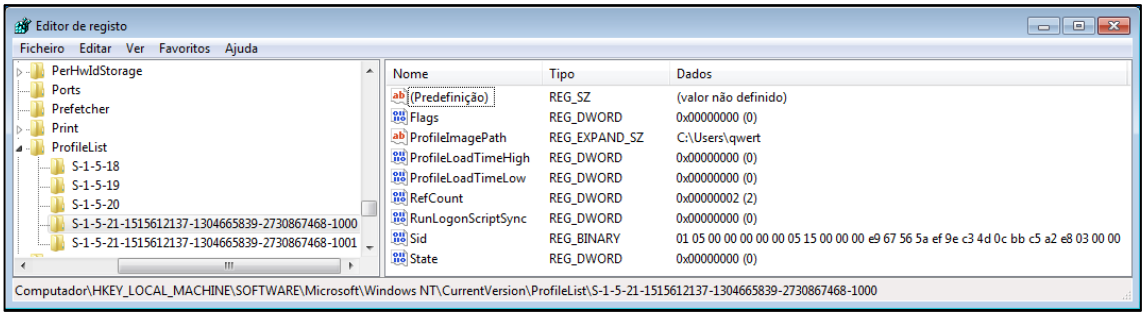
Seznam místních uživatelských profilů

V rejstříku: HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList

Uživatelé systému

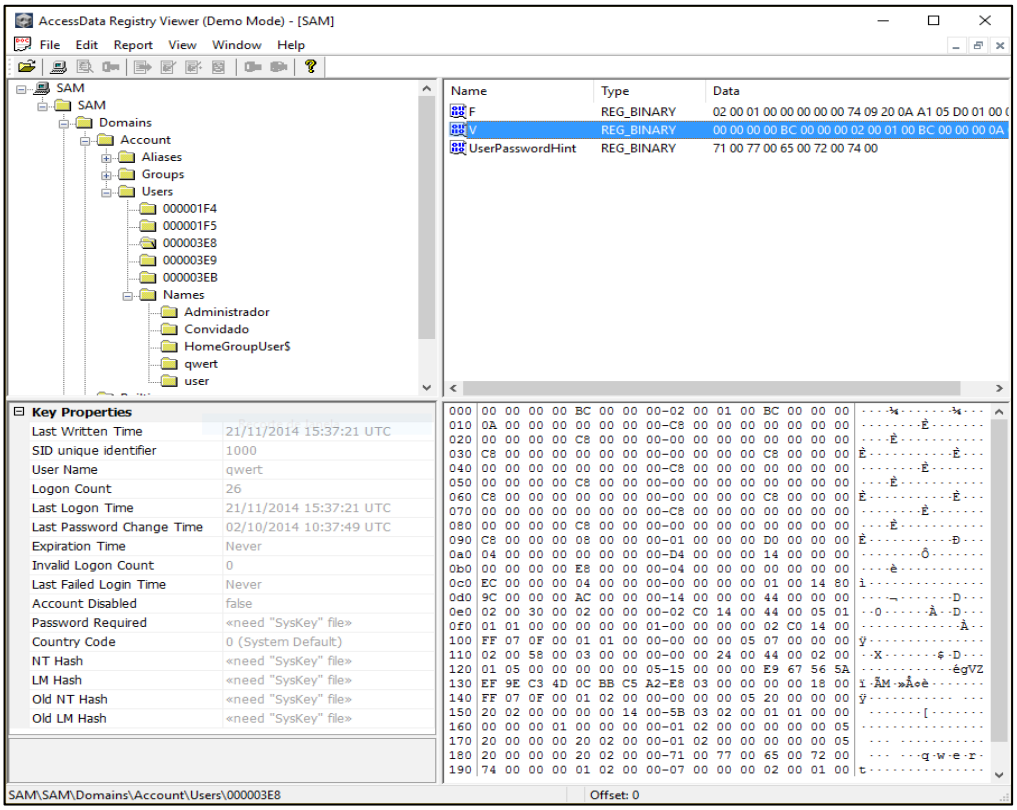
V souboru: SAM\SAM\Domény\Účty\Uživatelé\

Při zobrazení tohoto klíče registru v Editoru registru můžete vidět, jak se tyto informace zobrazují (Obrázek 60).



Obrázek 60 - Zobrazení uživatelů v editoru registru

Stejné informace lze získat pomocí specifických nástrojů pro získávání informací o uživatelích, jako je například AccessData Registry Viewer (Obrázek 61).



