**Univerzita Hradec Králové**
**Fakulta informatiky a managementu**
**Katedra Informačních technologií**

# Forenzní analýza diskových úložišť – video tutoriály

Bakalářská práce

Autor: Jaromír Bobek
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Svoboda Tomáš Ph.D.

Hradec Králové Listopad 2022

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 25.4.2023 Jaromír Bobek

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Tomáši Svobodovi Ph.D. za metodické vedení práce a podnětné připomínky.

## Anotace

Tato bakalářská práce se zabývá forenzní analýzou disků počítačů na platformě OS Windows. V teoretické části je rozebrán způsob ukládání dat na diskových úložištích, základní principy forenzní analýzy a obvyklé techniky a programy pro získání a následnou interpretaci dat. V praktické části se zabývám konkrétními příklady využití předem vybraného programu se zaměřením na analýzu historie prohlížení webových prohlížečů doplněnou o video tutoriály.



## Klíčová slova

SSD, HDD, sektor, RAM, bitová kopie, hash, OSForensics, SQLite



## Annotation

### Title: Disk Storage Forensics – Video Tutorials

This bachelor thesis deals with forensic analysis of disk storage on Windows OS platform. The theoretical part discusses the way data is stored on disk storage devices, the basic principles of forensic analysis and common techniques and programs for data acquisition and subsequent interpretation. In the practical part, I discuss specific examples of the use of a preselected program, focusing on the analysis of web browsing history with video tutorials.



## Keywords

SSD, HDD, sector, RAM, bit-for-bit copy, hash, OSForensics, SQLite

# Obsah

1 Úvod ... 1

2 Cíl práce ... 2

3 Metodika zpracování ... 3

4 Rozdělení diskových úložišť ... 4

4.1 Typy disků (1) ... 4

4.1.1 Hard-disk drive (HDD) ... 4

4.1.2 Solid-state drive (SSD) ... 8

5 Forenzní analýza ... 15

5.1 Úvod do forenzní analýzy ... 15

5.2 Kdy je třeba analyzovat ... 15

5.3 Programy pro forenzní analýzu ... 17

5.3.1 Autopsy Digital Forensics ... 17

5.3.2 Microsoft COFEE ... 18

5.3.3 FTK Forensic Toolkit ... 19

5.3.4 OSForensics ... 20

5.3.5 Oxygen Forensics Detective ... 21

5.3.6 Závěr ... 22

5.4 Právní stránka forenzní analýzy ... 23

6 Analyzujeme zařízení útočníka ... 25

6.1 První kroky ... 25

6.2 Analýza bitové kopie ... 30

6.2.1 Shrnutí programu ... 61

6.2.2 Podrobná analýza historie webových prohlížečů ... 62

7 Shrnutí výsledků ... 74

8 Závěry a doporučení ... 75

9 Seznam použitých zdrojů ..... 76

10 Přílohy ..... 83

# Seznam obrázků

*Obrázek 1 - Perpendikulární princip.* (4) ..... 5
*Obrázek 2 - Plotna disku* (6). ..... 6
Obrázek 3 - Ukázka nejpoužívanějších rozhraní SSD disků (15). ..... 9
*Obrázek 4 - Výpis ze S.M.A.R.T. u SSD disku.* ..... 9
Obrázek 5 - Princip Hammingova algoritmu pro opravu na 2 KB prostoru (max. chyba je 1 bit) (13). ..... 11
Obrázek 6 - Porovnání běžně používaných algoritmů (13). ..... 11
Obrázek 7 - Blokové schéma SSD disku (14). ..... 12
*Obrázek 8 - Typy paměťových NAND hradel* (16). ..... 13
*Obrázek 9 - Program Autopsy.* ..... 18
*Obrázek 10 - Program Microsoft COFEE* (31). ..... 19
*Obrázek 11 - Program FTK Imager.* ..... 20
*Obrázek 12 - Program OSForensics.* ..... 21
*Obrázek 13 - Program Oxygen Forensic Detective* (35). ..... 22
*Obrázek 14 - Zařízení Forensic UltraDock FUDv6 pro blokaci zápisu na disk* (41). ..... 26
*Obrázek 15 - Box pro NVMe SSD s přepínačem pro blokaci zápisu (IcyBox External Enclosure for M.2 NVMe SSD)* (46). ..... 27
*Obrázek 16 - Blokace zápisu v programu OSForensics.* ..... 28
*Obrázek 17 - Vytvoření image disku v programu OSForensics.* ..... 28
*Obrázek 18 - Průběh vytváření bitové kopie disku v programu OSForensics.* ..... 29
*Obrázek 19 - Možnosti rychlého přidání image disku do virtualizačního programu VMware* ..... 30
*Obrázek 20 - Příklad procházení dat na image disku.* ..... 31
*Obrázek 21 - Informace poslední připojené síti.* ..... 32
*Obrázek 22 - Informace o uživatelském účtu.* ..... 32
*Obrázek 23 - Informace o nainstalovaném operačním systému.* ..... 33
*Obrázek 24 - Timeline všech událostí v ročním zobrazení.* ..... 34
*Obrázek 25 - Timeline všech událostí v denním zobrazení.* ..... 34
*Obrázek 26 - Poslední použité soubory. U spousty souborů a složek chybí časová značka.* ..... 35

*Obrázek 27 - Chronologický seznam událostí v systému.* ..... 36
*Obrázek 28 - Nalezené soubory v kategorii Anti-Forensics Artifacts.* ..... 37
*Obrázek 29 - Seznam posledních stažených souborů včetně zdrojové URL adresy.* ..... 38
*Obrázek 30 - Procházení historie prohlížení internetových prohlížečů hromadně chronologicky.* ..... 39
*Obrázek 31 - Graf četnosti návštěv internetových stránek.* ..... 40
*Obrázek 32 - Vyhledávané pojmy v internetových prohlížečích.* ..... 41
*Obrázek 33 - Uložená hesla v prohlížečích.* ..... 41
*Obrázek 34 - Data z vyplněných formulářů.* ..... 42
*Obrázek 35 - Nalezené soubory sdílené prostřednictvím peer-to-peer sítě.* ..... 43
*Obrázek 36 - Výpis všech uložených cookies z prohlížečů.* ..... 44
*Obrázek 37 - Filtrování konkrétních cookies dle parametrů.* ..... 44
*Obrázek 38 - Výpis v minulosti připojených USB zařízení.* ..... 45
*Obrázek 39 - Příklad připojeného telefonu, kde vidíme jednoznačné IMEI, to může pomoci pro identifikaci a sběru dat z dalších zdrojů.* ..... 46
*Obrázek 40 - Příklad připojeného disku s konkrétním modelovým označením.* ..... 47
*Obrázek 41 - Přiřazené disky k počítači.* ..... 48
*Obrázek 42 - Nalezené přihlašovací údaje a produktové klíče.* ..... 48
*Obrázek 43 - Okno pro vygenerování hashů hesel pro všechny zadané kombinace.* ..... 50
*Obrázek 44 - Možnosti výběru znakových sad.* ..... 50
*Obrázek 45 - Obnova hesla z hashe.* ..... 51
*Obrázek 46 - Hledání souborů hle parametrů a atributů.* ..... 52
*Obrázek 47 - Příklad výsledků vyhledávání v podadresáři souborů s příponou PNG.* ..... 53
*Obrázek 48 - Výpis nalezených smazaných souborů.* ..... 54
*Obrázek 49 - Příklad zobrazeného souboru.* ..... 54
*Obrázek 50 - Příklady nalezených souborů s odlišnou datovou strukturou od přípony v názvu.* ..... 55
*Obrázek 51 - Výpis programů se seznamem složek, ke kterým program přistupuje.* ..... 56
*Obrázek 52 - Příklad výpisu dříve připojených zařízení.* ..... 58
*Obrázek 53 - Náhledy (některých již smazaných) multimediálních souborů.* ..... 59
*Obrázek 54 - Příklad hledání hexadecimálního řetězce.* ..... 60
*Obrázek 55 - Vytvoření a provnání hashe souboru.* ..... 61

*Obrázek 56 - Přehled vyzkoušených webových prohlížečů.* ..... 62
Obrázek 57 - Graf podílů webových prohlížečů (56). ..... 63
*Obrázek 58 - Uživatelská data prohlížeče Chrome.* ..... 64
*Obrázek 59 - Uživatelská data prohlížeče Vivaldi.* ..... 64
*Obrázek 60 - Tabulky v souboru History.* ..... 65
*Obrázek 61 - Příklad struktury tabulky visits.* ..... 66
*Obrázek 62 - Tabulka urls* ..... 67
*Obrázek 63 - Historie prohlížeče Firefox (verze 111).* ..... 67
*Obrázek 64 - Historie prohlížeče Internet Explorer (verze 11).* ..... 68
*Obrázek 65 - Historie v prohlížeči Microsoft Edge.* ..... 69
*Obrázek 66 - Historie v prohlížeči Opera (verze 97).* ..... 69
*Obrázek 67 - Historie v prohlížeči Google Chrome (verze 111).* ..... 70
*Obrázek 68 - Tabulka urls souboru History v prohlížeči Vivaldi (verze 5.7).* ..... 70
*Obrázek 69 - Tabulka urls souboru History v prohlížeči Brave (verze 1.50).* ..... 71
*Obrázek 70 - Tabulka urls souboru History v prohlížeči Seznam.cz (verze 6.19).* ..... 72
*Obrázek 71 - Tabulka HistoryUrls souboru 5.db v prohlížeči Seznam.cz.* ..... 72
*Obrázek 72 - Uložený náhled webové stránky v prohlížeči Safari (verze 5.1.7 pro Windows).* ..... 73

## Seznam tabulek

*Tabulka 1- Typy buněk SSD úložišť.* ..... 12
*Tabulka 2 - Přehled splnění podmínek vybraných programů.* ..... 23

# 1 Úvod

Digitální forenzní analýza je obor, který se zabývá získáváním a následnou interpretací nalezených důkazů v rámci kriminalistického vyšetřování. Obecně se tento obor zabývá forenzní analýzou počítačů, síťových prvků nebo i mobilních telefonů, veškeré uvedená zařízení jsou využívána na denní bázi a z toho důvodu mohou obsahovat cenné informace. Pro získání dat se využívají speciální techniky, které umožní získání dat z různých typů úložišť, ať už se jedná o pevné disky, disky typu SSD, RAM paměť počítače nebo USB flash disky. Tyto nástroje slouží pro hloubkovou analýzu uložených dat, zjistí informace o souborech a složkách nebo je možné obnovit již smazané soubory.

Forenzní analýza je proces, který umožní nalezená data použít jako důkazní materiál u soudu. Je to velmi komplexní proces, který vyžaduje rozsáhlou znalost používaných počítačových systémů, případně i kryptografie a dalších podoborů v oblasti IT. Forenzní analýza se pak zabývá identifikací, získání dat a následné analýze a správné interpretaci.

Jelikož webové prohlížeče na počítači využívá naprostá většina uživatelů počítače, jsou vhodné pro ukázku a celkový úvod do takto rozsáhlého tématu. Webové prohlížeče obsahují spoustu informací z každodenního prohlížení jako je historie o dříve navštívených webových stránkách, uložené přihlašovací údaje spolu s hesly, session tokeny přihlášení a další citlivé informace. Forenzní analýza umožňuje tyto údaje získat a analyzovat je.

V této bakalářské práci se zaměřím v teoretické části na úvod fungování disků v počítačích typu HDD a SSD pro následné pochopení způsobu uložení dat, úvodu a popisu digitální forenzní analýzy, v praktické části následnému úvodu do forenzní analýze prostřednictvím vybraných programů na platformě Windows s konkrétní ukázkou pomocí video tutoriálů.

# 2 Cíl práce

Cílem práce je představení technologií využívaných u diskových úložišť, popsání základních rozdílů včetně shrnutí důležitých aspektů pro dlouhodobé uložení dat s minimalizací rizika poškození nebo ztráty dat na úložištích. Dále pak uvedení a seznámení do tématu forenzní analýzy a popsání důležitých postupů.

Výsledkem práce bude shrnutí základních postupů v případě forenzní analýzy disků u počítačů na platformě Windows a následně podrobné popsání způsobu ukládání dat v případě historie procházení ve webových prohlížečích s doplněním o video tutoriály.

# 3 Metodika zpracování

Práce se bude zabývat způsoby získání dat pomocí forenzní analýzy disku s instalací OS Windows pomocí běžně dostupných programů. Program, který bude v práci využit bude vybrán na základě předem stanovených kritérií.
Práce by měla zodpovědět na následující otázky:

1) Jaké jsou hlavní rozdíly ve způsobu ukládání dat mezi HDD a SSD?
2) Jaká data lze obvykle z disku získat běžně dostupnými forenzními nástroji?
3) Jsou výrazné rozdíly v principu ukládání dat programu mezi jednotlivými webovými prohlížeči?
4) Jsou získaná data uživatelsky čitelná? Nejsou nijak šifrovaná samotným programem?

Výsledkem práce bude zhodnocení použitých postupů a stanovení úspěšnosti získání dat.

# Teoretická část

# 4 Rozdělení diskových úložišť

Pro pochopení, jakým způsobem jsou data ukládána, možnosti obnovení smazaných souborů nebo i, jak by mohlo dojít k poškození a znehodnocení disků ať už úmyslně, případně i neúmyslně při forenzní analýze je důležité znát technické parametry, princip funkce a způsob zápisu dat jednotlivých typů úložišť. Disky a další paměťová média lze rozdělit na několik skupin dle použité technologie a využití. V práci se budu zabývat následujícími typy:

- Hard-disk drive (HDD)
- Solid-state drive (SSD)

Mimo jiné existuje spousta dalších skupin nebo podskupin, které se liší drobnými rozdíly bez zásadního rozdílu v případě forenzní analýzy (například SSHD – kombinace HDD a SDD disku pro často používané soubory), případně zastaralé nebo minimálně používané technologie (USB disky, CD/DVD, diskety, optické, folio nebo LTO disky), které ale mohou mít řadu specifických výhod. Jelikož obvykle systémových diskem v počítačích jsou pouze dva uvedené typy disků, budu se v práci věnovat pouze těm, nicméně ve spoustě případů by jiný typ disku mohl mít malý vliv na způsob forenzní analýzy.

Vzhledem k tomu, že data potřebujeme pro forenzní analýzu, pravděpodobně se jedná o cenná data. Z toho důvodu v technickém popisu budou rozebrány následující parametry pro každý typ úložiště z ohledu na životnost uložených dat.

Oba parametry jsou důležité jak pro analyzovaný disk, tak i pro disk, kam budeme data klonovat pro pozdější uchování.

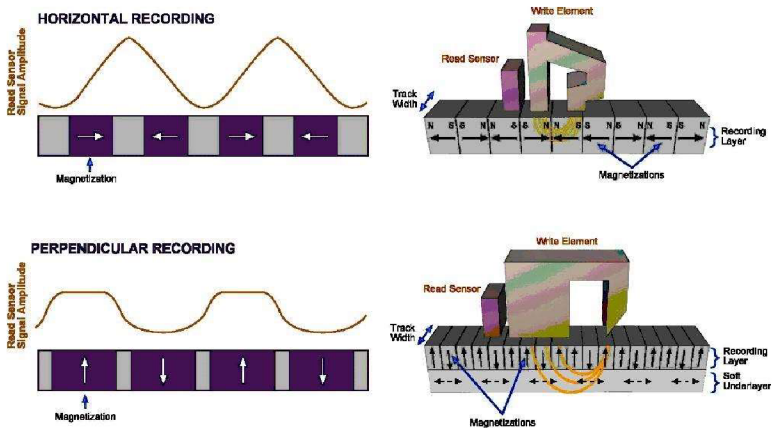
## *4.1 Typy disků (1)*

### 4.1.1 Hard-disk drive (HDD)

#### 4.1.1.1 Základní popis a princip funkce

Jedná se o nevolatilní paměťové médium. Data jsou zapisována a čtena pomocí magnetické indukce. Plotna disku obsahuje následující části:

Disk obvykle obsahuje více ploten, kdy je možné číst z obou stran každé plotny. Pro každou stranu je nutná čtecí hlava. Plotna je tvořena obvykle pevným plátem pevného nemagnetického materiálu z hliníku
(historické disky), skla (zejména 2,5" a menší disky) nebo keramiky
(3,5" disky) a zrnek různých slitin kobaltu z důvodu jeho magnetických vlastností. Původně byly disky navrženy pro čtení a zápis přímo kolmo k ose plotny, pro možnost hustšího zápisu je nyní využíván Perpendikulární princip – kolmý záznam, které využívá průchod magnetického pole i plotnou (2; 3; 4).




*Obrázek 1 - Perpendikulární princip.* **(4)**

a) stopa disku (track)

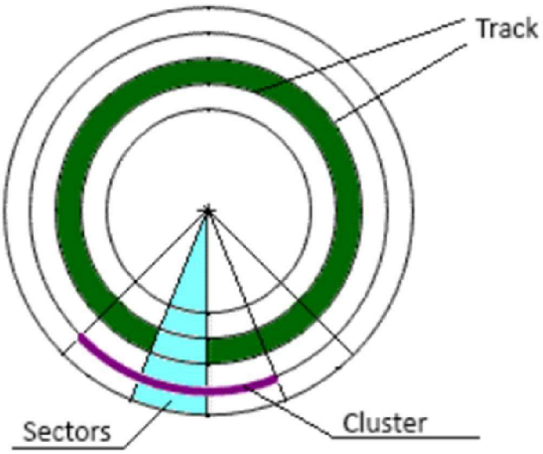
Jedná se o soustředné kružnice na každé plotně číslované od 0 z vnější části plotny. Dříve byl typický poslední index 1023, nicméně z důvodu postupného zvyšování kapacity začal být nedostatečný, a tak byl nejdříve problém řešen přemapováním adres s vyšším indexem řadičem disku, následně proběhl přechod na tabulku GUID Partition Table, poté se již o nastavení stopy na disku nestaral operační systém, ale pouze samotný řadič disku. Magnetická část stopy je široká přibližně 200 nm na vnějším okraji disku a postupně se zužuje k šířce přibližně 20 nm. Velikost magnetických oblastí je aktuálně na hranici technických možností, jelikož v případě, že by oblasti byly příliš blízko u sebe nebo by se jednalo o spojitou magnetickou oblast, docházelo by k ovlivňování sousedních oblastí jejich magnetickým polem, a tak možnému poškození dat již při zápisu (5; 2; 3).

b) sektor (sector)

Sektory jsou kružnicové výseče z plotny disku, přičemž každý sektor měl obvykle 512 bajtů, přibližně od roku 2010 je standardem velikost jednoho sektoru 4096

bajtů. Velikost jednoho sektoru je také pevnou velikostí, kterou na disku zabere jakýkoli menší soubor. V praxi to znamená, že textový dokument o velikosti několik stovek bajtů na pevném disku zabere 4096 bajtů prostoru. Číslování sektorů začíná od indexu 1 (2).

c) cylindr
Cylindr znamená jednu stopu na všech plotnách disku. Řadič disku tak ukládá a čte data v jednu chvíli na více stop najednou, a tak dochází k vyšší rychlosti.




*Obrázek 2 - Plotna disku* **(6).**

Disky jsou rozděleny do velikostí dle průměru plotny v palcích. Nejčastějšími variantami jsou velikosti 3,5” a 2,5”. Větší rozměr je typický pro stolní počítače, NAS servery a další nepřenosná zařízení, případně externí disky s vysokou kapacitou. Rozměr 2,5” se vyskytuje zejména v noteboocích a externích discích s USB řadičem. U určitých specifických zařízení se lze setkat s menšími rozměry (v historii například telefon Nokia N91 nebo hudební přehrávač iPod Classic (7), u aktuální generace zařízení se již menší než 2,5“ pevné disky prakticky nevyskytují).

#### 4.1.1.2 Životnost disku

Životnost disku a i uložených dat lze rozdělit na dvě zásadní skupiny:

a) životnost při připojeném napájení a čtení/zápisu na disk
b) životnost dat po odpojení napájení a uložení disku na bezpečné místo

Rozdělení je zásadní, jelikož při soustavné čtení a zápisu je nejpravděpodobnější, že dojde k mechanickému poškození a tím znepřístupnění dat, případně i poškození disku čtecí

hlavou. V případě uložení na bezpečné místo mohou být data ztracena zejména rozpadem magnetického pole, které slouží jako datová informace (8).

#### *4.1.1.2.1 Životnost disku při připojeném napájení*

Disk obsahuje spoustu mechanických komponent, kdy jedna vadná součást obvykle způsobí částečnou nebo úplnou ztrátu možnosti přečíst či zapsat data. K poškození může dojít buď během běžného provozu nebo vnějšími vlivy jako vystavení extrémním teplotám, tekutinám nebo silnému magnetickému poli. K poškození může také dojít nárazem, kdy například čtecí hlava poškodí vrstvu na plotně disku (6). Z toho důvodu může být při forenzní analýze důležité zajišťované disky hlídat před například zaměstnancem firmy, odkud jsou zajištěné důkazy, jelikož by mohl shozením disku na zem data znehodnotit.

Poruchovost disků je výrobci udávána jako střední doba mezi poruchami (MTBF) nebo roční poruchovost (AFR). Například Seagate u svých disků uvádí střední dobu mezi poruchami 1,2 milionu hodin a roční poruchovost 0,73 % (9).