Obrázek 61 - Zobrazení uživatelů v programu AccessData Registry Viewer

5.2.4. Síť

Protokol obsahuje také různé síťové informace, například bezdrátové sítě, ke kterým se systém připojil:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\NetworkList\

V této lokalitě je možné identifikovat:

- Název sítě (SSID)
- Název domény / intranetu

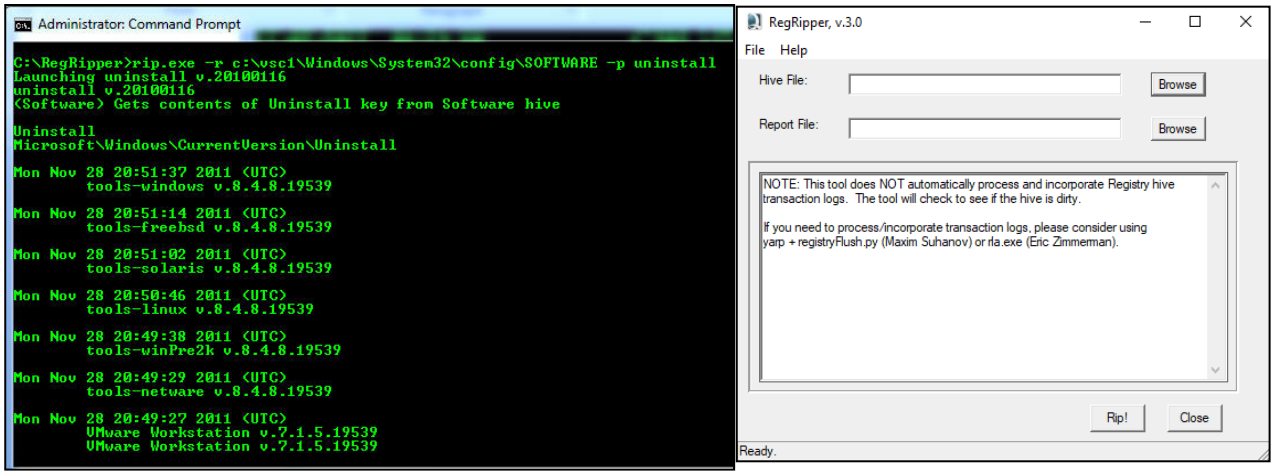
- Datum/čas posledního připojení (prostřednictvím data/času zápisu příslušného klíče).
- Adresa MAC brány

5.2.5. Analýza registru systému Windows - RegRipper

Pokud jde o analýzu registru systému Windows, existuje mnoho forenzních nástrojů, které můžeme použít k usnadnění analýzy informací obsažených v registru systému Windows. Zaměříme se zde na některé bezplatné nástroje, jako jsou RegRipper, RegistryReport a Windows Registry Recovery.

RegRipper (http://github.com/keydet89) je open source forenzní aplikace vyvinutá Harlanem Carveym a napsaná v jazyce PERL, jejímž cílem je získávat informace ze souborů registru systému Windows čitelným způsobem.

RegRipper (Obrázek 62) lze použít prostřednictvím příkazového řádku a grafického rozhraní k extrakci specifických informací z každého souboru registru. Při použití příkazového řádku je možné vybrat zásuvný modul, který má být použit pro každý oddíl registru, zatímco v případě příkazového řádku se použijí všechny zásuvné moduly dostupné pro vybraný oddíl. Výsledek extrahovaných informací lze zobrazit na obrazovce nebo uložit do textového souboru, v případě použití příkazového řádku. Prostřednictvím jeho grafického rozhraní bude nutné zadat výstupní umístění, nazvané Report File (Soubor s hlášením), pro vytvoření textového souboru s výsledkem všech zásuvných modulů aplikovaných na příslušný hive registru.

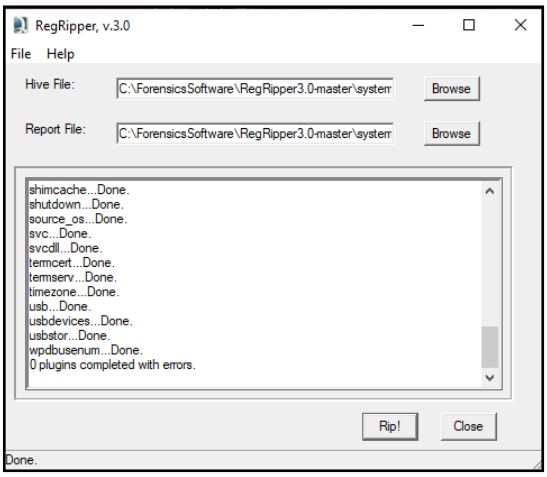


Obrázek 62 - Použití programu RegRipper

Prostřednictvím příkazového řádku je možné zkontrolovat dostupné zásuvné moduly, které lze použít, pomocí argumentu "-l -c".

```
C:\RegRipper3.0-master>rip -l -c > c:\list.csv
```

V režimu grafického uživatelského rozhraní (Obrázek 63) nemůžeme vybrat jeden zásuvný modul, ale Hive, který chceme analyzovat.



Obrázek 63 - Použití grafického uživatelského rozhraní programu RegRipper

Výstupní soubor (Obrázek 64)

```
----------------------------------------
winver v.20200525
(Software) Get Windows version & build info

ProductName              Microsoft Windows XP
CSDVersion               Service Pack 3
BuildLab                 2600.xpsp.080413-2111
RegisteredOrganization   ubinet
RegisteredOwner          ubinet
InstallDate              2000-01-01 17:45:17Z
----------------------------------------
```

Obrázek 64 - Výstupní soubor RegRipperu

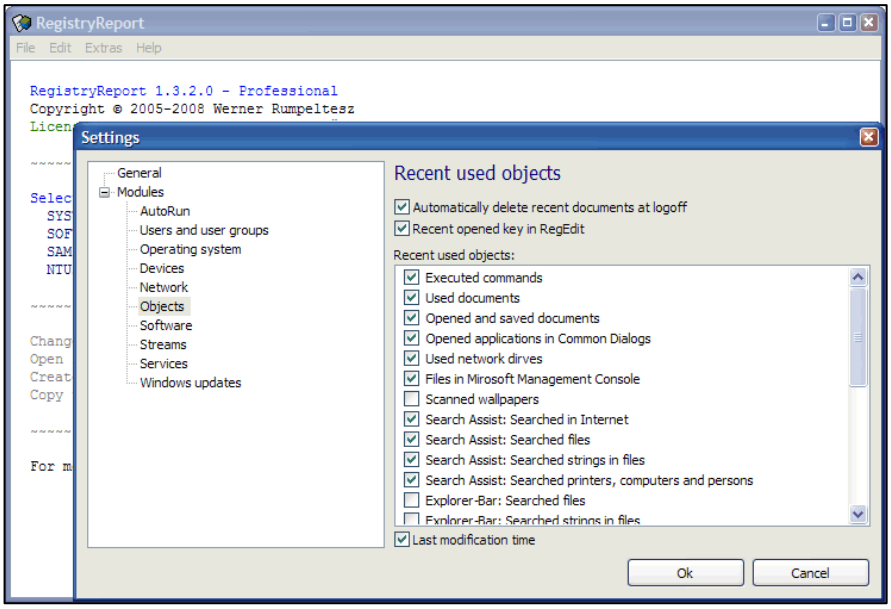
Existují i další forenzní aplikace se stejným cílem, tedy interpretovat obsah souborů registru, například Registry Report a Windows Registry Recovery.

RegistryReport

Stejně jako RegRipper i Gaijin Registry Repport prezentuje informace z registru snadno čitelným a prohledávatelným způsobem. Funguje jednoduše a umožňuje vybrat informace, které chcete z registru získat, pomocí zaškrtávacích políček, jak je znázorněno na obrázku Obrázek 65.