Dle datového centra Backblaze, Inc. na vzorku 25 000 disků dojde k selhání disku během trvalého provozu v průběhu prvního cyklu, který trvá 1,5 roku disk selže v 5,1 % případů ročně, v dalším cyklu poruchovost klesne na 1,4 % a po třech letech se zvýší na 11,8 % ročně.

#### *4.1.1.2.2 Životnost disku po uložení bez napájení*

Při uložení dat na disk a odpojení od počítače může dojít ke ztrátě dat několika způsoby: (10; 11)

a) rozpad magnetického pole

   Permanentní magnety ztrácejí své magnetické pole přibližně o 1 % za rok. V tomto případě by po 69 letech bude s velkou pravděpodobností většina sektorů poškozena, jelikož magnetická zrnka ztratila polovinu své síly. Tomu lze předejít například znovu zapsáním dat na disk, jelikož dojde k obnově domén, případně archivací nějakým algoritmem, který podporuje obnovu dat i když je část dat poškozená.

b) geomagnetická bouře

V některých oblastech jsou magnetické vlivy tak silné, že může dojít k poškození dat na disku, případně při uložení disku na místo výskytu dalších magnetických polí. Tomu lze předcházet uložením na místo, kde k takovým vlivům dochází co nejméně nebo jsou alespoň částečně odizolované – například do sklepa.

c) odpojení disku ještě před zapsáním všech dat

Pro urychlení přístupu na disk disky používají vyrovnávací paměť, kam se data nejprve nahrají a poté je až řadič disku uloží na disk. Pokud dojde k odpojení ještě před zapsáním všech dat, data ve vyrovnávací paměti se ztratí.

d) koroze

Vlivem vlhkosti ve vzduchu může dojít ke korozi částí disku a tak poškození ať už elektroniky, tak i mechanických částí disku.

e) zastarání technologie

Tím, jak vývoj elektroniky postupuje, nemusí být po dlouhé době jednoduché sehnat zařízení, které umí komunikovat s původní technologií nebo datovým formátem disku.

Obecně lze tedy říci, že data na disku vydrží přibližně 5 let, poté je vhodné je opět zálohovat na nový disk, případně i převést do nového formátu. U cenných dat je doporučováno data zálohovat na nové úložiště po přibližně třech letech (11).

### 4.1.2 Solid-state drive (SSD)

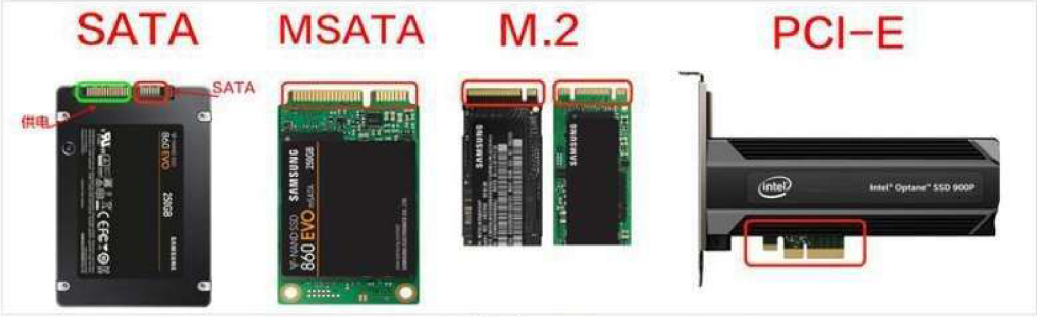
#### 4.1.2.1 Základní popis a princip funkce

Jedná se nevolatilní paměťové médium. Oproti HDD neobsahuje žádné pohyblivé součásti, má obvykle menší spotřebu energie, nulovou přístupovou dobu a vyšší rychlosti. Také mají vyšší pořizovací cenu za jednotku kapacity. Tento cenový rozdíl se však postupem vývoje zmenšuje.

Samotný SSD disk se skládá z několika částí: (12; 13; 14)

a) rozhraní (host interface)

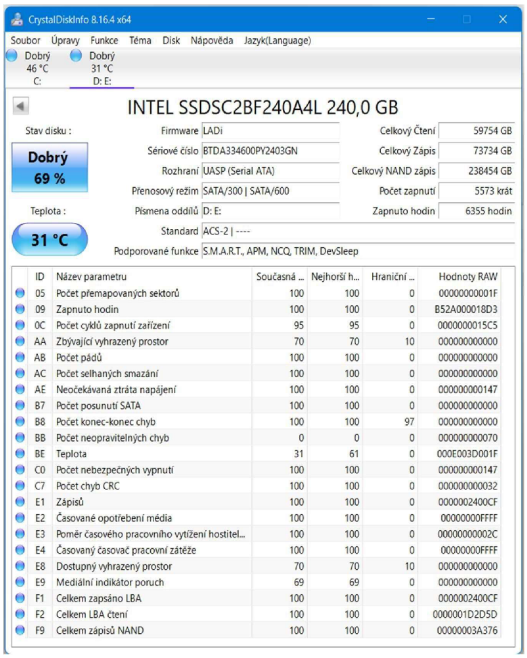
Slouží pro komunikaci a přenos dat s počítačem, typicky se jedná o SATA řadič, PCIe, případně USB.




Obrázek 3 - Ukázka nejpoužívanějších rozhraní SSD disků **(15)**.

b) S.M.A.R.T.

Jedná se o systém pro monitorování stavu disku. Lze zobrazit například počet selhání smazání, celkový objem zapsaných nebo přečtených dat nebo zbývající životnost disku, to by měl být jeden z nejdůležitějších parametrů pro predikci možnosti selhání. V případě, že by se blížil počet přepsání, řadič disk přepne do režimu pouze pro čtení, aby si uživatel mohl data ještě zálohovat před tím, než by mohlo docházet k poškození dat. Ve S.M.A.R.T. ale nelze například zjistit případ, kdy by na nějaké oblasti disku docházelo k nadměrnému opotřebení buněk.




*Obrázek 4 - Výpis ze S.M.A.R.T. u SSD disku.*
Zdroj: vlastní

c) Vyrovnávání opotřebení (wear leveling)

Každá NAND buňka disku má omezený počet cyklů zápisu. Wear Leveling umožňuje rozložit nutné opotřebení buněk do všech aktuálně dostupných. Pokud by docházelo pouze k zápisu na jedno fyzické místo, mohlo by brzy dojít k výraznému opotřebení, a tak ztrátě nebo poškození dat už po zápisu. Řadič tedy používá svůj algoritmus pro rozdělení mezi zbývající bloky rovnoměrně.

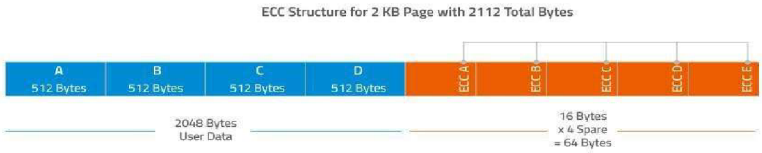
d) Poruchy čtení a programu (read and program disturb)
Postupným vývojem dochází ke zmenšování potřebného fyzického prostoru NAND hradel pro uložení jednotky kapacity. V případě, že dochází ke čtení jedné buňky, pokud by byla ihned čtena vedlejší buňka, bude ovlivněna čtením předchozí, a tak by došlo k přečtení upravených dat. Řadiče tedy využívají různé algoritmy pro předcházení tohoto jevu.

e) Šifrování a dešifrování (encrypt abd decrypt engine)
Vybavenější disky nebo disky určené pro podnikové prostředí jsou často vybaveny dedikovaným hardwarovým šifrovacím obvodem. Obvykle je využíváno 256bitové šifrování AES.

f) Vyrovnávací paměť a mezipaměť (buffer/cache)
Řadič pro rychlou práci s diskem využívá jinou rychlou volatilní paměť, obvykle SRAM/DRAM. Cache slouží k tomu, aby operační systém v počítači mohl na disk data zapsat a zároveň disk mohl data organizovat, nulovat buňky apod. bez viditelného zpomalení rychlosti.

g) Mikroprocesor (RISC processor)
Procesor slouží pro celé řízení běhu disku. Jeho výkon ovlivňuje výkon celého řadiče.

h) Detekce a oprava chyb (EEC engine)
Slouží pro opravu několika poškozených bitů při čtení nebo zápisu. Detekce chyb je důležitá zejména u levných disků, kde je ukládání více bitů na jednu NAND buňku – čím je více bitů v jedné buňce, tím více hrozí jejich vzájemné ovlivňování a tak i poškození dat. Maximální počet bitů, který dokáže disk sám opravit závisí na použitém algoritmu.




Obrázek 5 - Princip Hammingova algoritmu pro opravu na 2 KB prostoru (max. chyba je 1 bit) **(13)**.

| | Hamming | Reed-Solomon | BCH | LDPC |
|---|---|---|---|---|
| Error Correction | Single-bit | Single-bit (Can detect two-bit) | Multi-bit | |
| Flash Type | SLC | MLC | MLC/TLC | |
| Error Type | Scattered | Burst | Scattered | |
| Soft Bit Decoding | No | | | Yes |
| Error Correction Capability | Limited | High | | |
| Performance | Medium | | High | Very High |

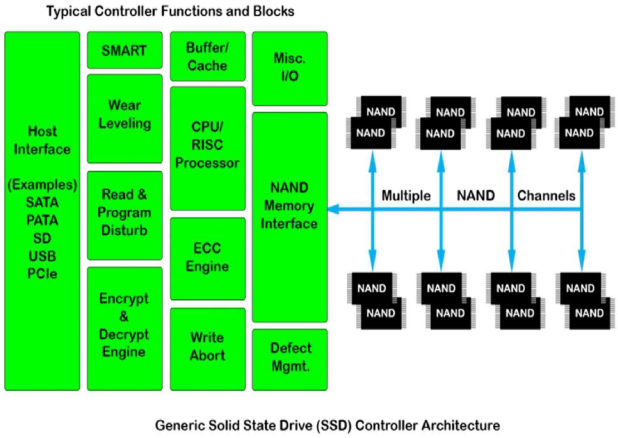
Obrázek 6 - Porovnání běžně používaných algoritmů **(13)**.

i) Blokace zápisu (write abort)
Tento obvod slouží zejména na chvíle, kdy dojde k náhlému výpadku napájení během zápisu a tak je nutné ještě data z mezipaměti přenést na fyzický disk a také zajišťuje, aby nedošlo k poškození metadat a firmware disku.

j) I/O rozhraní (Misc. I/O)
Slouží pro ovládání a spínání jednotlivých komponent řadiče, například spínání samostatných NAND bloků.

k) Rozhraní NAND paměti (NAND memory interface)
Komunikuje přímo s NAND moduly. Může být jeden, ale i 10 a více. Každý kanál je obvykle spojen s jedním nebo dvěma NAND bloky.

l) Správa chyb (defect mgmt.)
V případě, že řadič zjistí chybu čtení nebo zápisu z NAND hradel, pokusí se samoopravným mechanismem data opravit, daný adresní prostor přestane využívat a namapuje rezervní adresní prostor.



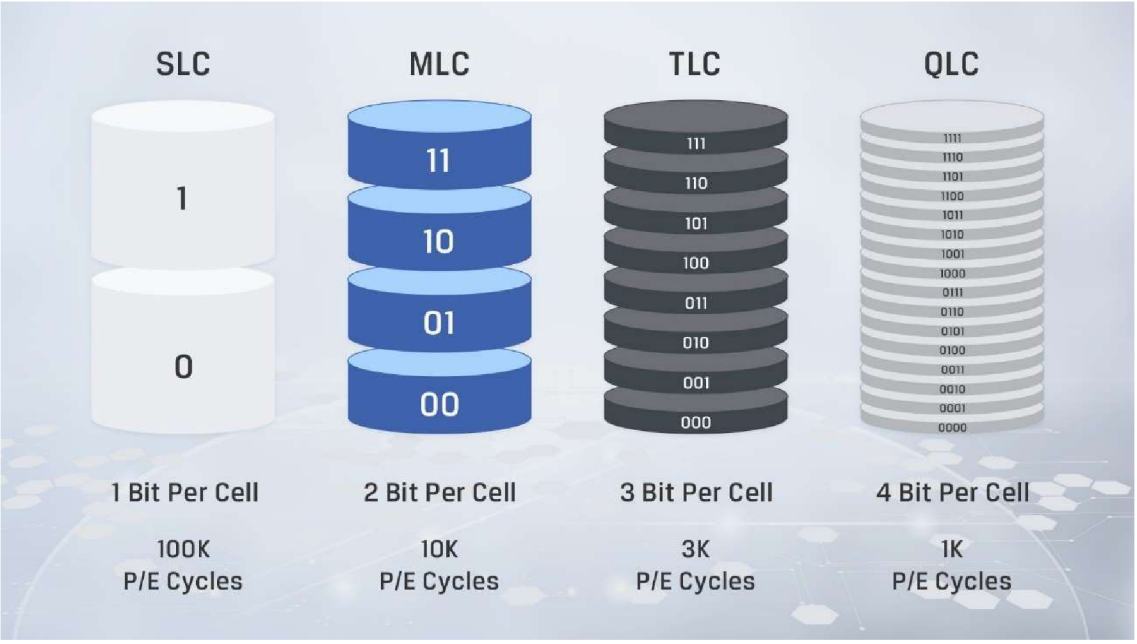

Obrázek 7 - Blokové schéma SSD disku **(14)**.

Paměťová NAND hradla mohou být tvořeny různými typy buněk – jednotlivé typy se liší zejména počtem uložených bitů na jednu buňku, životností a pořizovací cenou. Zároveň také čím více bitů musí být uloženo v jedné buňce, tím více musí řadič rozlišovat úrovní, a tak je větší pravděpodobnost, že dojde k nějaké chybě. Samoopravné mechanismy jsou navrhovány tak, aby u buněk, kde je uloženo více bitů byl algoritmus schopen opravit více chyb najednou. Snižující se počet přepisů je dán tím, že při změně například každého ze čtyř bitů je přepsána jedna a ta samá buňka.

Nejčastější typy buněk jsou uvedeny v tabulce: (16)

| **Typ** | **Počet bitů** | **Počet přepsání** | **Poznámka** |
|---|---|---|---|
| SLC | 1 | 100 000 | vyšší rychlosti |
| MLC | 2 | 10 000 | eMLC dosahuje většího počtu přepisů |
| TLC | 3 | 3 000 | |
| QLC | 4 | 1 000 | nejlevnější, nejpomalejší |

*Tabulka 1- Typy buněk SSD úložišť.*




*Obrázek 8 - Typy paměťových NAND hradel* **(16)**.

## 4.1.2.2 Životnost disku

### *4.1.2.2.1 Životnost disku při připojeném napájení*

Disk neobsahuje mechanické komponenty, které by se mohly poškodit například otřesy nebo pádem jako u pevných disků. V discích má obvykle nejnižší životnost přímo paměťový modul, nicméně jelikož disky jsou běžně používány pouze posledních deset let, není tolik statistických dat jako u HDD. Základní metrikou pro zjištění očekávané zbývající životnosti může být parametr Terabytes Written (TBW). Ten lze zjistit ve S.M.A.R.T. disku a očekávanou životnost uvádí výrobci u konkrétních modelů disků. Zároveň parametr TBW obvykle omezuje prodlouženou záruku (například záruka 5 let nebo do 3200 TBW – Kingston KC3000 (17)). U aktuálně prodávaných disků se parametr udávávané TBW výrobcem pohybují v rozmezí přibližně 250–7000 TBW dle ceny a zaměření disku, nejprodávanější disky dosahují hodnot okolo 1000 TBW (18). Při běžném používání disku jako systémový disk v počítači obvykle kapacita disku morálně zastará dříve, než by bylo na disk přepsáno tolik dat. Pro příklad u 500 GB disku s 1000 TBW by bylo nutné každý den zapsat přibližně 550 GB dat po dobu 5 let. Výjimka může nastat u serverů nebo specifických výpočetních stanic, případně pokud z důvodu nějaké chyby některý z programů velmi vytěžuje disk (ESET a zapnutý idle scan, Outlook a vadné *.pst a další (19)). Částečně prodlužuje životnost disku funkce TRIM, která po smazání dat pouze zašle

řadiči informaci, které bloky již neobsahují žádná data, na disku je fyzicky nesmaže, ale dojde k přepsání až při zapsání dalších dat, zároveň řadič přednostně využívá méně opotřebené bloky paměti (20). To může být pro forenzní analýzu podstatné, jelikož smazaná data se na disku stále nacházejí.

#### *4.1.2.2.2 Životnost disku po uložení bez napájení*

Data jsou v NAND blocích uložena formou elektrického náboje (kapacita C [F]). Postupem času dochází k samovybíjení, pokud by se nějaké hradlo vybilo pod určitou mez, dojde ke změně 1–4 bitů dle technologie disku (viz. typy buněk výše). Tomu zabraňuje modul správy chyb, který je schopen kompenzovat několik bitů se špatnými daty a zároveň řadič, ten data po připojení napájení opět obnoví (vrátí požadovanou hodnotu náboje do NAND hradla) (14; 21).

Životnost disku při pravidelném používání bývá obvykle 5 a více let, dle opotřebení bloků. Oproti HDD je ale problém s tím, že pokud dojde k poškození disku, data ve většině případů je složité nebo úplně nemožné obnovit (22).

V případě uložení disku bez připojeného napájení dochází ke ztrátě dat následujícími způsoby:

a) ztráta elektrického náboje
   Nejpravděpodobnější varianta, pokud by nedošlo k mechanickému poškození. Pokud dojde k odpojení disku od napájení, elektronika již nemůže obnovovat náboj v zapsaných blocích. Postupem času tak může dojít až k takové úrovni, že opravné algoritmy nebudou schopny poškozené bity obnovit. Dle JEDEC standardu by měl být disk čitelný po roce od odpojení napájení při uložení za teploty 30 °C, u podnikových disků po 3 měsících při 40 °C.
b) koroze
   Vlhkost vzduchu může způsobit korozi a následné poškození el. obvodů disku.
c) zastarání technologie
   Tím, jak vývoj elektroniky postupuje, nemusí být po dlouhé době jednoduché sehnat zařízení, které umí komunikovat s původní technologií nebo datovým formátem disku.

# 5 Forenzní analýza

## 5.1 Úvod do forenzní analýzy

Digitální forenzní analýza je proces, kdy dochází k získávání dat a následné analýze a interpretaci z elektronických zařízení jako jsou telefony, tablety nebo počítače pro účely vyšetřování, soudního nebo trestního řízení jako důkazní materiál. Cílem analýzy je nalézt veškeré vhodné a usvědčující důkazy pro potvrzení nebo vyvrácení tvrzení v trestním nebo soudním řízení (23).

V případech forenzní analýzy jsou používány zejména následující metody: (23)

- bitová kopie
- analýza dat na disku
- analýza dat aplikací a programů
- analýza provozu na síti
- analýza systémových souborů

V rámci této práce se budu zabývat zejména prvními třemi body. V rámci analýzy je zapotřebí veškeré důkazy (tedy i data) zabezpečit tak, aby nedošlo k jejich úmyslné či neúmyslné změně či znehodnocení, jelikož data jsou obecně velmi náchylná ke změně – nestálá, případně by mělo být prokazatelné, že ke změně nedošlo například funkcí kontrolního součtu. Je tedy nutné zajistit neporušenost a dodržování standardů a předpisů, aby mohly být v soudním řízení použity (24).

Forenzní analýzou se ale nezabýváme jen ve chvíli, kdy někdo spáchá trestný čin prostřednictvím daného zařízení, ale i v případech, kde dojde k napadení vnitřní sítě, napadení počítače škodlivým malwarem apod. pro následné vyšetření, jakým způsobem došlo k prolomení bezpečnostních ochran, stanovení rozsahu škod a i k určení viníka, vše tedy záleží pouze na rozsahu zanechaných usvědčujících dat a na schopnostech vyšetřovatele data najít a správně interpretovat.

Jelikož je stále více trestných činů provedeno za přítomnosti moderních technologií, je stále důležitější sbírání důkazních materiálů touto formou, aby docházelo k objasnění a následné dosažené spravedlnosti (25).

## 5.2 Kdy je třeba analyzovat

Případy, kdy je třeba provést forenzní analýzu lze rozdělit na dvě hlavní skupiny. Postup je v obou případech podobný, nicméně určité kroky se liší anebo je možné je vynechat.

Obecně ale nelze uvést jediný manuál s přesnými kroky a postupy, jelikož každá situace je individuální, záleží na spoustě okolností, například zda můžeme server odpojit, vypnout, na čase, který můžeme analýze věnovat a tak dále (26).

Hlavní kategorie jsou následující:

a) analyzujeme zařízení útočníka
   Tato kategorie zahrnuje případ, kdy dojde k trestnému činu (nebo jiné události) a dojdeme k závěru, že v jeho zařízení mohou být důkazní materiály pro potvrzení nebo vyvrácení činu. Obvykle lze hledat různé dokumenty, historii prohlížení v internetovém prohlížeči, historii e-mailové nebo chatové komunikace, zdrojové kódy naprogramovaných škodlivých programů apod.
   Jelikož k zařízení musíme mít fyzický přístup a ten získáme až po delší době po incidentu, analyzujeme data obvykle jen na discích nebo jiných médiích, například kopie obsahu RAM paměti počítače (RAM dump) je již pravděpodobně zbytečná a další informace by neposkytla. Také se data na zařízení po zabavení již nemění, a tak máme více času na samotnou analýzu bez přímé nutnosti jednotlivé úkoly prioritizovat a přijít se závěrem v co nejkratším čase.
b) analyzujeme naše zařízení, na kterém došlo k incidentu
   Obecně samotné organizace mají vlastní manuály, jak v různých případech postupovat. V těchto případech je nutné si stanovit, zda můžeme zařízení úplně odstavit. Může jít například o případ, kdy jde o důležitý server, který ale nebyl zasažen takovým způsobem, aby to plně bránilo obvyklému používání. Opačným případem může být ransomware, který postupně šifruje všechna data v síti a tak je žádoucí, aby bylo spojení co nejdříve ukončeno a došlo k minimalizaci budoucích škod. Obecně je ale dobrým začátkem počítač úplně nevypínat a nejdříve provést RAM dump, abychom si uložili zbytky škodlivého kódu, jelikož po vypnutí počítače by došlo k vymazání paměti RAM a hrozí, že určitá data již nebudeme mít k dispozici. Dobře napsané škodlivé programy mají často za cíl i smazat data nutná k identifikaci, jakým způsobem mohl být kód spuštěn nebo informace o jeho tvůrci. Je tedy vhodné získat informace ze všech možných zdrojů. Následuje bitová kopie systémového disku, obvykle při vypnutém počítači, ale v závislosti na okolnostech i při zapnutém, veškerá posbíraná data následně analyzujeme a hledáme důležité informace nebo nesrovnalosti.

V následujících kapitolách se budu zabývat zejména první kategorii, jelikož cílem praktické práce bude forenzní analýza historie webových prohlížečů.

## 5.3 Programy pro forenzní analýzu

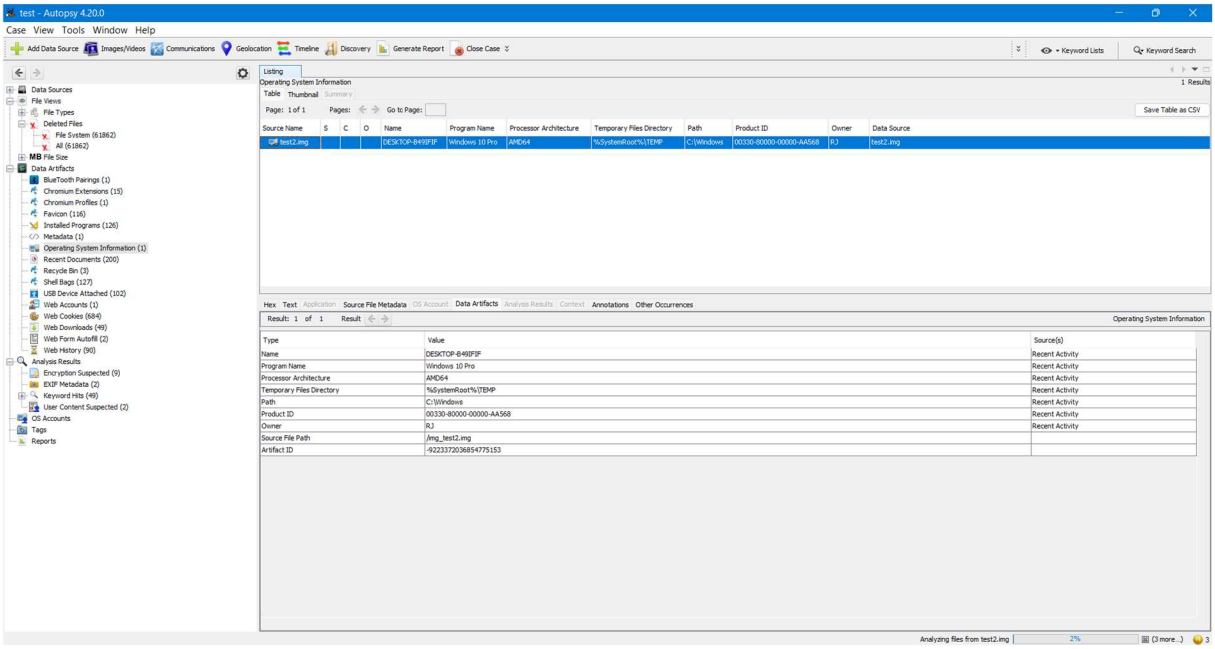
Programů, které zprostředkují nástroje na analýzu dat existuje řada. V přehledu uvedu seznam prověřených programů spolu s jejich krátkým popisem funkčnosti a rozdílů oproti jiným a následně vyberu, kterým se dále budu zabývat v této práci. Programy jsou v seznamu uvedeny abecedně.

### 5.3.1 Autopsy Digital Forensics

Program Autopsy je vyvíjen společností Basis Technology Corp. za podpory open-source komunitního vývoje. Program je zaměřen na použití s rozšiřujícími moduly, které je možné získat z různých zdrojů – od společnosti stojící za nástrojem nebo od komunity. Dále umožňuje členění zjištěných dat do případů, zároveň je možné na jednom případu pracovat v týmu pracovníků. Software je dostupný zdarma pod licencí GPL, zpoplatněna je pouze případná technická podpora (27).

Klíčové vlastnosti:

- jednoduché prostředí
- méně funkcí
- automatické hledání potencionálně důležitých dat
- zobrazení dat v timeline, smazaných souborů, indexovaných hledání, hashování souborů a další
- licence pro použití zdarma
- poměrně pomalé procházení, velmi pomalé načítání bitové kopie (jednotky až desítky hodin)

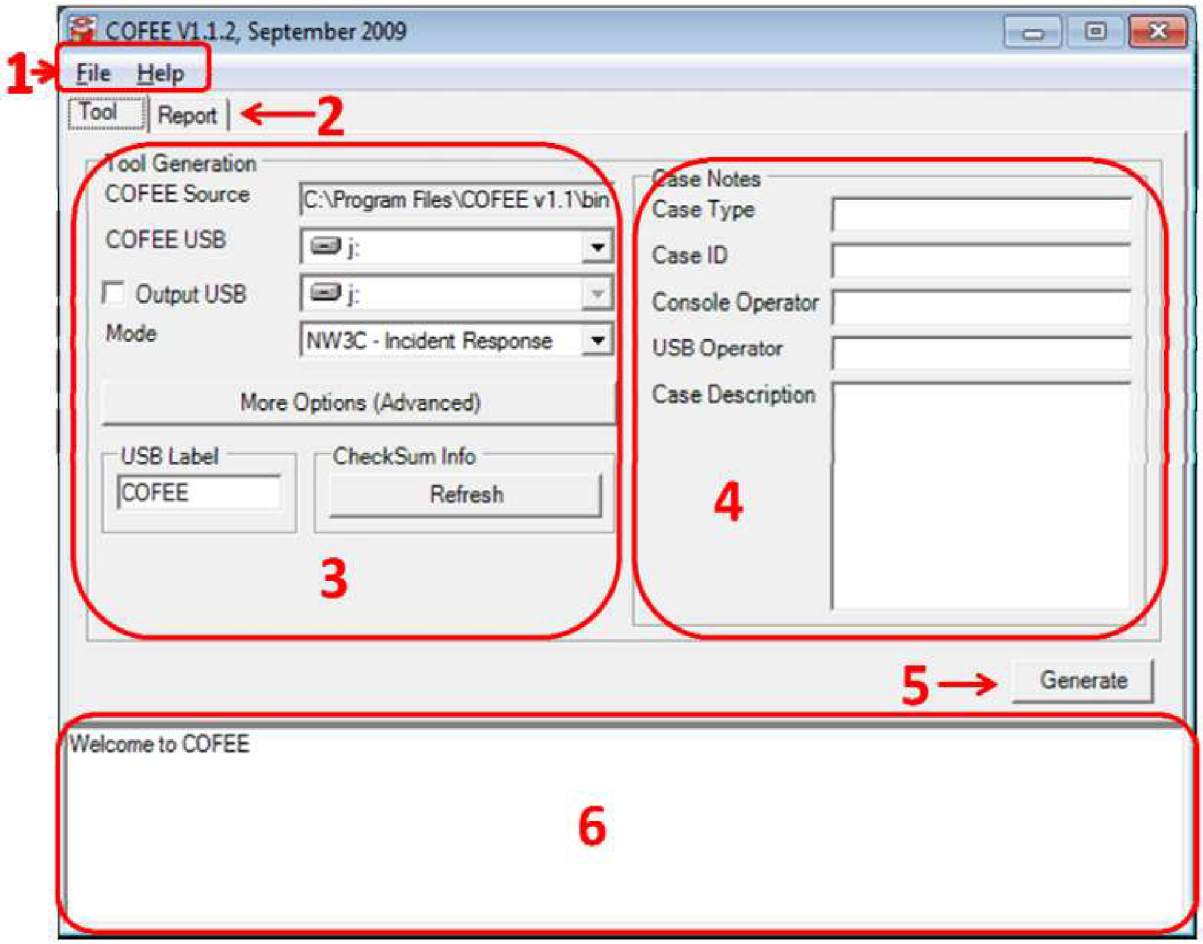



*Obrázek 9 - Program Autopsy.*
Zdroj: vlastní

### 5.3.2 Microsoft COFEE

Jedná se o nástroj pod celým názvem Computer Online Forensic Evidence Extractor vyvíjený společností Microsoft pro živou forenzní analýzu počítačů s OS Windows poskytovaný zdarma orgánům činném v trestném řízení. Software není běžně dostupný, nicméně v roce 2009 unikl veřejně ve verzi 1.1.2 spolu s dokumentací.

Z důvodu nedostupnosti nástroje se nástrojem nebudu dále zabývat (28; 29; 30).

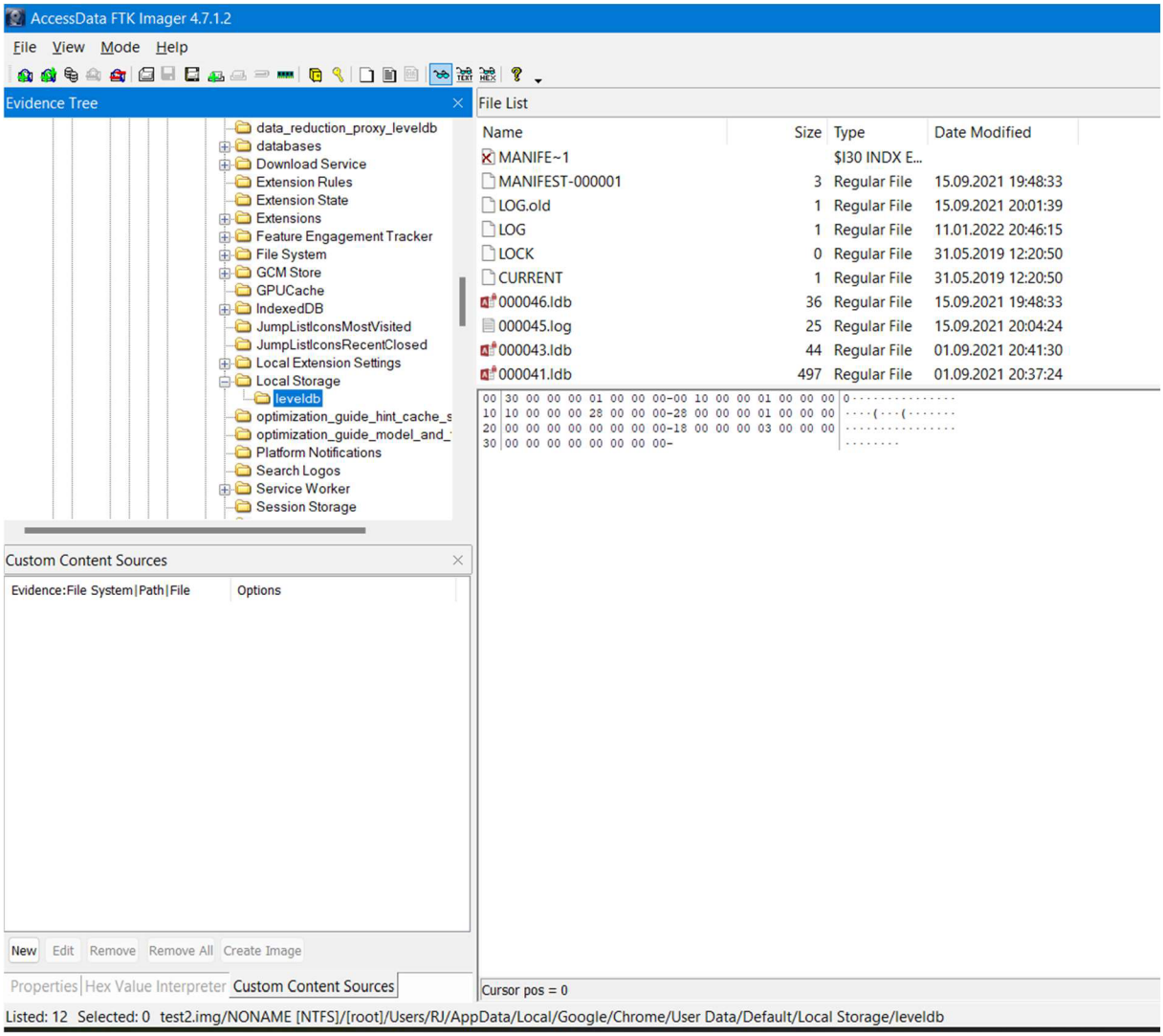



*Obrázek 10 - Program Microsoft COFEE* **(31)**.

### 5.3.3 FTK Forensic Toolkit

Software se zaměřuje zejména na prohledávání souborů na disku, hledání textový řetězců a vytváření databází slov pro slovníkový způsob prolomování hesel. Dokáže počítat hashe po vytoření image disku pro porování integrity. Je distribuován zdarma základní balíček FTK Imager, rozšiřující licence jsou poskytovány za individuální smluvní poplatek (32). Klíčové vlastnosti:

- složitější uživatelská přívětivost
- méně funkcí
- zaměřuje se převážně na procházení surových dat




***Obrázek 11 - Program FTK Imager.***
Zdroj: vlastní

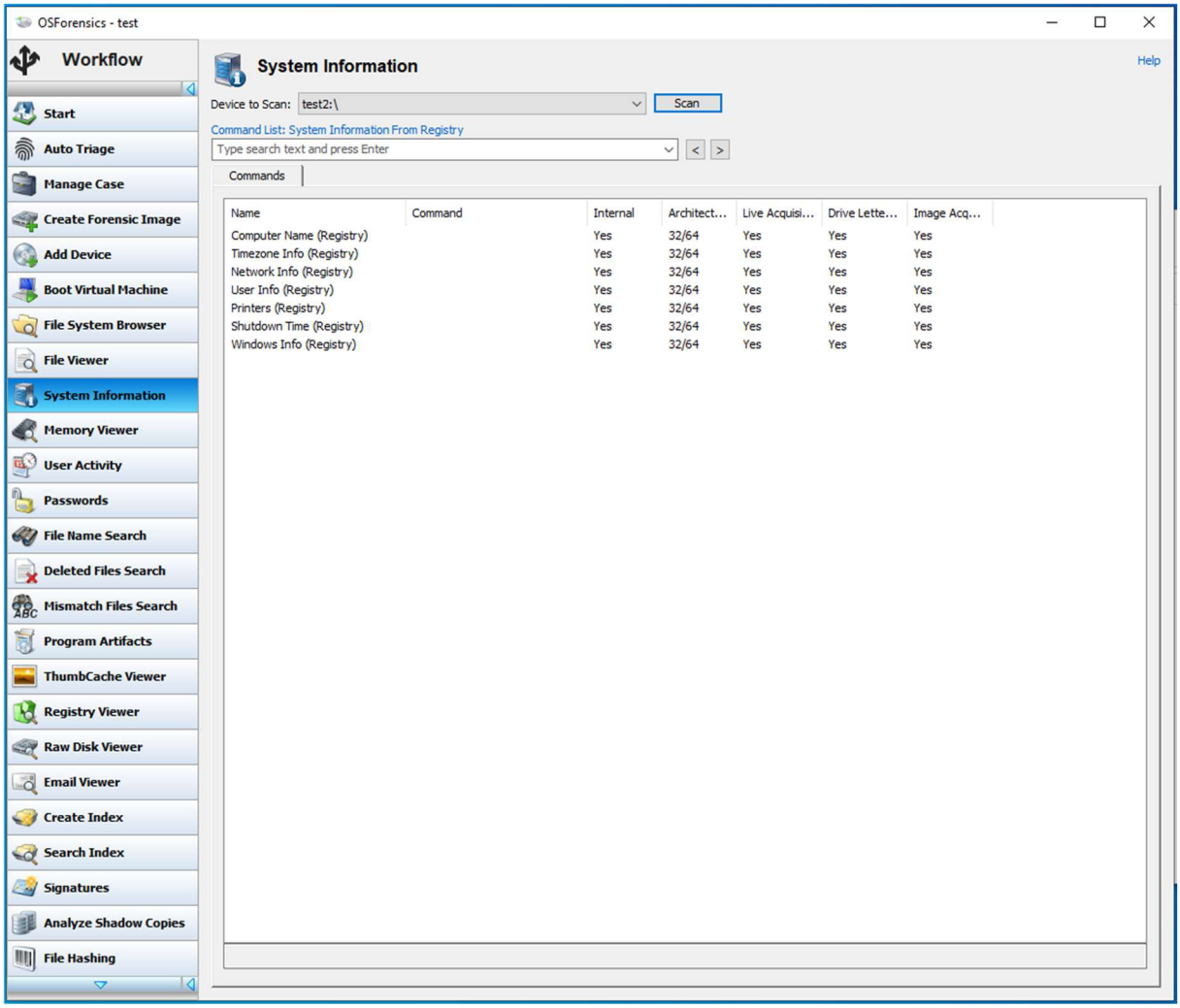
### 5.3.4 OSForensics

Program se zaměřuje na komplexní správu případu, přidávání jednotlivých nalezených souborů a dat a umožňuje práci v týmu. Zvládá roztřídění nalezených potencionálně důležitých dat do kategorií, procházení disku po souborech nebo RAW obsah disku, vytváření a procházení dumpu RAM paměti. Je možná práce s vytvořenými kopiemi pamětí nebo na živém počítači. Je poskytován placeným předplatným na každého uživatele nebo doživotní licencí s omezením délky softwarové podpory, případně zkušební verzi zdarma (33).

Klíčové vlastnosti:

- rozsáhlý výběr nástrojů

- jednoduché použití
- třídění nalezených dat do timeline, kategorií nebo procházení souborů disku
- možnost spustit dříve vytvořený image prostřednicvím VMware Workstation




*Obrázek 12 - Program OSForensics.*
Zdroj: vlastní

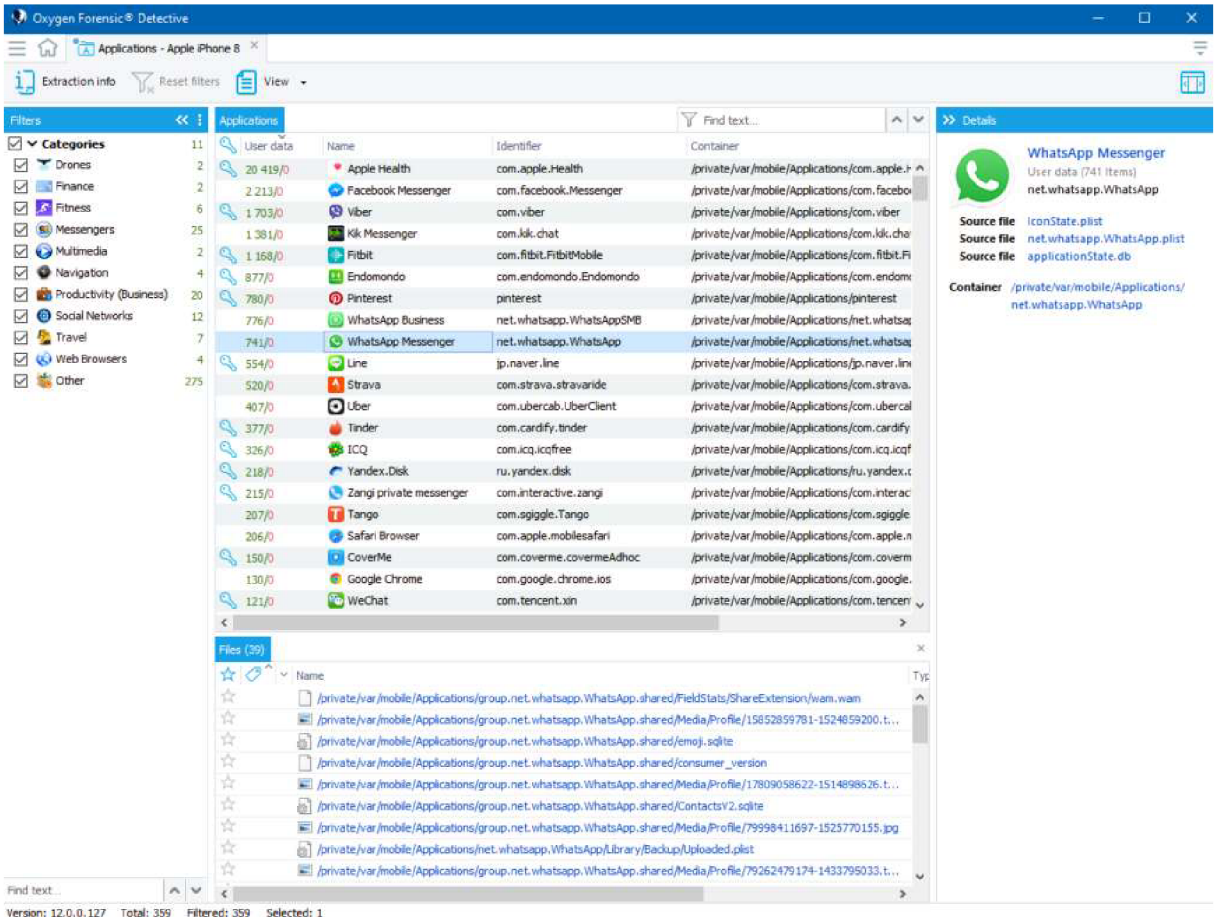
### 5.3.5 Oxygen Forensics Detective

Software umožňuje správu případů, organizaci práce v týmu nebo komunikaci s dalšími nástroji pro hlubší analýzu. Zaměřují se na rozbor dat z různých zařízení od počítačů přes telefony po drony, extrakci textů z obrázků, analýzu klíčových slov a další. Dle jejich webové prezentace i umožňuje obejít odemykání telefonu pomocí pinu na většině používaných telefonů s iOS (pouze zařízení s provedeným jailbreakem) a Androidem

(neměla by být vyžadována root oprávnění). Nepodařilo se mi získat ani zkušební verzi software, z toho důvodu jsem jej nemohl nijak vyzkoušet (34).