Zdroj: https://gaijin.at/en/files?dir=old-software registryreport

https://github.com/jschicht?tab=repositories

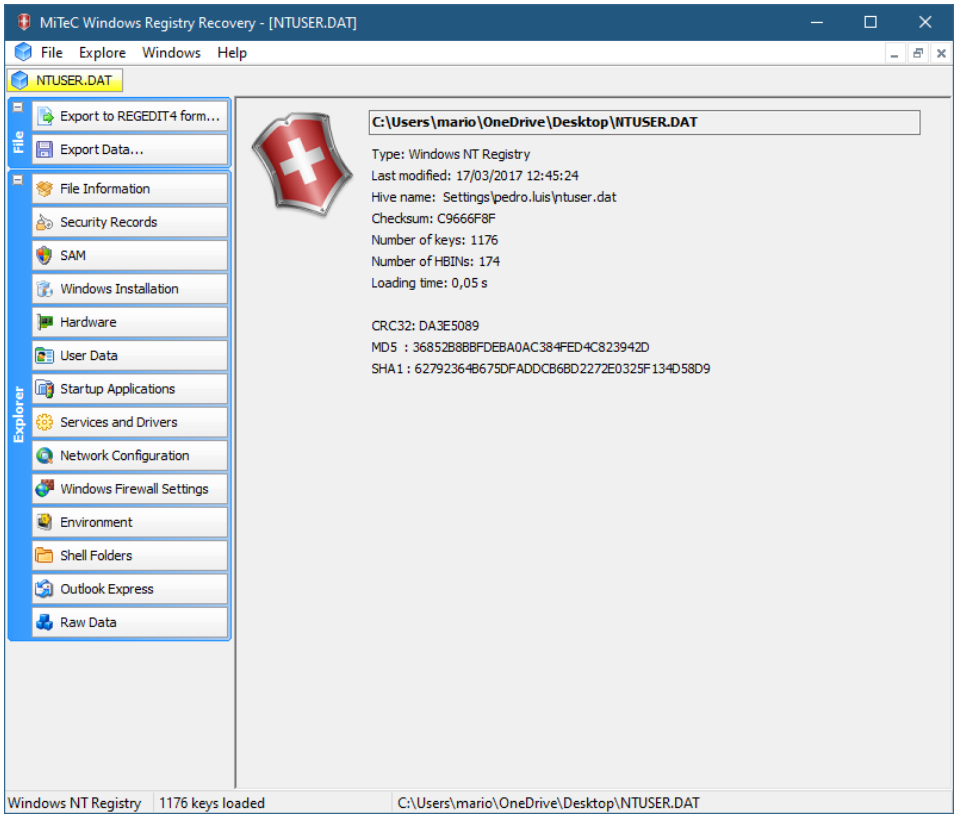


Obrázek 65 - Použití nástroje RegistryReport

Zdroj: https://www.gaijin.at/en/files?dir=old-software&sort=N&order=A registryreport

Obnovení registru systému Windows

WRR (Obrázek 66) je jednou z aplikací, které můžeme použít pro analýzu registru systému Windows.



Obrázek 66 - Použití programu MiTeC Windows Registry Recovery

Zdroj: http://www.mitec.cz/wrr.html

5.3. Analýza systémů založených na Linuxu

Digitální kriminalistika v operačních systémech MS Windows je široce rozšířená, ať už prostřednictvím kurzů a vědeckých článků, nebo prostřednictvím nových médií, jako jsou videa. Digitální forenzní analýza v operačních systémech Linux není tak rozšířená, především proto, že je také mnohem méně rozsáhlá.

Souborové systémy

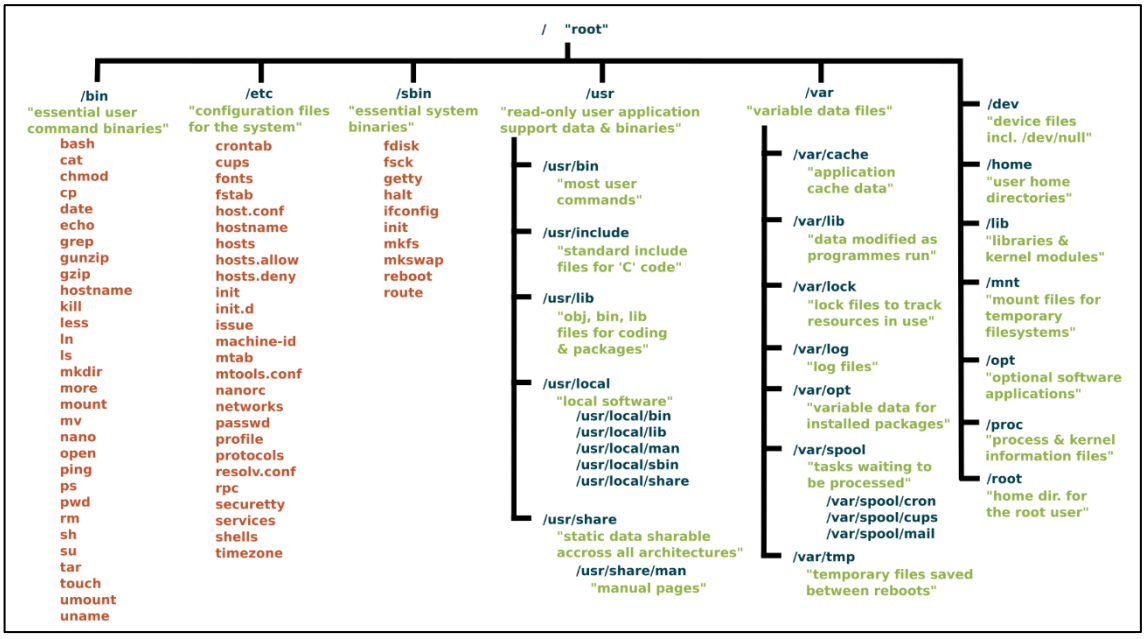
Standardním souborovým systémem v systému Linux je v současné době Ext4, i když podporuje různé typy souborových systémů.