Klíčové vlastnosti:

- extrakce dat z messengerů
- podpora velké škály zařízení
- vyhledávání a filtrování dat
- rozbor uložených dat spousty uživatelsky oblíbených aplikací
- poměrně vysoké hardwarové nároky




*Obrázek 13 - Program Oxygen Forensic Detective* **(35)**.

### 5.3.6 Závěr

Předchozí souhrn slouží pro výběr jednoho programu, který budu následně využívat v praktické části. Pro výběr vhodného kandidáta jsem si stanovil tyto podmínky:

1. Pravidelně aktualizován (poslední verze není starší než 1 rok).
2. Dostupný pro OS Windows verze 10 nebo novější.
3. Dostupný pro použití zdarma, se zkušební licencí zdarma bez omezení funkcionali nebo za poplatek do $50 za licenci pro jeden počítač.

4. Nástroj obsahující více funkcí.
5. Nástroj analyzující data nejčastějších webových prohlížečů.

Splnění podmínek jednotlivých programů je znázorněno v následující tabulce:

| **Název** | **Aktualizace** | **Pro Windows** | **Licence** | **Více funkcí** | **Webové prohlížeče** |
|---|---|---|---|---|---|
| **Autopsy DF** | ANO | ANO | ANO | ANO | ANO |
| **MS COFEE** | ? | ANO | NE | ? | ? |
| **FTK** | ANO | ANO | NE | ANO | ANO |
| **OSForensics** | ANO | ANO | ANO | ANO | ANO |
| **Oxygen FD** | ANO | ANO | ? | ANO | ANO |

*Tabulka 2 - Přehled splnění podmínek vybraných programů.*

Na základě tabulky výše jsem dospěl k závěru, že podmínky splňují nástroje Autopsy Digital Forensics a OS Forensics. Jelikož jsou funkčně poměrně srovnatelné, ale načítání bitové kopie v programu Autopsy DF trvalo desítky hodin a celkově je program velmi pomalý, zvolil jsem pro použití v praktické části program OS Forensics.

## 5.4 Právní stránka forenzní analýzy

Právo uživatele na soukromí je v civilizované společnosti důležitým aspektem každého občana. Z toho důvodu je nutné mít stanovená přesná pravidla v jakých je možné forenzní analýzu využít.

Jelikož se práce právní stránkou důkladně nezabývá, ale zároveň přímo s tématem souvisí, tato část práce bude brána pouze jako krátký přehled a úvod do tématu.

Jakými přesně se forenzní analýza bude řídit zákony je dáno zejména účelem, proč a z jakého důvodu je k analýze přistupováno.

Obvykle lze důvody rozdělit na dvě kategorie:

a) analyzuji vlastní zařízení
   Například došlo k infikaci cizím škodlivým softwarem a snažím se zjistit, jakým konkrétním způsobem se do počítače dostal a posbírat co nejvíce doprovodných informací, například které soubory mohly uniknout mimo místní síť. V takovém případě se jedná o naše zařízení, naše data a tak můžeme své zařízení bez omezení procházet, tedy provést forenzní analýzu na základě práva vlastnit majetek a nakládat s ním, tyto práva upravuje Občanský zákoník (zákon č. 89/2012 Sb) (36).

b) analyzuji cizí zařízení
   Pro příklad byl spáchán trestný čin a pracovník policie sbírá důkazy pro jednoznačnou identifikaci a usvědčení pachatele. Forenzní analýza tak může být jedním z důkazů v řízení před soudem (37; 38).

   Zákony, které upravují proces získání důkazů k soudu jsou následující:

   - Občanský soudní řád (zákon č. 99/1963 Sb.) (39)
   - Trestní řád (zákon č. 141/1961 Sb.) (37)
   - Správní soudní řád (zákon č. 150/2002 Sb.) (40)

Jelikož při forenzní analýze často procházíme citlivá osobní data, je nutné mít před analýzou dat jistotu, že se nedopouštíme žádného protiprávního jednání.

# Praktická část

# 6 Analyzujeme zařízení útočníka

V této kapitole se zaměříme na konkrétní ukázkovou situaci, ta bude následně i výsledkem praktické části bakalářské práce. Předpokládejme, že jsme obdrželi již vypnutý počítač s operačním systémem Windows, ve kterém by mohly být dostupné důkazní materiály, jelikož očekáváme, že mohl vyhledávat například dostupnost zbraní a další detaily na internetu. Naším cílem je provést forenzní analýzu a získat tak materiály, které by mohly být dále použity při trestním řízení.

Jelikož se jedná o modelovou situaci, je nutné si předem stanovit přesné podmínky a to následovně:

- obdržíme vypnutý počítač ze kterého vyjmeme systémový disk
- disk v počítači není žádným způsobem šifrovaný, je nepoškozený a lze z něj číst data
- použitým operačním systémem byl Windows 10 nainstalovaný standardním způsobem
- splňujeme veškeré právní podmínky pro provedení forenzní analýzy
- zpracovávaná data jsou pouze fiktivní, bakalářská práce nebude dále řešit, zda jsme nalezli důkazy, ale pouze, zda se nám povedlo dostat k umístění, kde by data mohla být

Po splnění těchto podmínek můžeme přistoupit k forenzní analýze. U rámci praktické části bakalářské práce budeme provádět forenzní analýzu získaného disku v rámci této ukázkové situace. Z využitého software lze zmínit předem vybraný program OS Forensics v první části a DB Browser for SQLite ve druhé části v rámci analýzy alternativních webových prohlížečů.

Celkově se praktická část práce bude zabývat na ukázku a popis konkrétních postupů a technik v oblasti forenzní analýzy.

Důležitou součástí pak bude závěr a zhodnocení úspěšnosti v rámci získání požadovaných dat. V závěru budou také shrnuty možné překážky pro provedení forenzní analýzy.

## *6.1 První kroky*

První kroky se zařízením budou následující:

1. Bitová kopie všech disků a pamětí

Jelikož zařízení dostaneme vypnuté, dump paměti RAM nemá příliš smysl. Výjimkou může být situace, kdy se k nám zařízení dostane ještě zapnuté a jde o případ, kdy pravděpodobně důležitá data můžeme dostat i z RAM paměti.
Bitovou kopii je vhodné provést s fyzickým zařízením, které bude blokovat jakékoli i nechtěné nebo systémové pokusy o zapsání na disk. Příkladem může být zařízení Forensic UltraDock FUDv6, které lze použít pro SATA i historické PATA disky i Mini PCIe disky. Zařízení lze zakoupit za doporučenou cenu $399.


*Obrázek 14 - Zařízení Forensic UltraDock FUDv6 pro blokaci zápisu na disk* **(41)**.

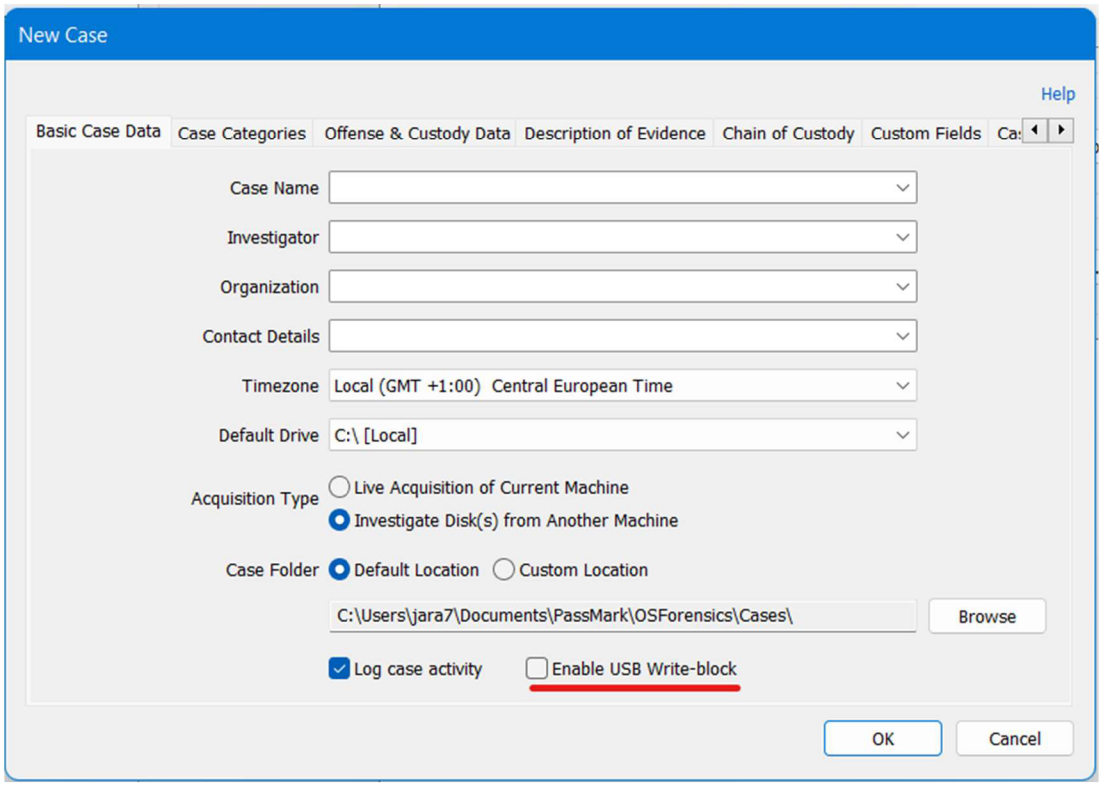
K zařízení tedy připojíme disk, u kterého chceme provést bitovou kopii a následně například programem OSForensics v záložce Create Forensic Image zvolíme zdrojový disk, uložení cílového souboru ve formátu *.img a algoritmus kontrolního součtu pro ověření, že data byla korektně zkopírována.

Možným levnějším řešením mohou být jednoúčelové boxy na disky s USB výstupem, které mají přepínač pro blokaci zápisu na disk. Nicméně je vhodné předem kontrolním součtem ověřit, zda daný box opravdu blokuje zápis kompletně a ani jej nevyužívá například pro svá dočasná data. Metodiku testu lze

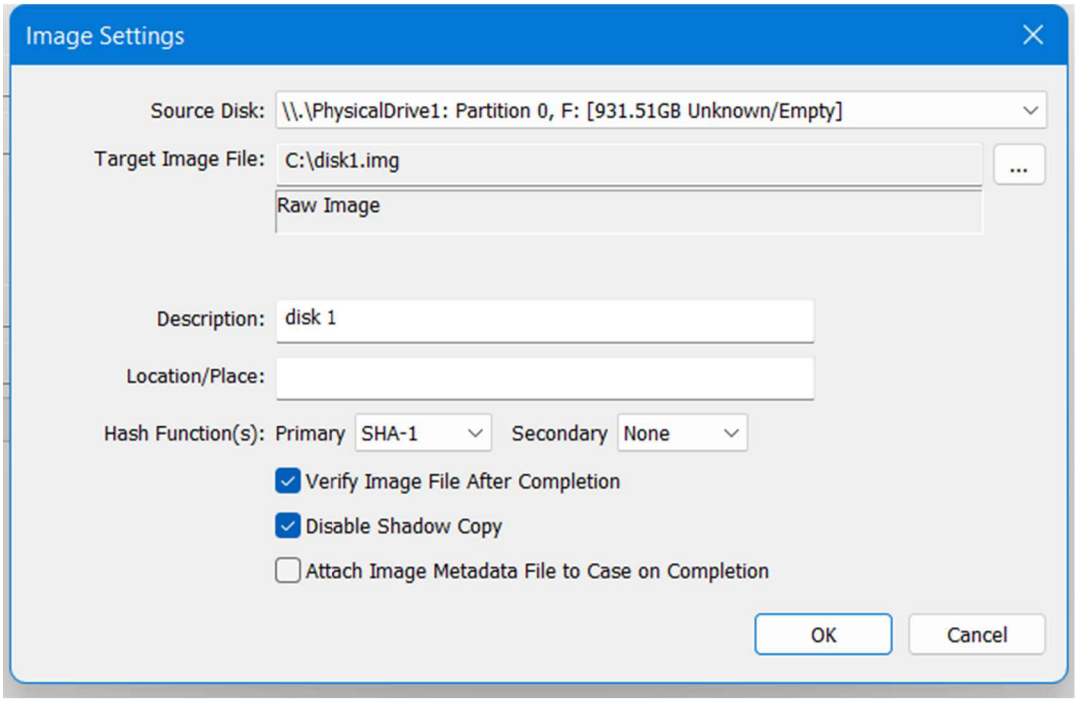
najít například v dokumentu Hardware Write Blocker (HWB) Assertions and Test Plan (42) a příklad shrnutí výsledků v dokumentu Test Results for Hardware Write Block Device – Federated Testing Suite, US Department of Homeland Security (43). Na svém webu Národní institut standardů a technologie (National Institute of Standards and Technology, NIST, USA) zveřejňuje vyhotovené testy komerčních blokátorů zápisu (44). Příkladem neúspěšného blokátoru z posledních testovaných může být Coolgear SS-127ASD USB 3.0 to SATA/IDE Adapter with Write-Protection, který propustil změnu sektorů pod Windows i Linuxem (45).


*Obrázek 15 - Box pro NVMe SSD s přepínačem pro blokaci zápisu (IcyBox External Enclosure for M.2 NVMe SSD)* **(46)**.

Případným nouzovým řešením může být softwarová blokace zápisu v samotném programu.

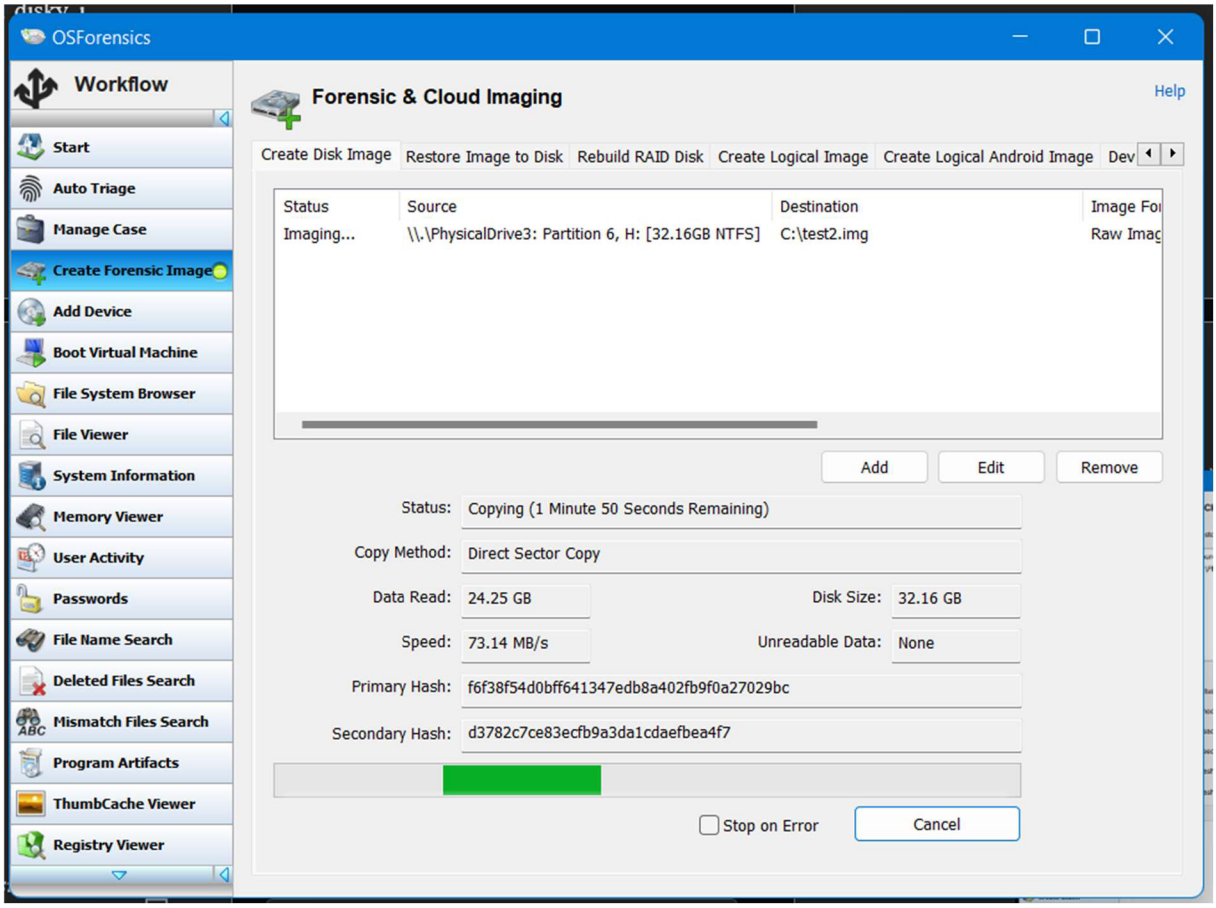



*Obrázek 16 - Blokace zápisu v programu OSForensics.*
Zdroj: vlastní




*Obrázek 17 - Vytvoření image disku v programu OSForensics.*
Zdroj: vlastní

Následně můžeme spustit klonování disku do souboru. Je dobré mít na paměti, že potřebujeme mít prostor, kam uložit celou kapacitu všech disků včetně prázdných sektorů (to následně může být zmenšeno kompresí o prázdné sektory).




*Obrázek 18 - Průběh vytváření bitové kopie disku v programu OSForensics.*
Zdroj: vlastní

Pro ukázku je použit jeden oddíl na externím SSD disku s nainstalovanými Windows 10. Celková doba vytváření kopií je dána tím pomalejším z cílového a zdrojového disku a celkové kapacitě zdrojového disku. Po dokončení je provedeno ověření kontrolního součtu.

2. Záloha
   Vytvoříme zálohu bitové kopie včetně textového souboru s kontrolním součtem, který program vložil do stejného adresáře. Je to důležité zejména z toho důvodu, že image disku lze i spustit jako virtuální systém a potřebujeme mít vždy možnost se vrátit ke přesně stejným datům, s jakými jsme původní disk útočníka převzali

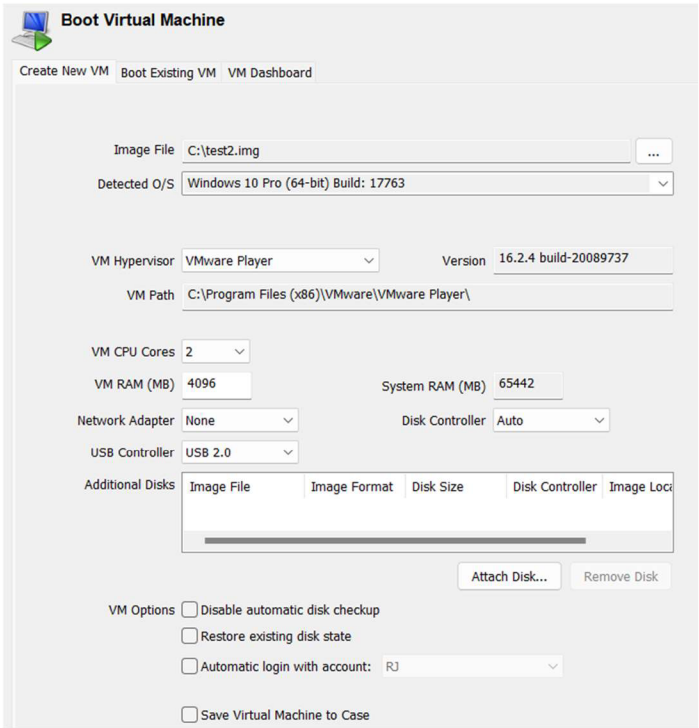
včetně možnosti ověřit, zda data nebyla nějakým způsobem změněna nebo poškozena, to je při dokazování důležité.