Souborový systém Linux	**Data**	
Ext	1992	Znamená "rozšířený souborový systém" a byl to první souborový systém vytvořený pro Linux v roce 1992.
Ext2	1993	Podporoval disky s kapacitou až 2 TB a nepodporoval žurnálování. Protože nepoužívá žurnálování, lze jej používat na USB klíčenkách.
Ext3	1999	Stejně jako Ext2, ale s výhodou žurnálování.
Ext4	2006	Současná verze Ext. types má oproti svým předchůdcům několik výhodných vlastností, například menší fragmentaci systému, práci s velkými soubory a další. EXT4 podporuje maximální velikost souborového systému 1EB (1 Exabyte) a maximální velikost souboru 16 TB. Je možné mít neomezený počet podadresářů

Obecné úvahy

1. Neexistují žádné soubory protokolu jako v operačním systému Windows
2. Informace by měly být shromažďovány na rozptýlených místech
3. Různé struktury systémových souborů v různých distribucích

Strukturu souborů a složek systému Linux lze shrnout takto Obrázek 67.

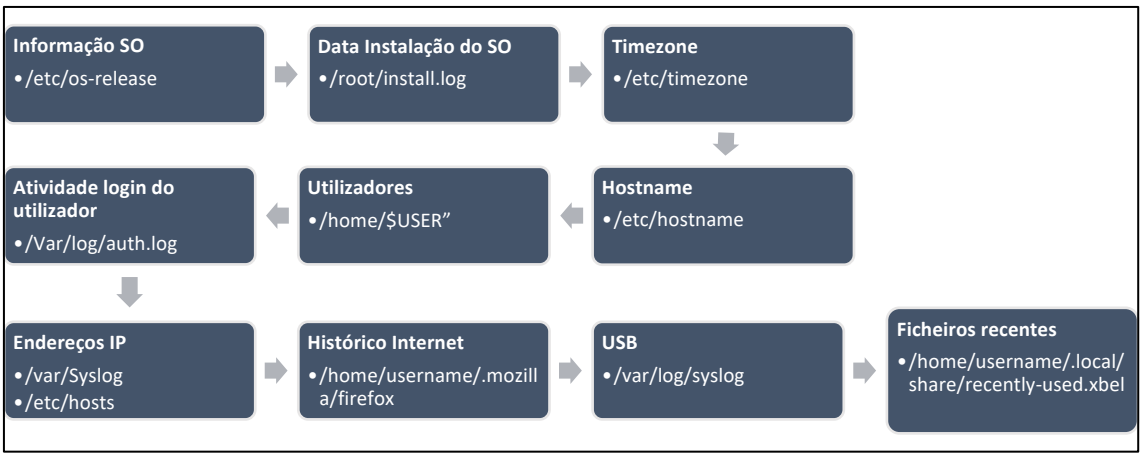


Obrázek 67 - Struktura systémových souborů Linuxu

Zdroj: The Linux Foundation - https://linuxfoundation.org/blog/classic-sysadmin-the-linux-filesystem-explained/

5.3.1. Zajímavosti v systémech Linux

Analýza činnosti uživatelů v systémech Ubuntu Linux by měla probíhat podle posloupnosti ověřování a shromažďování informací, jak je uvedeno v části Obrázek 68.



Obrázek 68 - Návrh na shromažďování informací o systému Linux

Automatické spouštění programů spuštěných v systému :

Mějte na paměti, že mnoho programů je nakonfigurováno tak, aby se spouštěly automaticky při startu systému. Informace o programech, které se mají spouštět při startu, se nacházejí v adresáři "**/etc/rc.local**".

Přístup k dokumentům :

Zkoušející může zjistit, ke kterým dokumentům bylo v poslední době přistupováno. Soubor obsahující tyto informace se nachází v adresáři **/home/user/.local/share/recently-used.xbel.** K zobrazení obsahu souboru lze použít příkaz **cat.** Soubor .xbel poskytuje podrobné informace o souborech, ke kterým uživatel přistupoval, například čas přístupu a modifikace, a..

Nainstalované aplikace :

Informace o aplikacích jsou ve složce **/usr/bin a** knihovny potřebné pro aplikace jsou ve složce **/usr/lib.** Seznam aplikací lze získat příkazem **ls -l /usr/bin/.** Je možné zjistit datum instalace, oprávnění, velikost atd.

Informace o síti:

Ubuntu uchovává seznam sítí připojených k systému v: **/etc/NetworkManager/system-connections**

Soubor **/var/log/syslog** obsahuje datum a čas navázání síťového připojení.

Připojená zařízení:

Adresář /dev poskytuje informace o hardwaru připojeném k systému.

Soubor **/var/log/syslog** obsahuje také informace o zařízeních připojených k systému.

Poslední přihlášení a aktivita uživatele::

Informace o posledním přihlášení lze získat v **/var/log/lastlog**

Procházení internetu:

Uvádíme umístění složek s navigačními informacemi ve dvou hlavních prohlížečích používaných v operačním systému Linux (Obrázek 69 a Obrázek 70). Po extrakci těchto obsahů je možné je analyzovat stejným způsobem jako v systému Windows .

Prohlížeč Firefox

OS	Localização Profile
Linux	/home/$username/.mozilla/firefox/Profiles

OS	Localização da Cache
Linux	/home/$username/.mozilla/firefox/Profiles

Obrázek 69 - Umístění informací prohlížeče Firefox

Google Chrome

OS	Localização
Linux	/home/$USER/.config/google-chrome/Default/Preferences

Obrázek 70 - Umístění informací v prohlížeči Google Chrome

6.

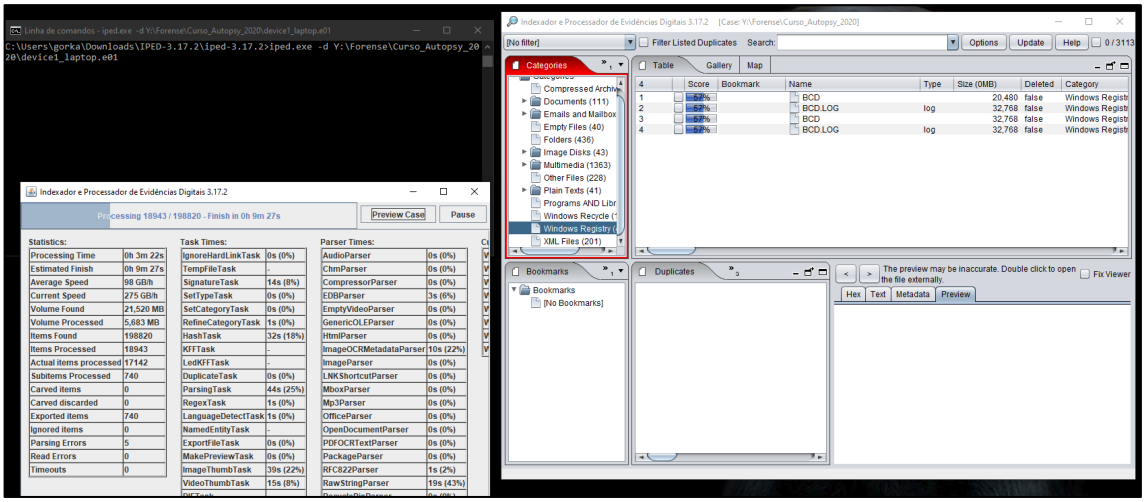
Forenzní analýza s bezplatnými sadami pro použití

6. Forenzní analýza s bezplatnými sadami pro použití

Forenzní analýza vyžaduje znalost specifických nástrojů, které dokáží získat a zpracovat požadované informace. Mnohé z nich jsou komerční nástroje, například OpenText EnCase, AccessData FTK, Magnet Axiom a další. Co se týče bezplatných nástrojů, je situace zcela odlišná, protože k použití je k dispozici jen velmi málo analytických sad. My se tak zaměříme na 2 z těchto sad, IPED a Autopsy The Sleuth Kit.