Zálohy je vhodné i zašifrovat, aby nehrozila možnost, že se cenná data i z pohledu soukromých dat útočníka dostanou do nesprávných rukou. Politika šifrování se obvykle řídí pravidly organizace.

## 6.2 Analýza bitové kopie

V programu OSForensics lze data v souboru bitové kopie procházet v následujících sekcích:

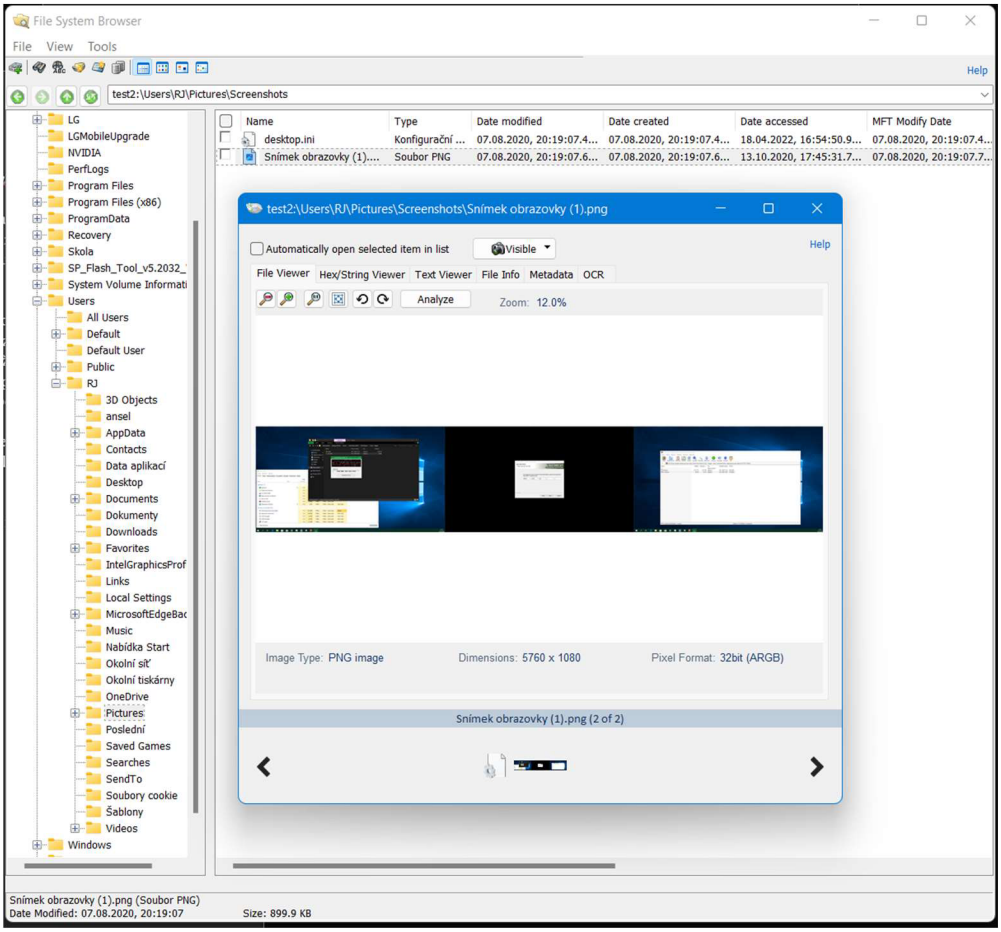
a) Boot Virtual Machine (spuštění virtualizovaného systému)
V případě, že se jednalo o systémový disk, lze jej spustit jako virtualizovaný systém prostřednictvím dalšího programu VMware player.
Nicméně u všech vyzkoušených image mi VMware napsalo pouze chybu čtení i v případech, kdy soubory disku VMware měly atribut čtení povolený, tuto funkci se mi tedy nepovedlo vyzkoušet.




*Obrázek 19 - Možnosti rychlého přidání image disku do virtualizačního programu VMware*
Zdroj: vlastní

b) File System Browser (procházení souborů)

V programu lze disk procházet podobně jako kdyby byl fyzicky připojený s tím rozdílem, že nehrozí změna původních dat. Pro nejběžnější mediální soubory má program vlastní přehrávač, všechny soubory lze zobrazit jako textový nebo hexadecimální řetězec spolu s metadaty a informacemi souboru – datum a čas poslední změny nebo vytvoření, EXIF data fotografie nebo R/W atributy.




*Obrázek 20 - Příklad procházení dat na image disku.*
Zdroj: vlastní

c) File Viewer
Prakticky stejná funkce jako File System Browser, obsahuje pouze méně možností nastavení náhledů mediálních souborů.

d) System Information (informace o systému)
V této sekci lze najít informace o nainstalovaném operačním systému a jeho komponentech. Pro identifikaci by bylo možné použít například:

- Název počítače uživatele

- Informace o nastavení sítě včetně poslední přiřazené IP adresy, datu a času přiřazení a expiraci a GUID síťové karty

| | |
|---|---|
| **Network GUID** | {e2b6134d-2bf8-4f53-bcbf-48aa500a4a06} |
| **Network Name** | Ethernet 2 |
| **IP (using DHCP)** | 192.168.1.10 (Yes) |
| **DHCP Server** | 192.168.1.1 |
| **DHCP Name Server** | 192.168.1.1 |
| **Lease Obtained** | středa 15. září 2021, 20:48:06 |
| **Lease Expires** | čtvrtek 16. září 2021, 20:48:06 |

*Obrázek 21 - Informace poslední připojené síti.*
Zdroj: vlastní

- Vytvořené uživatelské účty v systému s informacemi o posledním a prvním přihlášení, počtu celkových přihlášení a informace o hesle k účtu.

| | |
|---|---|
| **Username [ID]** | RJ [1001] |
| **Full Name** | |
| **Description** | |
| **Password Hint** | |
| **Account Created** | pátek 31. května 2019, 13:14:49 (can be inaccurate if registry permissions have been updated) |
| **Last Login** | úterý 11. ledna 2022, 21:46:08 |
| **Password Reset** | pátek 31. května 2019, 13:17:45 |
| **Password Fail Date** | středa 3. července 2019, 17:03:30 |
| **Password Fail Count** | 0 (reset after correct login) |
| **Login Count** | 48 |
| **Notes** | *Password never expires* |

*Obrázek 22 - Informace o uživatelském účtu.*
Zdroj: vlastní

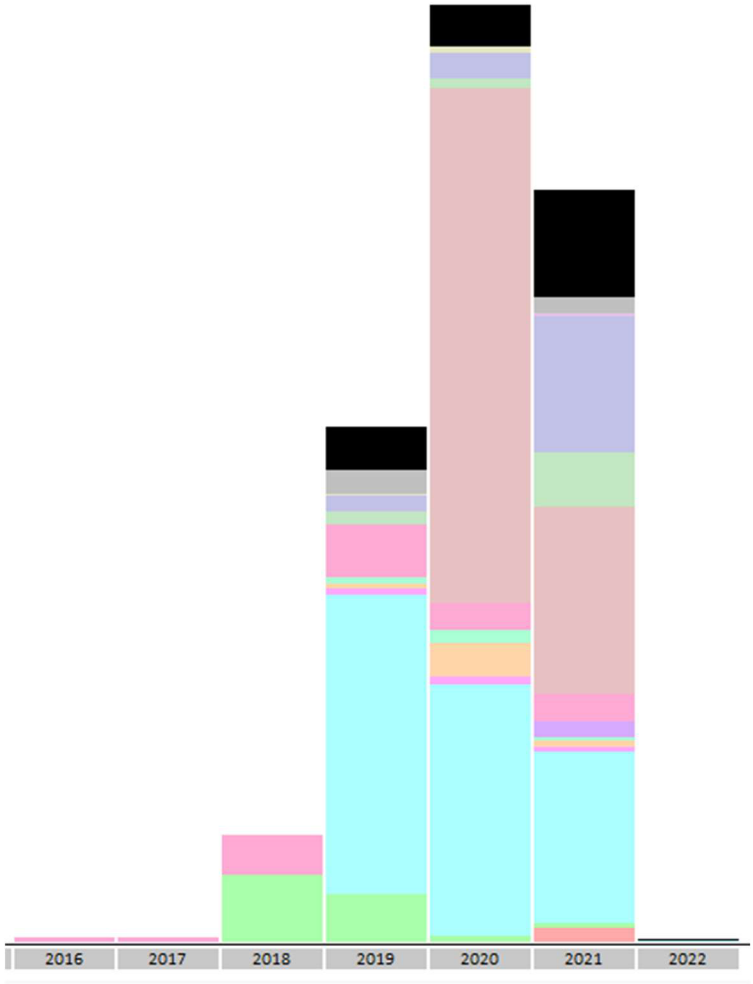
- Informace o nainstalovaných tiskárnách.
- Datum a čas posledního vypnutí počítače.
- Specifikace nainstalovaného OS.

| | |
|---|---|
| **Install path** | C:\Windows |
| **Build string** | 17763.rs5_release.180914-1434 |
| **Extended build string** | 17763.1.amd64fre.rs5_release.180914-1434 |
| **Build number** | 17763 |
| **Install date** | pátek 31. května 2019, 13:14:54 |
| **ProductName** | Windows 10 Pro |
| **Version** | 1809 |
| **ProductId** | 00330-80000-00000-AA568 |
| **DigitalProductId** | VK7JG-NPHTM-[redacted] |
| **RegisteredOwner** | RJ |
| **RegisteredOrganization** | |

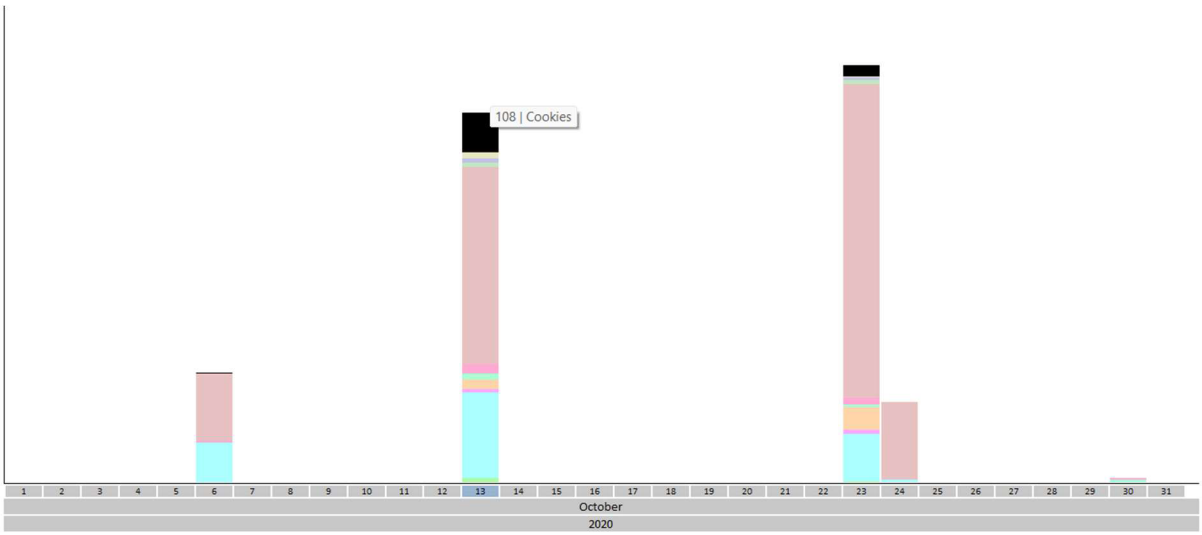
*Obrázek 23 - Informace o nainstalovaném operačním systému.*
Zdroj: vlastní

a) Memory Viewer (prohlížeč RAM paměti)
V rámci této sekce lze procházet buď informace o právě spuštěných procesech nebo extrahovat informace ze souboru RAM dumpu (bitová kopie RAM paměti počítače). Slouží ve spoustě případů k identifikaci malware na zasaženém počítači nebo odhalení jiného software, který byl naprogramován tak, aby pracoval skrytě bez vědomí uživatele. Dalším případem mohou být situace, kdy je soubor vytvořen, ale ještě není uložen na disk. Data je ale nutné získat ještě před vypnutím počítače, v opačném případě může dojít k jejich ztrátě.

e) User Activity (aktivity uživatele)
Na této kartě najdeme značné množství potencionálně zajímavých informací pro pozdější analýzu bez nutnosti přesně znát, kam například který internetový prohlížeč a v jakém formátu ukládá historii prohlížení, informace z registrů o přehledu událostí systému, posledních otevřených souborech, informace o dříve připojených zařízeních apod. Informace si lze zobrazit buď všechny chronologicky nebo rozdělené na kategorie. U každé informace lze najít přesnou adresu registru nebo souboru, kde jsou data uložena.
Dle dat jednotlivých událostí umí program vytvářet graf časové osy v kartě Timeline. To může být vhodné pro rychlý přehled, kdy byl počítač reálně používán. Barva v grafech označuje poměr jednotlivých kategorií.



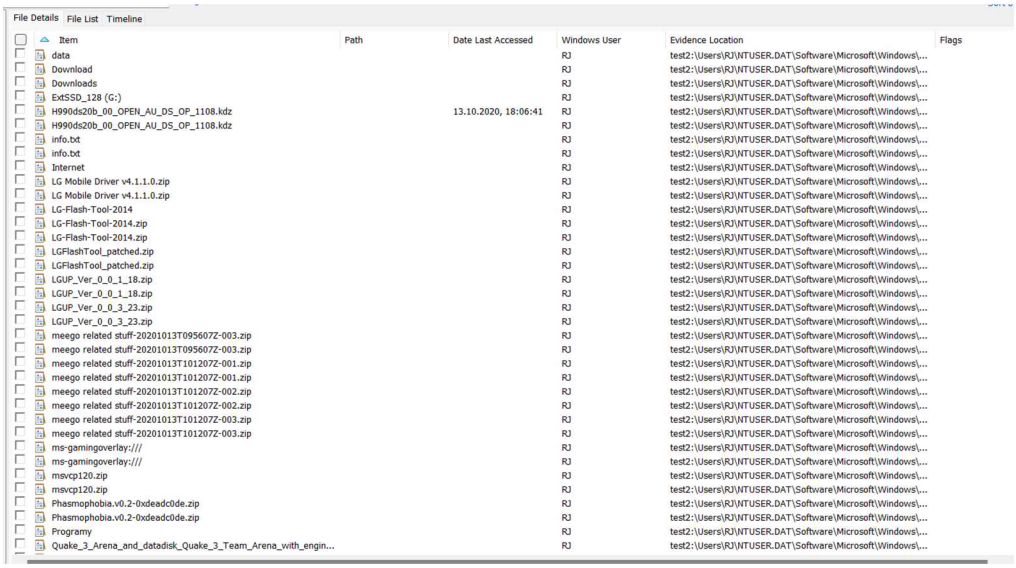

*Obrázek 24 - Timeline všech událostí v ročním zobrazení.*
Zdroj: vlastní




*Obrázek 25 - Timeline všech událostí v denním zobrazení.*
Zdroj: vlastní

Z kategorií lze zmínit zejména následující:

- Most Recently Used (poslední použité)
  Lze zobrazit poslední otevřené soubory v abecedním nebo chronologickém zobrazení, seznam posledních provedených akcí z okna Spustit, poslední použité zástupce, dále nejčastěji a poslední soubory reportované z Windows průzkumníka (MRU).

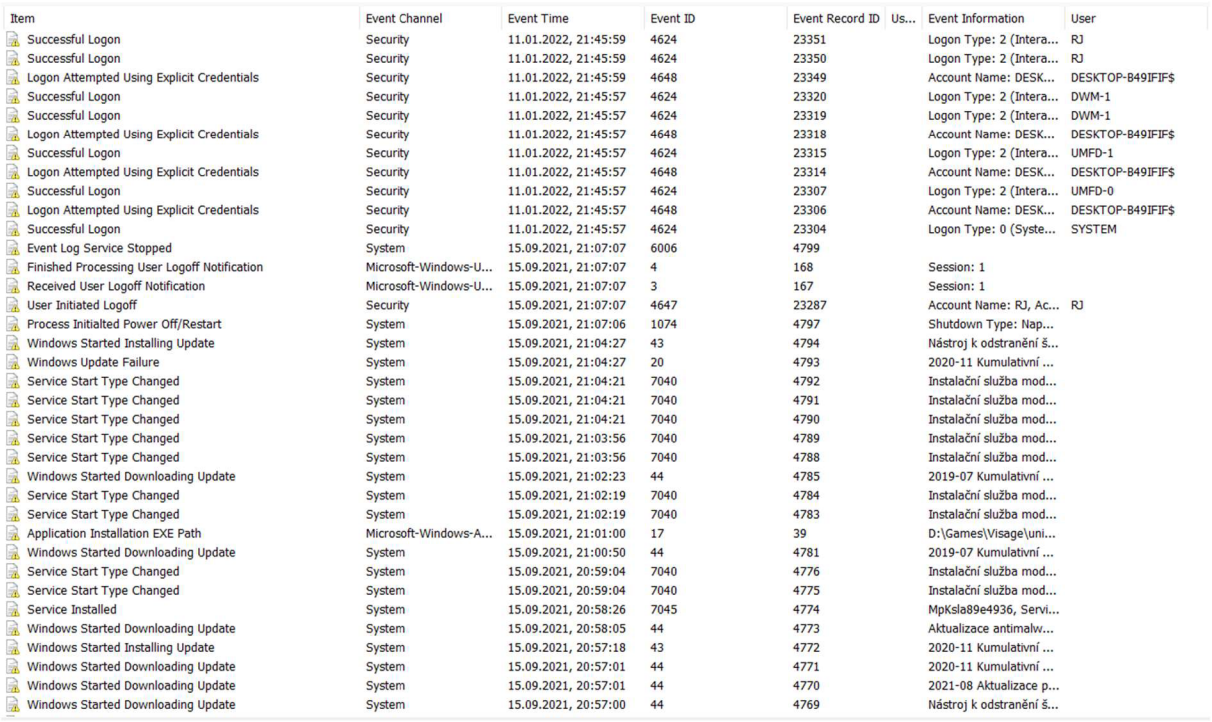



*Obrázek 26 - Poslední použité soubory. U spousty souborů a složek chybí časová značka.*
Zdroj: vlastní

- Installed Programs (nainstalované programy)
  Jak již název vypovídá, zobrazí seznam nainstalovaných programů v systému včetně postupně instalovaných aktualizací Windows a systémových programů.

- Autorun Commands
  Tato sekce obsahuje seznam programů, které mají povolený autostart po spuštění Windows.