6.1.IPED

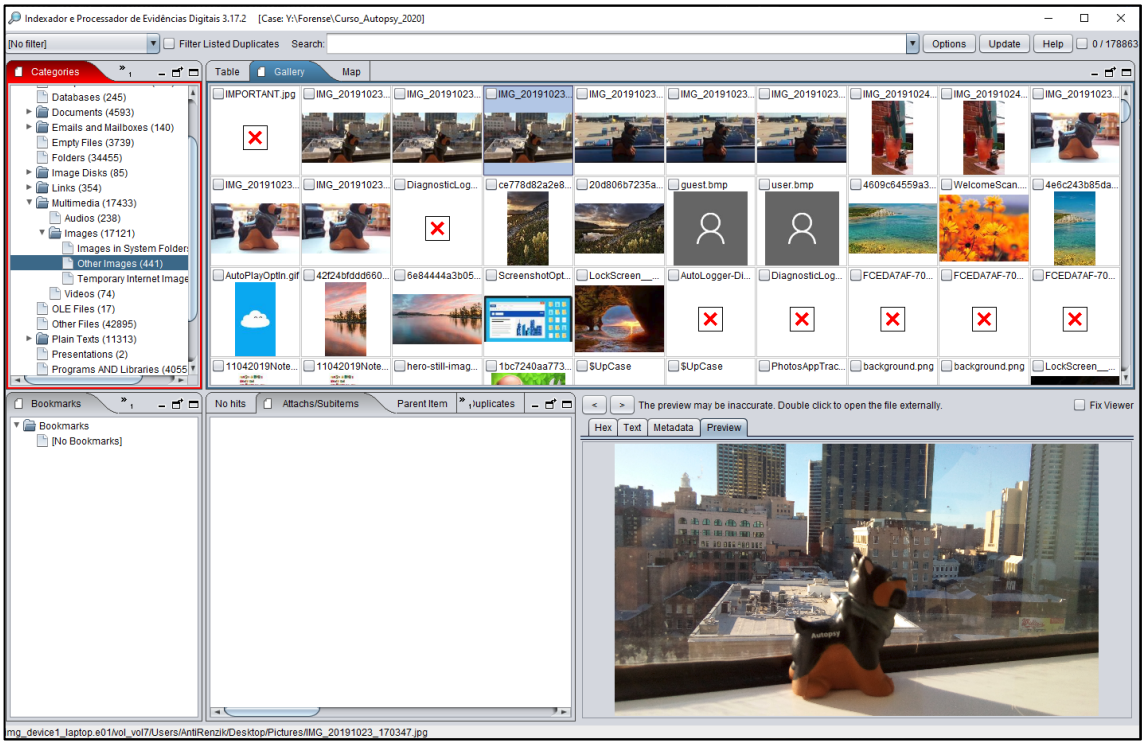
IPED - Indexer and Digital Evidence Processor je open source nástroj vyvinutý v jazyce Java brazilskou federální policií pro forenzní vyšetřování, který je známý svým dobrým výkonem zpracování (Obrázek 71. Byl vyvinut tak, aby umožňoval analýzu velkých objemů dat velkým počtem lidí, neboť byl záměrně vyvinut pro vyšetřování operace Lava Jato v Brazílii. Vysoký vícevláknový výkon s rychlostí zpracování až 400 GB/h umožňuje podporu rozsáhlých případů s velkým objemem zpracovávaných dat.



Obrázek 71 - Zpracování pomocí IPED

https://github.com/sepinf-inc/IPED

Jedná se o software, který vyžaduje určité znalosti při jeho používání, a to i přes jeho jednoduchý a intuitivní vzhled, jak je vidět na obrázku. Obrázek 72.



Obrázek 72 - Analýza pomocí IPED

Zdroj: https://github.com/sepinf-inc/IPED/wiki/Beginner's-Start-Guide

https://servicos.dpf.gov.br/ferramentas/IPED/

6.2. Pitevní sada Sleuth

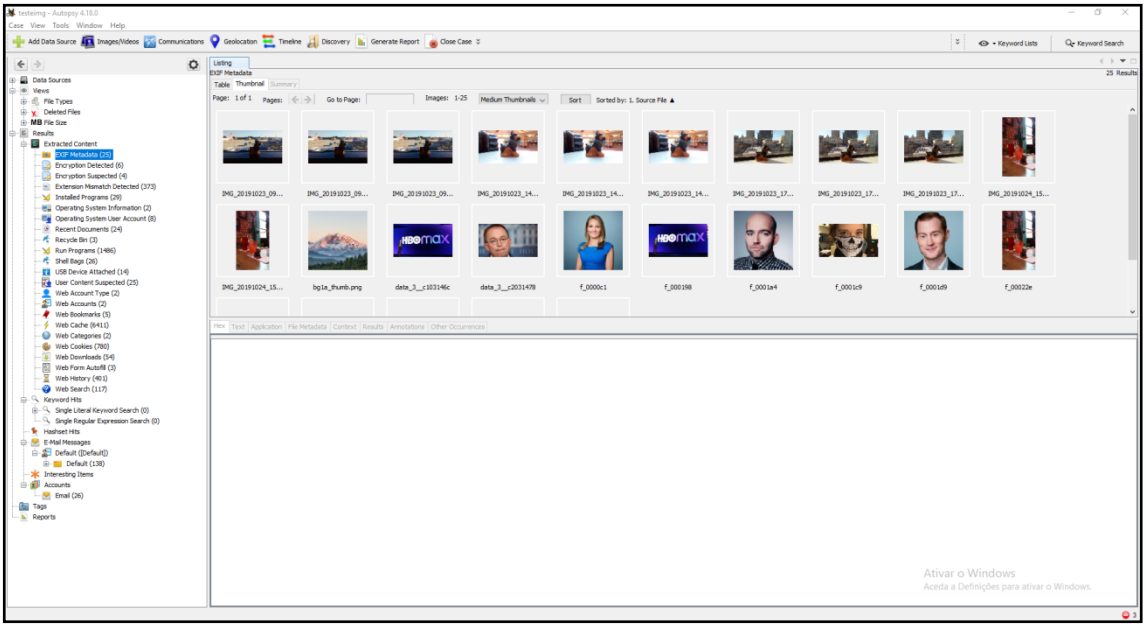
Sleuth Kit® je knihovna a také sada nástrojů, která umožňuje analýzu souborových systémů FAT, NTFS, Ext2/3/4 a UFS, včetně těch, které běžně používá operační systém Linux, dále umožňuje analýzu souborů a složek, obnovu smazaných souborů, vytváření *časové osy* činností se soubory, vyhledávání výrazů a používání databází *hash*.

https://github.com/sleuthkit/sleuthkit/blob/develop/NEWS.txt

Autopsy - Autopsy je grafické uživatelské rozhraní (GUI) sady The Sleuth Kit. Je to jedna z platforem s otevřeným zdrojovým kódem, která byla vyvinuta s cílem využít možností sady The Sleuth Kit k provádění forenzní analýzy zařízení, jako jsou pevné disky, multimediální karty, chytré telefony a další. Integruje také další forenzní nástroje, a to jak open source, tak komerční, prostřednictvím zásuvných modulů nebo doplňkových modulů v jazyce Java nebo Python.

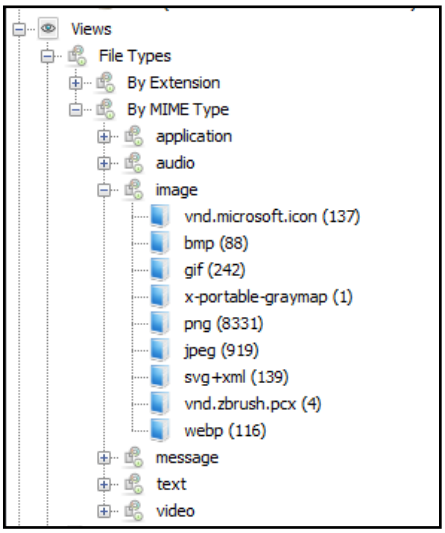
https://github.com/sleuthkit/autopsy/blob/develop/NEWS.txt

Jednoduché grafické rozhraní programu Autopsy (Obrázek 73).



Obrázek 73 - Analýza pomocí pitvy

Obsahuje levou boční nabídku s kategorizovanými informacemi, které identifikují soubory podle typu přípony a typu MIME, ale také podle všech kategorií, do kterých patří (- Kategorizace souborů v aplikaci Autopsy Obrázek 74).



Obrázek 74- Kategorizace souborů v aplikaci Autopsy

Verze

https://github.com/sleuthkit/autopsy/releases/

Zdrojový kód

https://github.com/sleuthkit/autopsy

Úkoly a požadavky

https://github.com/sleuthkit/autopsy/issues

7.

Digitální forenzní případová studie

7. Digitální forenzní případová studie

7.1. Případová studie 1: Hacking pomocí nástrojů O.S. Windows