- Event Logs
  Jde o chronologicky seřazený seznam úspěšných i neúspěšných pokusů o přihlášení uživatele do systému spolu s informacemi o výsledku instalovaných aktualizací a balíčků.



| Item | Event Channel | Event Time | Event ID | Event Record ID | Us... | Event Information | User |
|---|---|---|---|---|---|---|---|
| Successful Logon | Security | 11.01.2022, 21:45:59 | 4624 | 23351 | | Logon Type: 2 (Intera... | RJ |
| Successful Logon | Security | 11.01.2022, 21:45:59 | 4624 | 23350 | | Logon Type: 2 (Intera... | RJ |
| Logon Attempted Using Explicit Credentials | Security | 11.01.2022, 21:45:59 | 4648 | 23349 | | Account Name: DESK... | DESKTOP-B49IFIF$ |
| Successful Logon | Security | 11.01.2022, 21:45:57 | 4624 | 23320 | | Logon Type: 2 (Intera... | DWM-1 |
| Successful Logon | Security | 11.01.2022, 21:45:57 | 4624 | 23319 | | Logon Type: 2 (Intera... | DWM-1 |
| Logon Attempted Using Explicit Credentials | Security | 11.01.2022, 21:45:57 | 4648 | 23318 | | Account Name: DESK... | DESKTOP-B49IFIF$ |
| Successful Logon | Security | 11.01.2022, 21:45:57 | 4624 | 23315 | | Logon Type: 2 (Intera... | UMFD-1 |
| Logon Attempted Using Explicit Credentials | Security | 11.01.2022, 21:45:57 | 4648 | 23314 | | Account Name: DESK... | DESKTOP-B49IFIF$ |
| Successful Logon | Security | 11.01.2022, 21:45:57 | 4624 | 23307 | | Logon Type: 2 (Intera... | UMFD-0 |
| Logon Attempted Using Explicit Credentials | Security | 11.01.2022, 21:45:57 | 4648 | 23306 | | Account Name: DESK... | DESKTOP-B49IFIF$ |
| Successful Logon | Security | 11.01.2022, 21:45:57 | 4624 | 23304 | | Logon Type: 0 (Syste... | SYSTEM |
| Event Log Service Stopped | System | 15.09.2021, 21:07:07 | 6006 | 4799 | | | |
| Finished Processing User Logoff Notification | Microsoft-Windows-U... | 15.09.2021, 21:07:07 | 4 | 168 | | Session: 1 | |
| Received User Logoff Notification | Microsoft-Windows-U... | 15.09.2021, 21:07:07 | 3 | 167 | | Session: 1 | |
| User Initiated Logoff | Security | 15.09.2021, 21:07:07 | 4647 | 23287 | | Account Name: RJ, Ac... | RJ |
| Process Initialted Power Off/Restart | System | 15.09.2021, 21:07:06 | 1074 | 4797 | | Shutdown Type: Nap... | |
| Windows Started Installing Update | System | 15.09.2021, 21:04:27 | 43 | 4794 | | Nástroj k odstranění š... | |
| Windows Update Failure | System | 15.09.2021, 21:04:27 | 20 | 4793 | | 2020-11 Kumulativní ... | |
| Service Start Type Changed | System | 15.09.2021, 21:04:21 | 7040 | 4792 | | Instalační služba mod... | |
| Service Start Type Changed | System | 15.09.2021, 21:04:21 | 7040 | 4791 | | Instalační služba mod... | |
| Service Start Type Changed | System | 15.09.2021, 21:04:21 | 7040 | 4790 | | Instalační služba mod... | |
| Service Start Type Changed | System | 15.09.2021, 21:03:56 | 7040 | 4789 | | Instalační služba mod... | |
| Service Start Type Changed | System | 15.09.2021, 21:03:56 | 7040 | 4788 | | Instalační služba mod... | |
| Windows Started Downloading Update | System | 15.09.2021, 21:02:23 | 44 | 4785 | | 2019-07 Kumulativní ... | |
| Service Start Type Changed | System | 15.09.2021, 21:02:19 | 7040 | 4784 | | Instalační služba mod... | |
| Service Start Type Changed | System | 15.09.2021, 21:02:19 | 7040 | 4783 | | Instalační služba mod... | |
| Application Installation EXE Path | Microsoft-Windows-A... | 15.09.2021, 21:01:00 | 17 | 39 | | D:\Games\Visage\uni... | |
| Windows Started Downloading Update | System | 15.09.2021, 21:00:50 | 44 | 4781 | | 2019-07 Kumulativní ... | |
| Service Start Type Changed | System | 15.09.2021, 20:59:04 | 7040 | 4776 | | Instalační služba mod... | |
| Service Start Type Changed | System | 15.09.2021, 20:59:04 | 7040 | 4775 | | Instalační služba mod... | |
| Service Installed | System | 15.09.2021, 20:58:26 | 7045 | 4774 | | MpKsla89e4936, Servi... | |
| Windows Started Downloading Update | System | 15.09.2021, 20:58:05 | 44 | 4773 | | Aktualizace antimalw... | |
| Windows Started Installing Update | System | 15.09.2021, 20:57:18 | 43 | 4772 | | 2020-11 Kumulativní ... | |
| Windows Started Downloading Update | System | 15.09.2021, 20:57:01 | 44 | 4771 | | 2020-11 Kumulativní ... | |
| Windows Started Downloading Update | System | 15.09.2021, 20:57:01 | 44 | 4770 | | 2021-08 Aktualizace p... | |
| Windows Started Downloading Update | System | 15.09.2021, 20:57:00 | 44 | 4769 | | Nástroj k odstranění š... | |

*Obrázek 27 - Chronologický seznam událostí v systému.*
Zdroj: vlastní

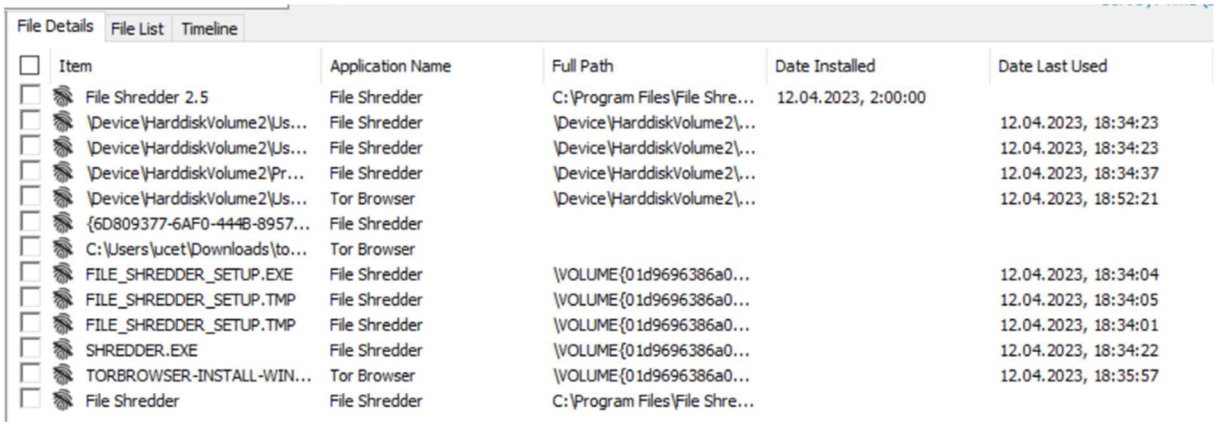
- Shellbags
  Zde lze najít seznam všech posledních otevřených složek prostřednictvím Windows Exploreru. Tento seznam může být zajímavý pro forenzní analýzu i z pohledu, že zůstávají uloženy i názvy složek na již odpojených externích médiích, což může být poměrně zajímavá informace ve spojení s dalšími zjištěnými daty nebo jako nápověda, jaké další informace ještě dále hledat.

- Recycle Bin
  Zde se zobrazí seznam všech souborů v Koši, nicméně procházení souborů v koši prostřednictvím modulu File System Browser se zdá přehlednější, zde pouze umí navíc přímo zobrazit celkovou velikost složky.

- Windows Search
  Podobně jako sekce Shellbags, Windows Search přímo neurčí, co se s počítačem dělo, ale seznam vyhledávaných a spuštěných programů

z nabídky Start může pomoci při skládání všech dílčích informací o používání počítače dohromady.

- Anti-Forensics Artifacts
  Program OSForensics umožňuje sbírání informací o používání dalších programů pro skrývání stop, může jít o různé nástroje pro šifrování dat jako VeraCrypt, AxCrypt nebo Gpg4win, programy pro zabránění obnovení smazaných souborů File Shredder, BCWipe nebo DiskBoss, program Slacker simulující, že se s počítačem pracuje, případně další nástroje jako Tor Browser pro prohlížení anonymnější odnože internetu nebo nástroje pro změnu časových značek u souborů. Tím může nastat situace, kdy má soubor starší časovou značku než byl vytvořen a může to značit stav, že pachatel se snažil něco skrýt nebo upravit.

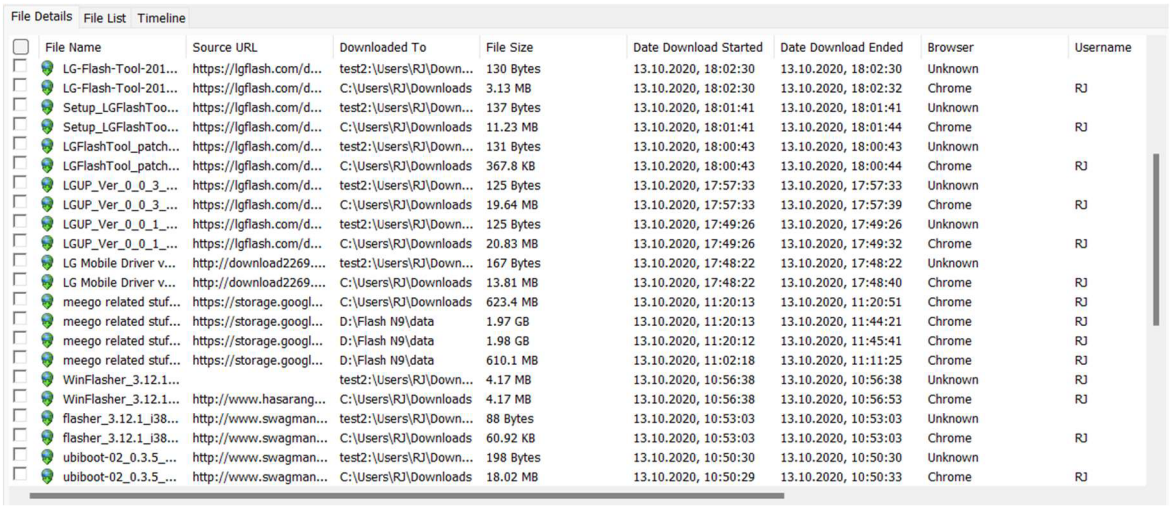



| Item | Application Name | Full Path | Date Installed | Date Last Used |
|---|---|---|---|---|
| File Shredder 2.5 | File Shredder | C:\Program Files\File Shre... | 12.04.2023, 2:00:00 | |
| \Device\HarddiskVolume2\Us... | File Shredder | \Device\HarddiskVolume2\... | | 12.04.2023, 18:34:23 |
| \Device\HarddiskVolume2\Us... | File Shredder | \Device\HarddiskVolume2\... | | 12.04.2023, 18:34:23 |
| \Device\HarddiskVolume2\Pr... | File Shredder | \Device\HarddiskVolume2\... | | 12.04.2023, 18:34:37 |
| \Device\HarddiskVolume2\Us... | Tor Browser | \Device\HarddiskVolume2\... | | 12.04.2023, 18:52:21 |
| {6D809377-6AF0-444B-8957... | File Shredder | | | |
| C:\Users\ucet\Downloads\to... | Tor Browser | | | |
| FILE_SHREDDER_SETUP.EXE | File Shredder | \VOLUME{01d9696386a0... | | 12.04.2023, 18:34:04 |
| FILE_SHREDDER_SETUP.TMP | File Shredder | \VOLUME{01d9696386a0... | | 12.04.2023, 18:34:05 |
| FILE_SHREDDER_SETUP.TMP | File Shredder | \VOLUME{01d9696386a0... | | 12.04.2023, 18:34:01 |
| SHREDDER.EXE | File Shredder | \VOLUME{01d9696386a0... | | 12.04.2023, 18:34:22 |
| TORBROWSER-INSTALL-WIN... | Tor Browser | \VOLUME{01d9696386a0... | | 12.04.2023, 18:35:57 |
| File Shredder | File Shredder | C:\Program Files\File Shre... | | |

*Obrázek 28 - Nalezené soubory v kategorii Anti-Forensics Artifacts.*
Zdroj: vlastní

- Downloads
  Obsah sekce přímo odpovídá názvu, zde lze najít seznam stažených souborů včetně zdrojové URL adresy, cílového adresáře a identifikaci webového prohlížeče, nicméně z testování v reálném použití některé starší verze prohlížečů založených na jádru Chromium zobrazuje jako Chrome a Microsoft Edge do verze 18 s jádrem EdgeHTML před přechodem na Chromium jako Unknown, stejně jako Mozillu Firefox.

Různé další alternativní prohlížeče i založené na jádru Chromium ale nenajde vůbec. Více tento aspekt bude popsán dále.

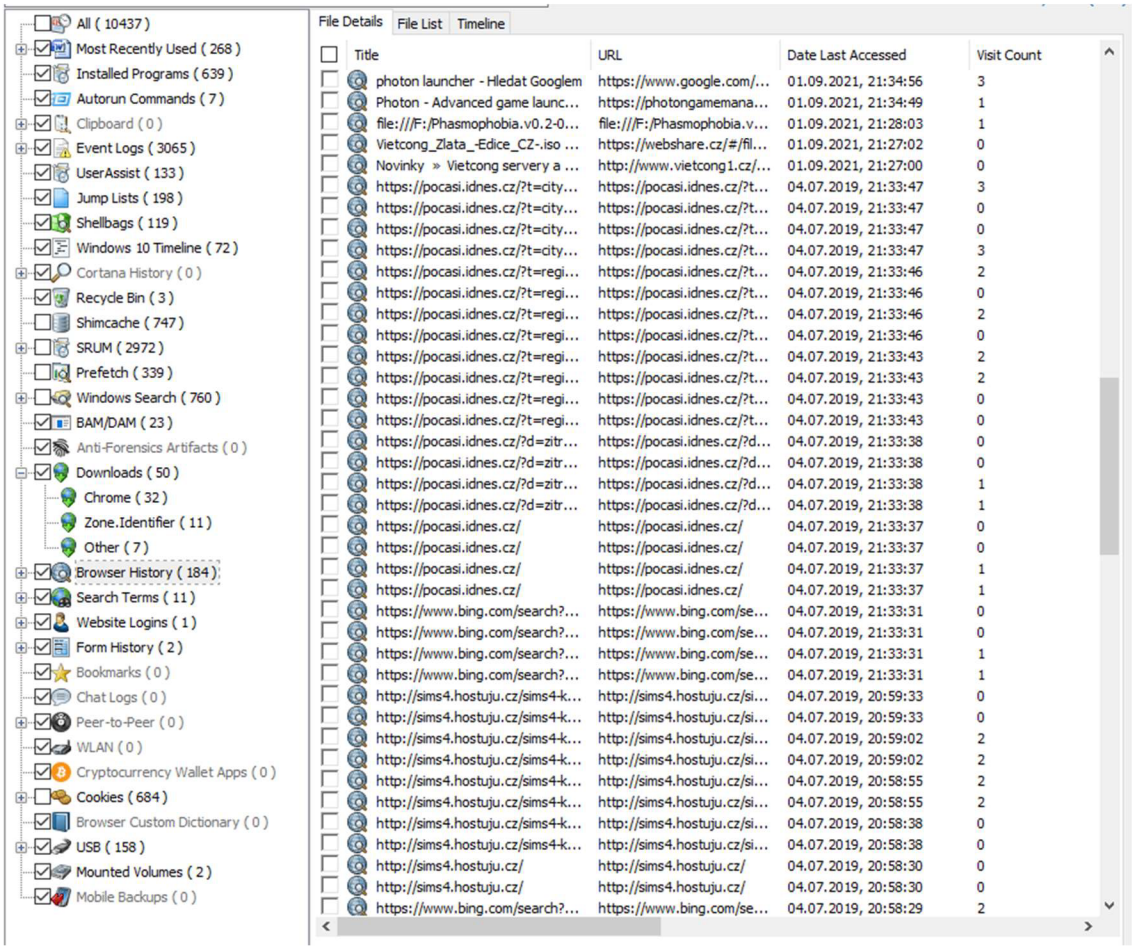


File Details | File List | Timeline

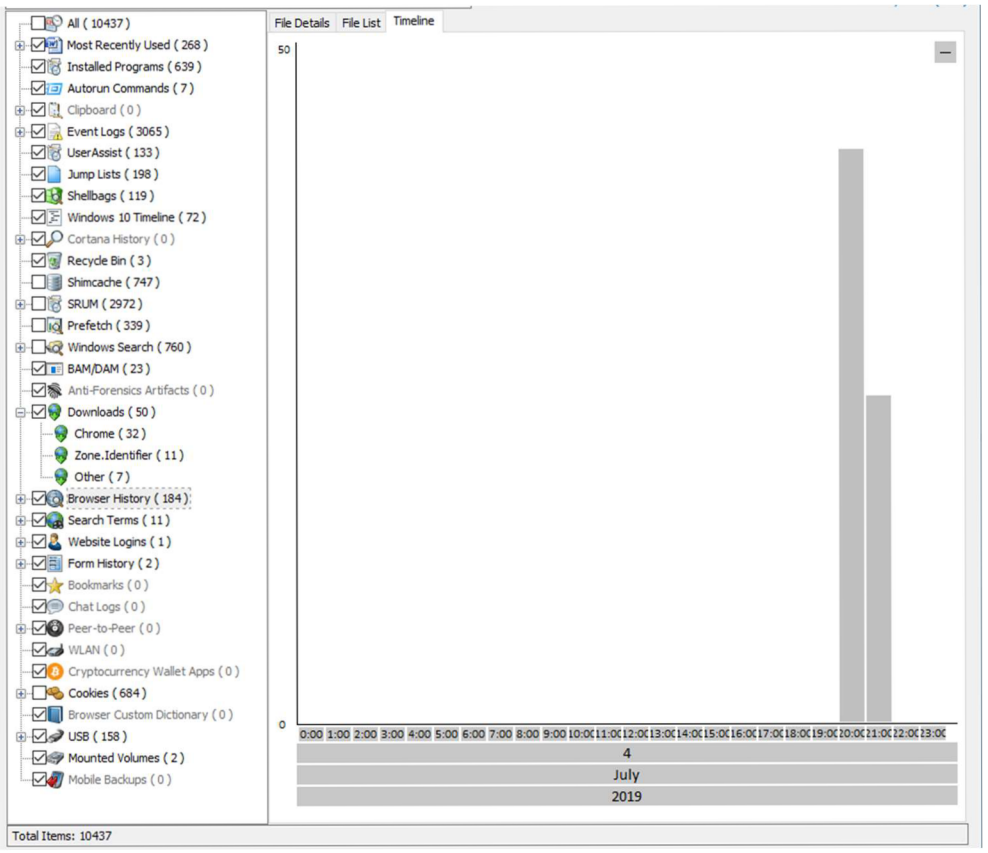
| File Name | Source URL | Downloaded To | File Size | Date Download Started | Date Download Ended | Browser | Username |
|---|---|---|---|---|---|---|---|
| LG-Flash-Tool-201... | https://lgflash.com/d... | test2:\Users\RJ\Down... | 130 Bytes | 13.10.2020, 18:02:30 | 13.10.2020, 18:02:30 | Unknown | |
| LG-Flash-Tool-201... | https://lgflash.com/d... | C:\Users\RJ\Downloads | 3.13 MB | 13.10.2020, 18:02:30 | 13.10.2020, 18:02:32 | Chrome | RJ |
| Setup_LGFlashToo... | https://lgflash.com/d... | test2:\Users\RJ\Down... | 137 Bytes | 13.10.2020, 18:01:41 | 13.10.2020, 18:01:41 | Unknown | |
| Setup_LGFlashToo... | https://lgflash.com/d... | C:\Users\RJ\Downloads | 11.23 MB | 13.10.2020, 18:01:41 | 13.10.2020, 18:01:44 | Chrome | RJ |
| LGFlashTool_patch... | https://lgflash.com/d... | test2:\Users\RJ\Down... | 131 Bytes | 13.10.2020, 18:00:43 | 13.10.2020, 18:00:43 | Unknown | |
| LGFlashTool_patch... | https://lgflash.com/d... | C:\Users\RJ\Downloads | 367.8 KB | 13.10.2020, 18:00:43 | 13.10.2020, 18:00:44 | Chrome | RJ |
| LGUP_Ver_0_0_3_... | https://lgflash.com/d... | test2:\Users\RJ\Down... | 125 Bytes | 13.10.2020, 17:57:33 | 13.10.2020, 17:57:33 | Unknown | |
| LGUP_Ver_0_0_3_... | https://lgflash.com/d... | C:\Users\RJ\Downloads | 19.64 MB | 13.10.2020, 17:57:33 | 13.10.2020, 17:57:39 | Chrome | RJ |
| LGUP_Ver_0_0_1_... | https://lgflash.com/d... | test2:\Users\RJ\Down... | 125 Bytes | 13.10.2020, 17:49:26 | 13.10.2020, 17:49:26 | Unknown | |
| LGUP_Ver_0_0_1_... | https://lgflash.com/d... | C:\Users\RJ\Downloads | 20.83 MB | 13.10.2020, 17:49:26 | 13.10.2020, 17:49:32 | Chrome | RJ |
| LG Mobile Driver v... | http://download2269.... | test2:\Users\RJ\Down... | 167 Bytes | 13.10.2020, 17:48:22 | 13.10.2020, 17:48:22 | Unknown | |
| LG Mobile Driver v... | http://download2269.... | C:\Users\RJ\Downloads | 13.81 MB | 13.10.2020, 17:48:22 | 13.10.2020, 17:48:40 | Chrome | RJ |
| meego related stuf... | https://storage.googl... | C:\Users\RJ\Downloads | 623.4 MB | 13.10.2020, 11:20:13 | 13.10.2020, 11:20:51 | Chrome | RJ |
| meego related stuf... | https://storage.googl... | D:\Flash N9\data | 1.97 GB | 13.10.2020, 11:20:13 | 13.10.2020, 11:44:21 | Chrome | RJ |
| meego related stuf... | https://storage.googl... | D:\Flash N9\data | 1.98 GB | 13.10.2020, 11:20:12 | 13.10.2020, 11:45:41 | Chrome | RJ |
| meego related stuf... | https://storage.googl... | D:\Flash N9\data | 610.1 MB | 13.10.2020, 11:02:18 | 13.10.2020, 11:11:25 | Chrome | RJ |
| WinFlasher_3.12.1... | | test2:\Users\RJ\Down... | 4.17 MB | 13.10.2020, 10:56:38 | 13.10.2020, 10:56:38 | Unknown | RJ |
| WinFlasher_3.12.1... | http://www.hasarang... | C:\Users\RJ\Downloads | 4.17 MB | 13.10.2020, 10:56:38 | 13.10.2020, 10:56:53 | Chrome | RJ |
| flasher_3.12.1_i38... | http://www.swagman... | test2:\Users\RJ\Down... | 88 Bytes | 13.10.2020, 10:53:03 | 13.10.2020, 10:53:03 | Unknown | |
| flasher_3.12.1_i38... | http://www.swagman... | C:\Users\RJ\Downloads | 60.92 KB | 13.10.2020, 10:53:03 | 13.10.2020, 10:53:03 | Chrome | RJ |
| ubiboot-02_0.3.5_... | http://www.swagman... | test2:\Users\RJ\Down... | 198 Bytes | 13.10.2020, 10:50:30 | 13.10.2020, 10:50:30 | Unknown | |
| ubiboot-02_0.3.5_... | http://www.swagman... | C:\Users\RJ\Downloads | 18.02 MB | 13.10.2020, 10:50:29 | 13.10.2020, 10:50:33 | Chrome | RJ |

*Obrázek 29 - Seznam posledních stažených souborů včetně zdrojové URL adresy.*
Zdroj: vlastní

- Browser History
  V sekci s historií prohlížečů lze najít a filtrovat data chronologicky, dle prohlížeče, url adresy, počtu návštěv nebo přihlášeného uživatele ve Windows. Stejně jako v předchozí kategorii se některé prohlížeče s jádrem Chromium zobrazují jako Google Chrome a jiné se nezobrazují. V sekci timeline je možné na sloupcovém grafu pozorovat četnost aktivit a následně tak jednoduše vybrat konkrétní sledované období.

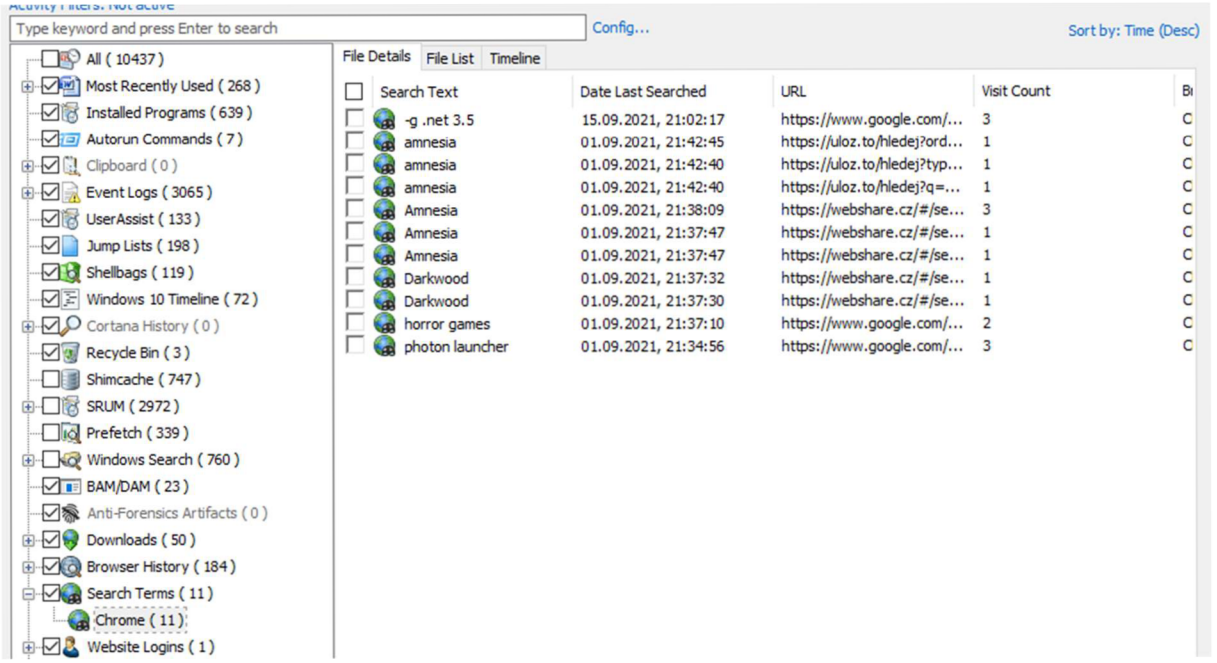



*Obrázek 30 - Procházení historie prohlížení internetových prohlížečů hromadně chronologicky.*
Zdroj: vlastní



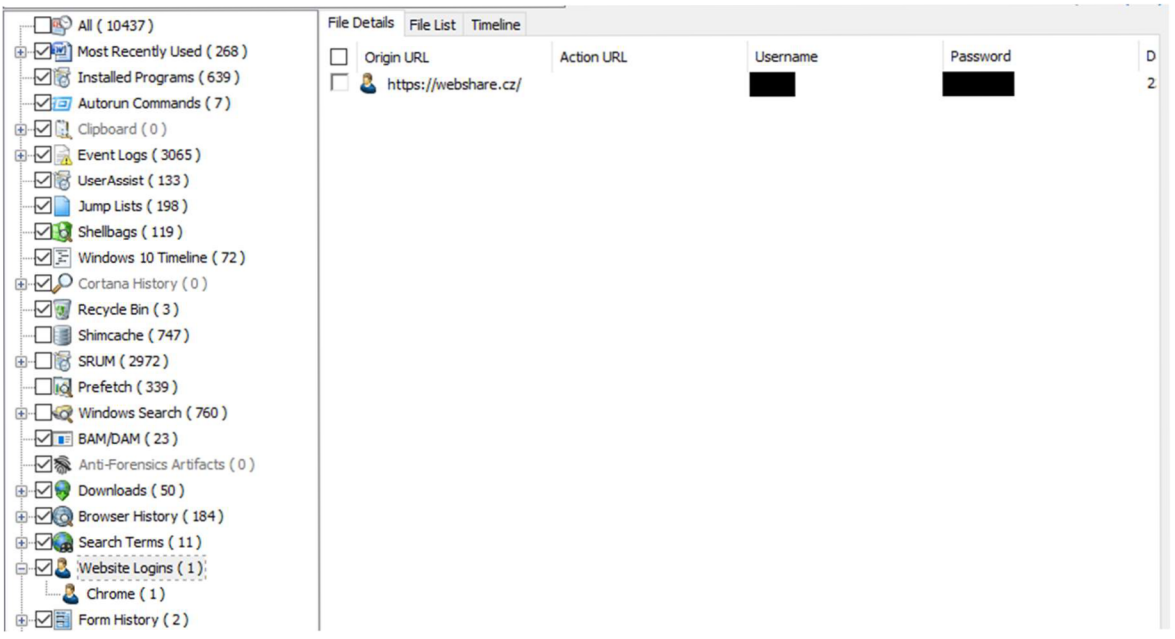

*Obrázek 31 - Graf četnosti návštěv internetových stránek.*
Zdroj: vlastní

- Search Terms
  Z této sekce lze jednoduše filtrovat vyhledávané pojmy ať už z vyhledávacího pole prohlížeče nebo i vyhledávacích polí navštívených webových stránek.



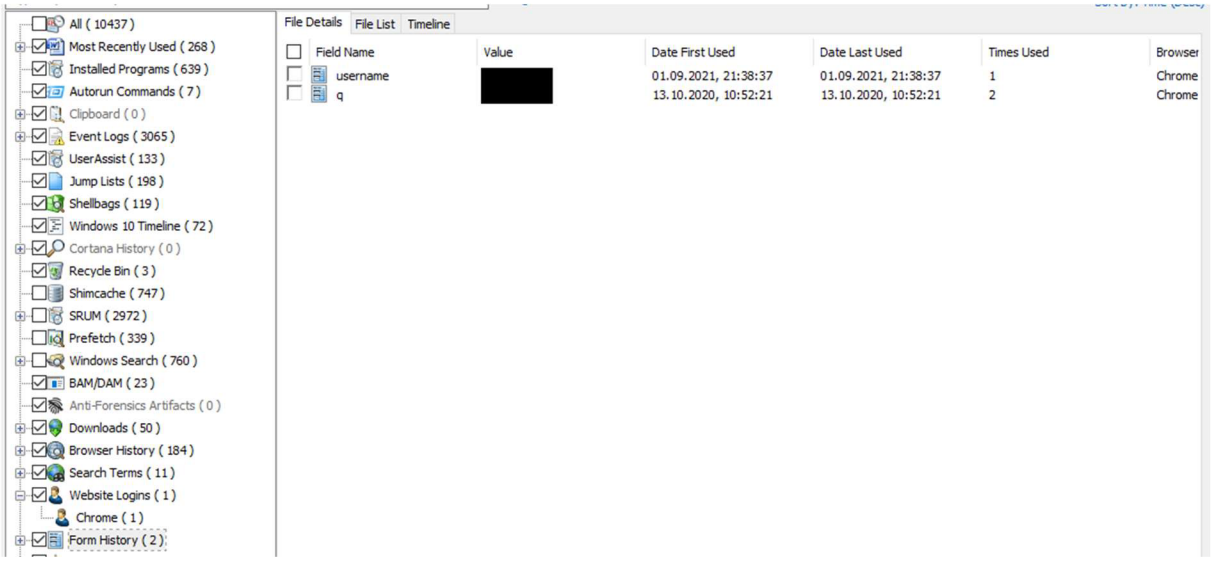

*Obrázek 32 - Vyhledávané pojmy v internetových prohlížečích.*
Zdroj: vlastní

- Website Logins
  Zde je sdružení všech uložených přihlašovacích jmen a hesel v čitelné podobě v prohlížečích mimo hesla uložená prostřednictvím externích doplňků pro správu hesel. Prokliknutím položky se lze dostat přímo k souboru, kde jsou data uložena.



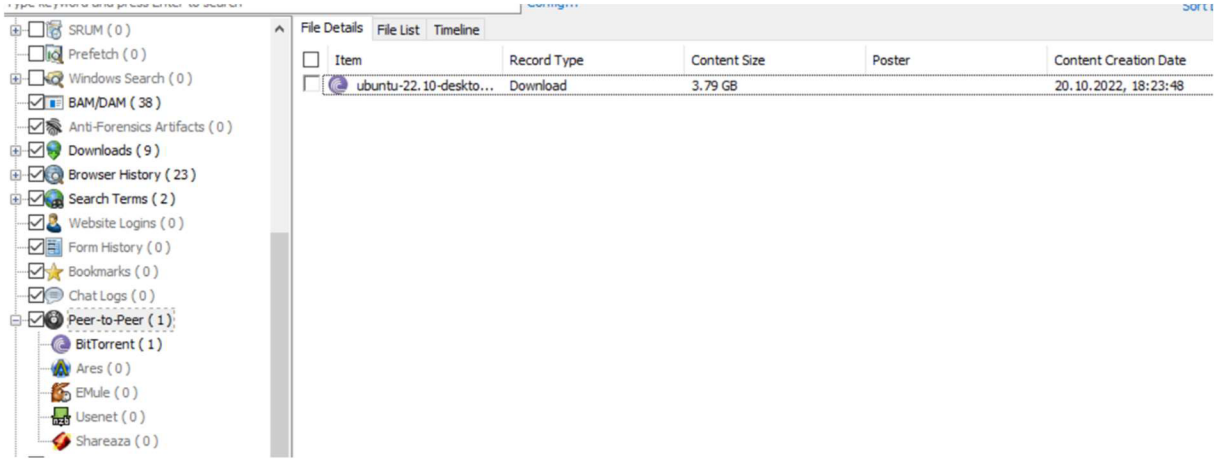

*Obrázek 33 - Uložená hesla v prohlížečích.*
Zdroj: vlastní

- Form History
  Je možné zobrazit obvykle automaticky uložená data pro přihlašovací formuláře nebo adresy pro případné navrhování doplňování při příští návštěvě webové stránky, návrh adresy při objednávce v internetovém obchodě apod.



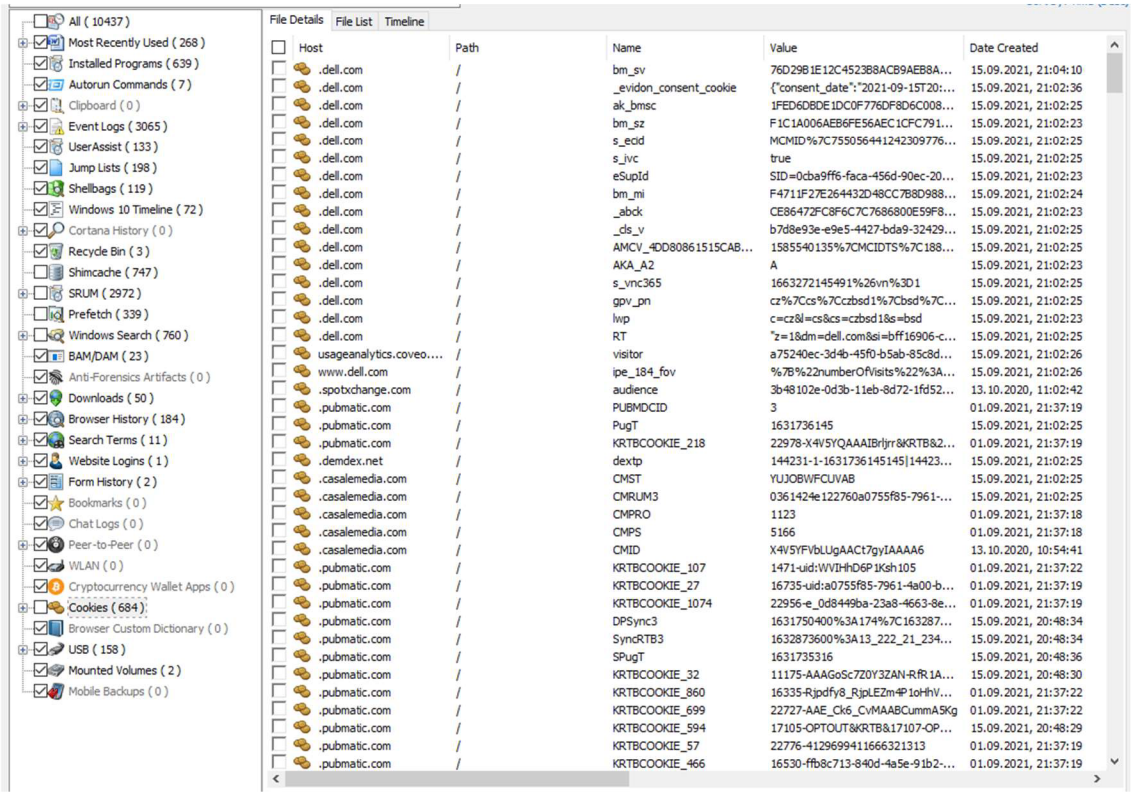

*Obrázek 34 - Data z vyplněných formulářů.*
Zdroj: vlastní

- Peer-to-peer
  Jedná se o způsob sdílení/stahování souborů mezi počítači způsobem, že data, která již má jiný uživatel sdílí uživatelům, kteří úsek dat ještě nemají stažený. V České republice je používání legální, nicméně často se tímto způsobem šíří obsah s autorskými právy a v tom případě je tímto způsobem autorské dílo šířeno dále dalším uživatelům, to je již nelegální využití tohoto protokolu.

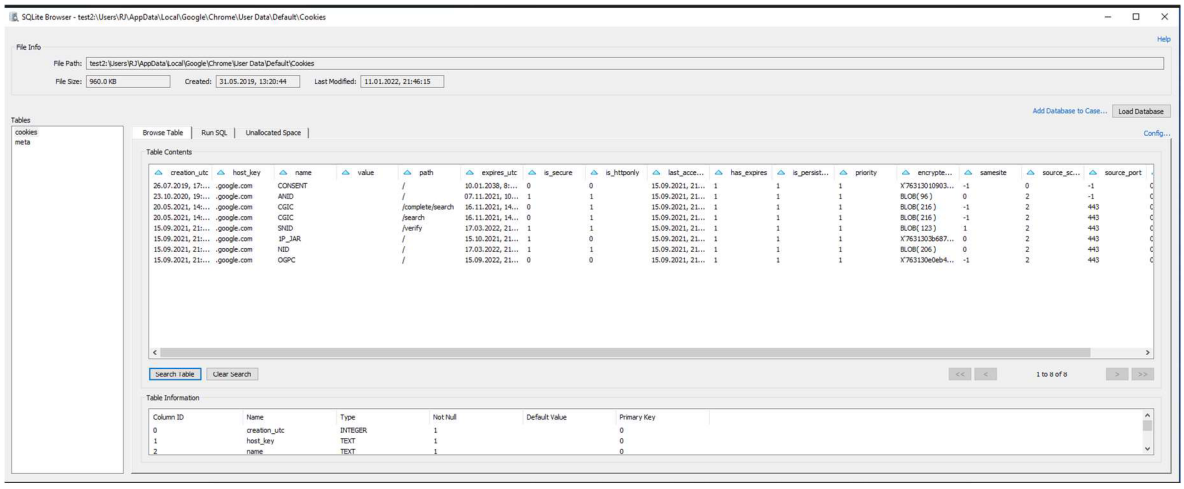



*Obrázek 35 - Nalezené soubory sdílené prostřednictvím peer-to-peer sítě.*
Zdroj: vlastní

- Cookies
  Uložená cookies v prohlížečích jsou data, které weby ukládají do prohlížeče uživatele. Obvykle se jedná o data, u kterých se počítá, že se mohou ztratit, jedná se tak o různé identifikátory pro cílení reklamy, uživatelské nastavení motivu na webu, skrytí banneru na webu e-shopu apod. Data jsou ukládána s podrobnostmi jako u zbývajících kategorií o prohlížeči nebo přihlášeném uživateli ve Windows. Po rozkliknutí lze data podrobně filtrovat dle všech dostupných parametrů (web, datum a čas, název klíče, konkrétní hodnota apod.) a následně procházet konkrétní data.




*Obrázek 36 - Výpis všech uložených cookies z prohlížečů.*
Zdroj: vlastní

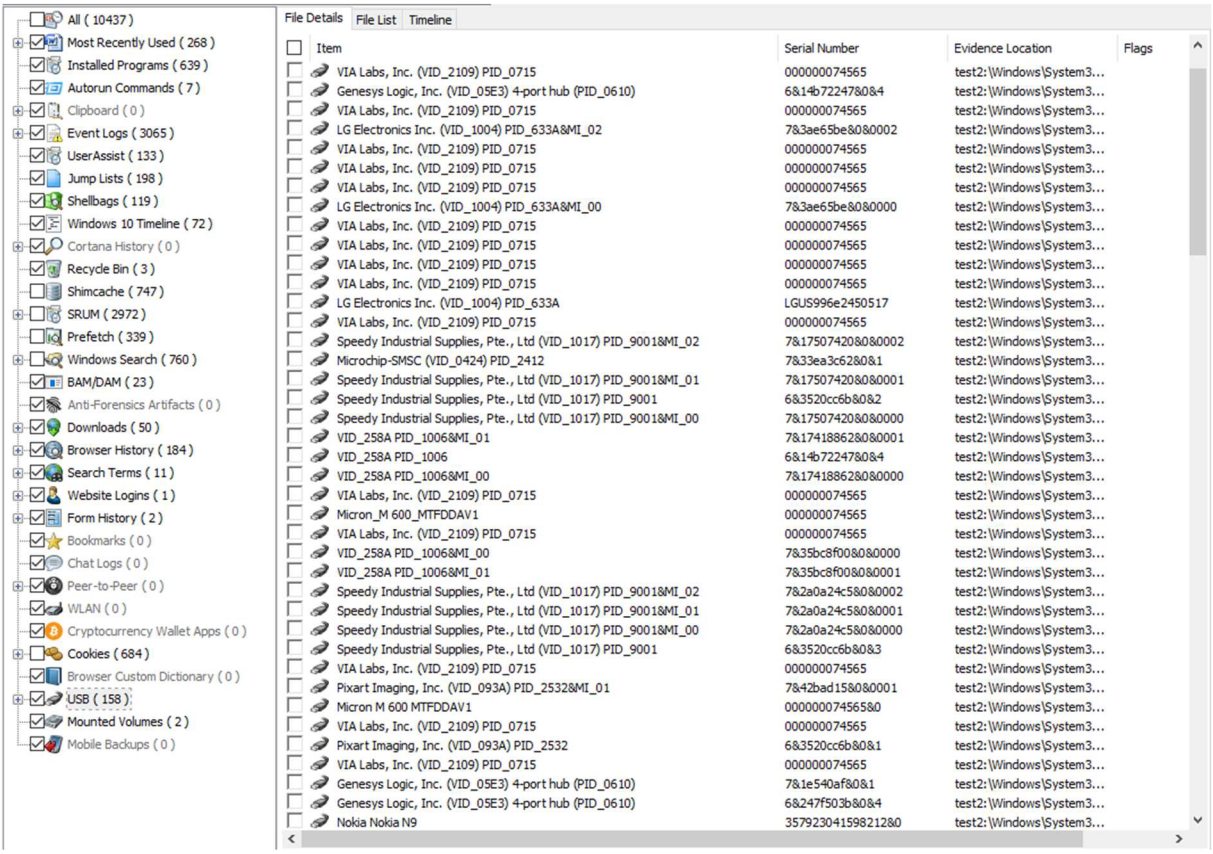



*Obrázek 37 - Filtrování konkrétních cookies dle parametrů.*
Zdroj: vlastní

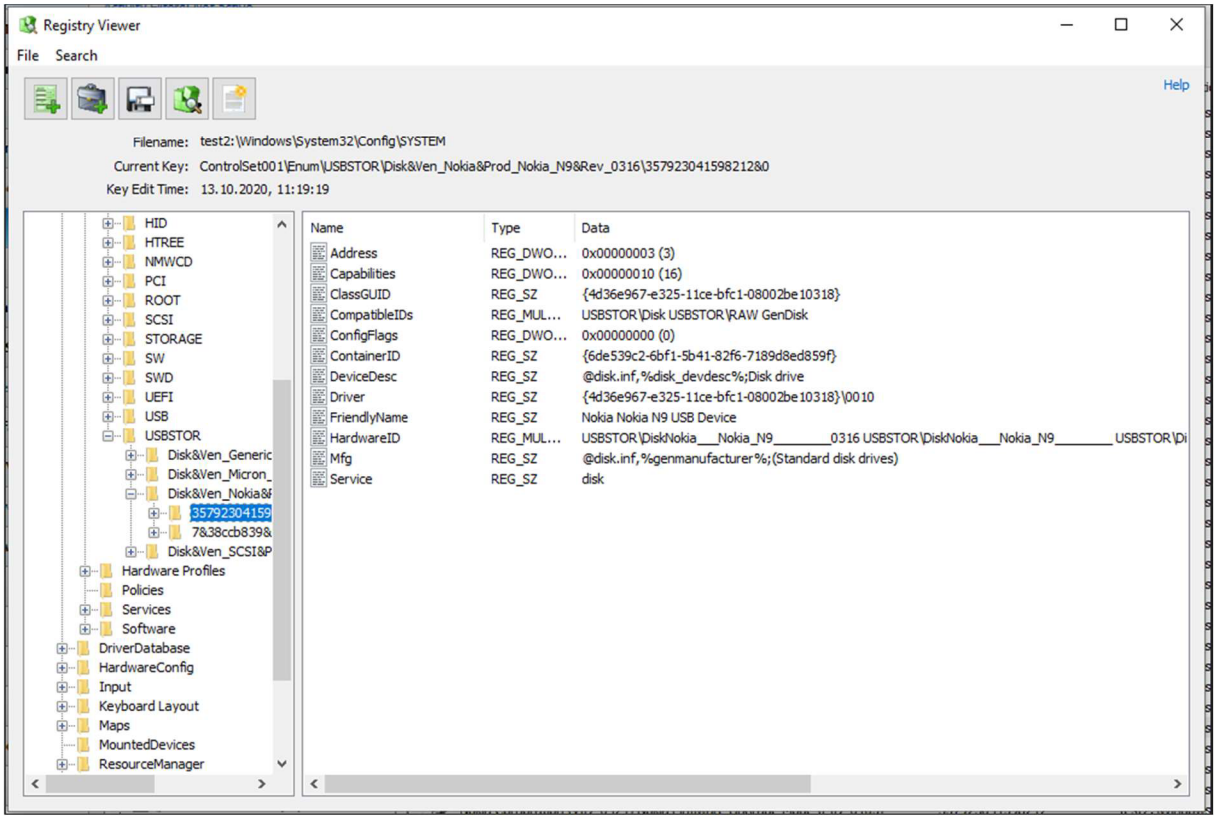
- USB

  Kategorie sdružuje informace o všech v minulosti připojených USB zařízeních, pro které musel OS využít nějaký ovladač spolu s názvem, a případně i sériovým číslem, pokud jej zařízení poskytlo. Při procházení konkrétních položek lze jednoduše přejít k položce v registru náležící

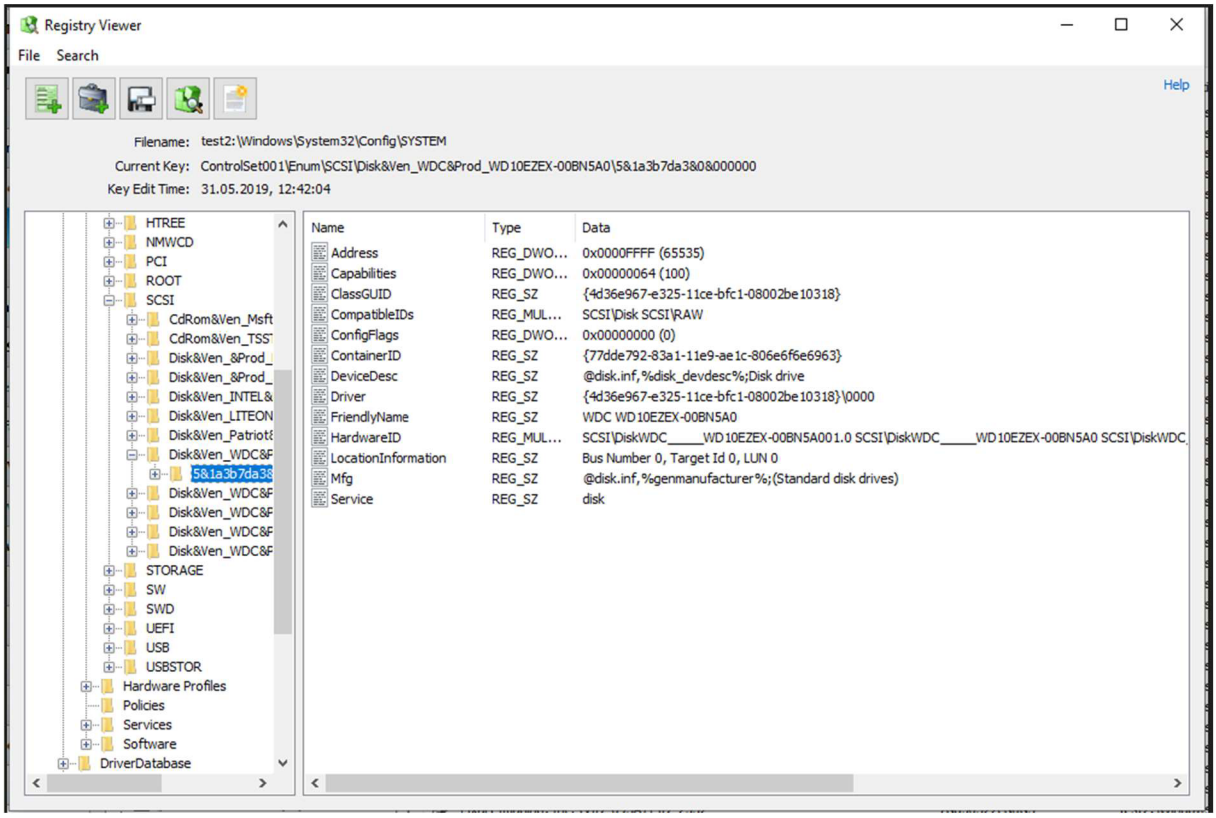
záznamu a tím tak například najít informaci o jaký typ zařízení šlo v případech, kde název nemusí být přesně vypovídající.




*Obrázek 38 - Výpis v minulosti připojených USB zařízení.*
Zdroj: vlastní

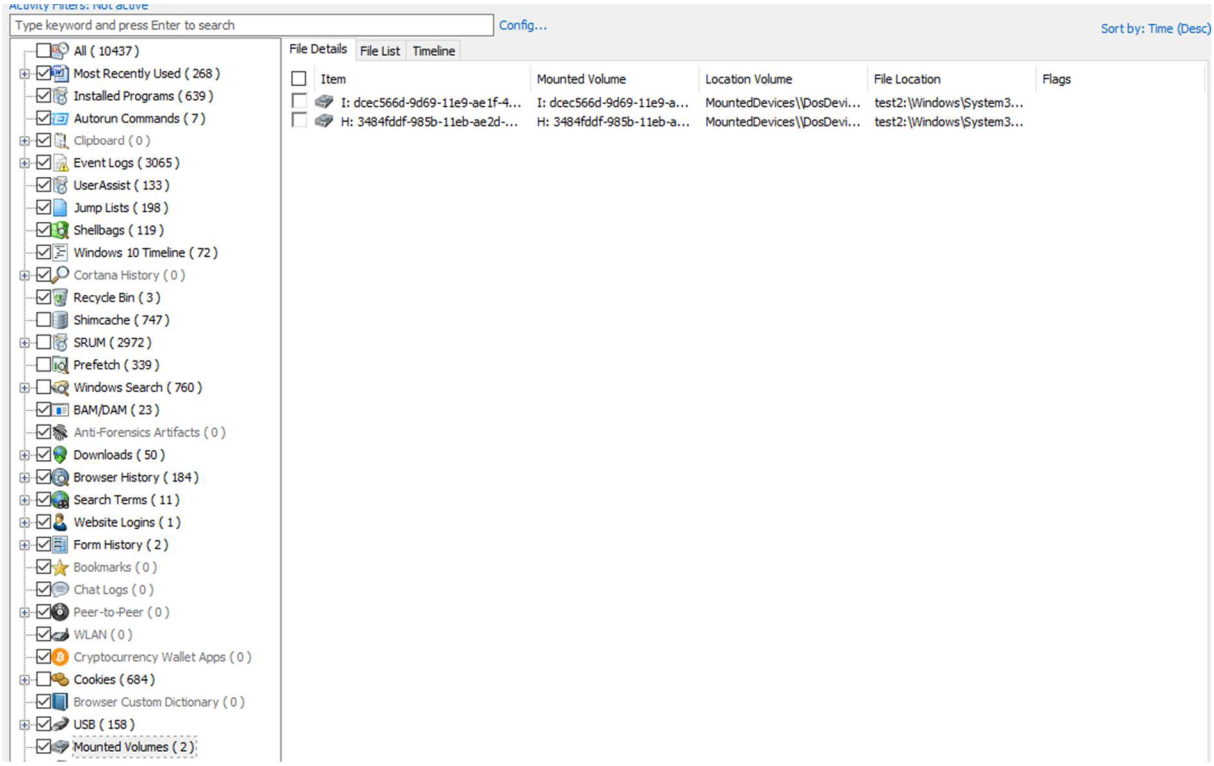



*Obrázek 39 - Příklad připojeného telefonu, kde vidíme jednoznačné IMEI, to může pomoci pro identifikaci a sběru dat z dalších zdrojů.*
Zdroj: vlastní




*Obrázek 40 - Příklad připojeného disku s konkrétním modelovým označením.*
Zdroj: vlastní

- Mounted Volumes
  Zde se zobrazí všechny disky, které mají přiřazené písmeno označení jednotky ve správci disků, nicméně chybí konkrétnější označení disku jako by byl například výrobce nebo model. Po rozkliknutí položky se objeví surová binární/hexadecimální data z registru, nicméně se mi nepodařilo zjistit nic čitelného, co by mohla znamenat. Převodem na text lze určit pouze DVD mechaniky a úložiště připojená jako MTP.



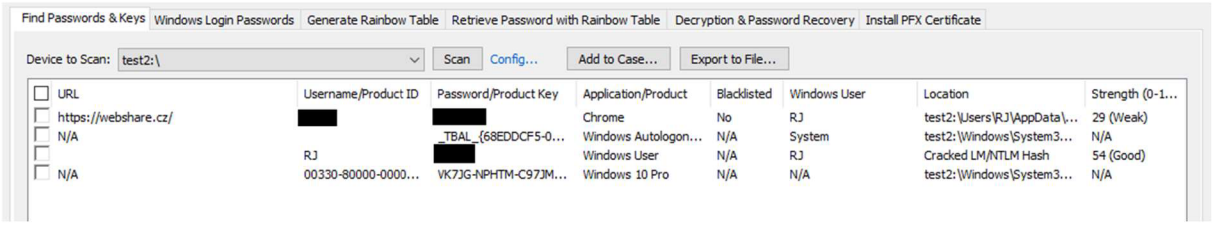

*Obrázek 41 - Přiřazené disky k počítači.*
Zdroj: vlastní

f) Passwords

V této kategorii se hromadně zobrazí veškeré nalezené produktové klíče na software od Microsoftu, přihlašovací údaje lokálních Windows účtů nebo uložená hesla v prohlížečích. V případě, že je dostupný pouze hash hesla, lze z časových důvodů u jednoduchých hesel formou brute-force (postupné testování všech možných kombinací hesel o určité délce a znakové sadě) heslo zpět obnovit do čitelné podoby.
Jelikož je sekce rozdělena na několik karet, zmíním ty nejdůležitější:

Find Passwords & Keys

- Kompletní výpis všech nalezených údajů s podrobnostmi.



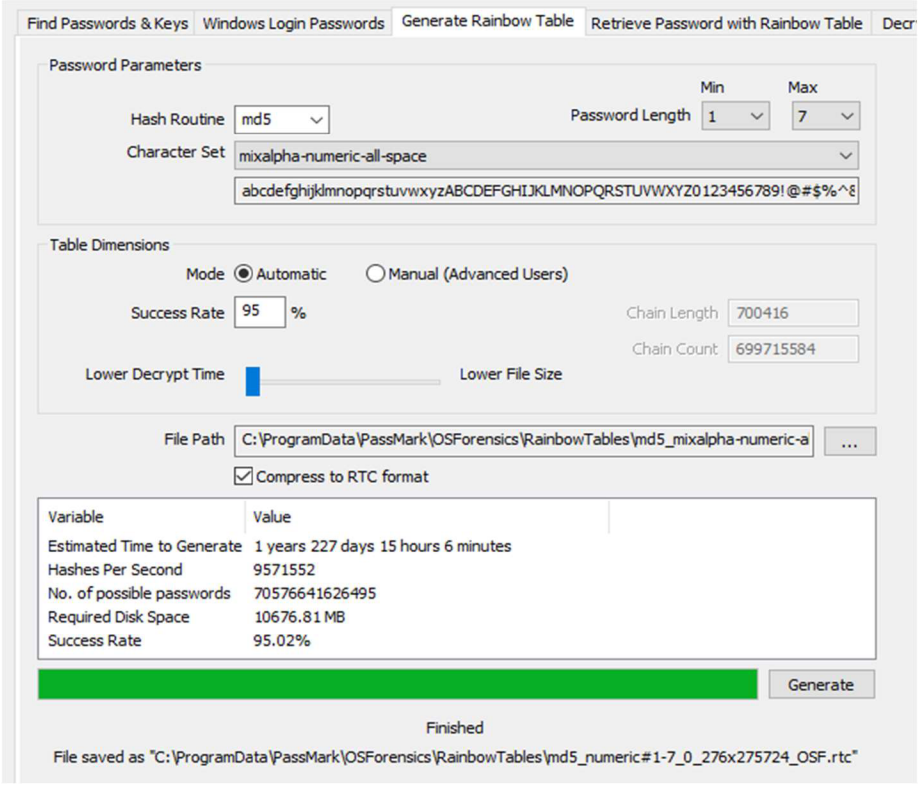

*Obrázek 42 - Nalezené přihlašovací údaje a produktové klíče.*
Zdroj: vlastní

Windows Login Passwords

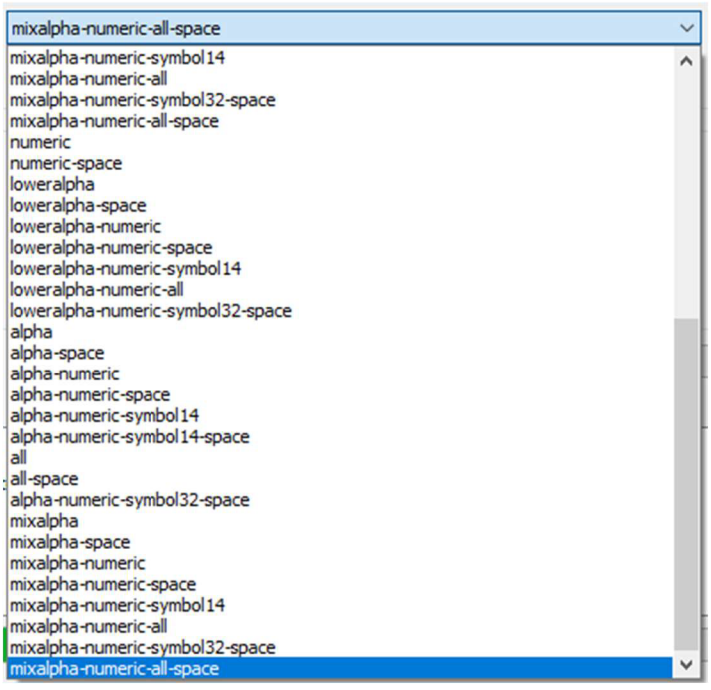
- Filtrovaný výpis uživatelských účtů Windows včetně těch systémových. V případě využívání doménových uživatelských účtů prostřednictvím Active Directory, lze načíst z cache informace o posledních přihlášených účtech.
- V případě zaškrtnutí checkboxu Test common passwords program metodou porovnávání hashe může obnovit hesla, které již v databázi programu mají vygenerované kombinace. V základu se jedná o číselné kombinace do 8 znaků a hesla ze slovníku nejčastějších hesel.

Generate rainbow table

- Karta slouží pro vygenerování kombinací hashů pro porovnávání již šifrovaných hesel a obnovení do čitelné podoby.
- Na výběr jsou 4 hashovací funkce (MD5, LM, SHA1 a NTLM), rozsah počtu znaků hesla a znaková sada, které může obsahovat od pouze čísel po speciální symboly.
- Po otevření karty je proveden několikasekundový test výkonu počítače, který slouží pro následný odhad času potřebného pro výpočet všech kombinací.
- Z časových důvodů nemusí být efektivní generování tabulek s velkým množstvím různých znakových sad, proto může být efektivnější stažení již dříve vygenerované tabulky na výkonnějším počítači. Například generování všech kombinací malých, velkých písmen a číslic na běžných počítačích může zabrat nejméně týden, každý další znak pak dobu ještě násobí. Tabulky lze například stáhnout na webu https://freerainbowtables.com (47) prostřednictvím peer-to-peer sítě uživatelů, kde si lze vybrat znakovou sadu a počet znaků, nicméně vzhledem k velikosti souborů a nejisté rychlosti připojení od uživatelů nemusí být stahování nutně rychlejší varianta, zejména u generování, které trvá řádově pouze dny.
- Může být efektivní nejdříve generovat jednoduché tabulky s malým množstvím kombinací (například pouze malá písmena a čísla) a až po neúspěšném pokusu generovat další kombinace. Pokud se heslo nachází v první, ušetříme čas s generováním dalších kombinací.



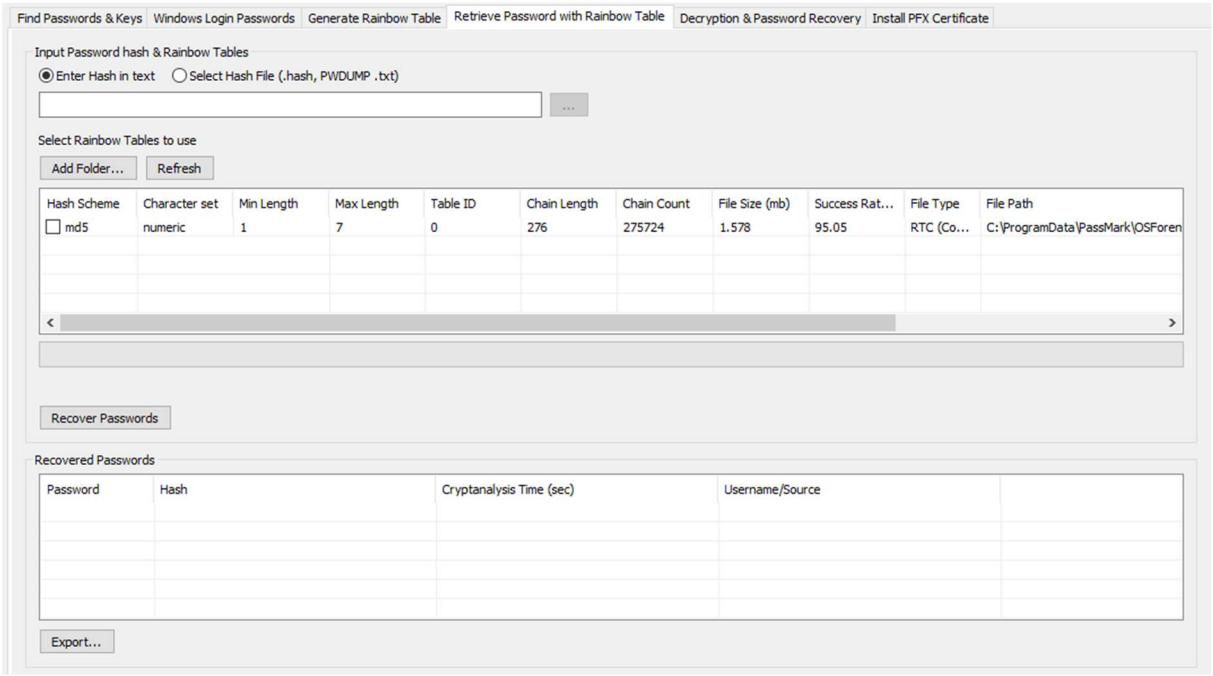

*Obrázek 43 - Okno pro vygenerování hashů hesel pro všechny zadané kombinace.*
Zdroj: vlastní




*Obrázek 44 - Možnosti výběru znakových sad.*
Zdroj: vlastní

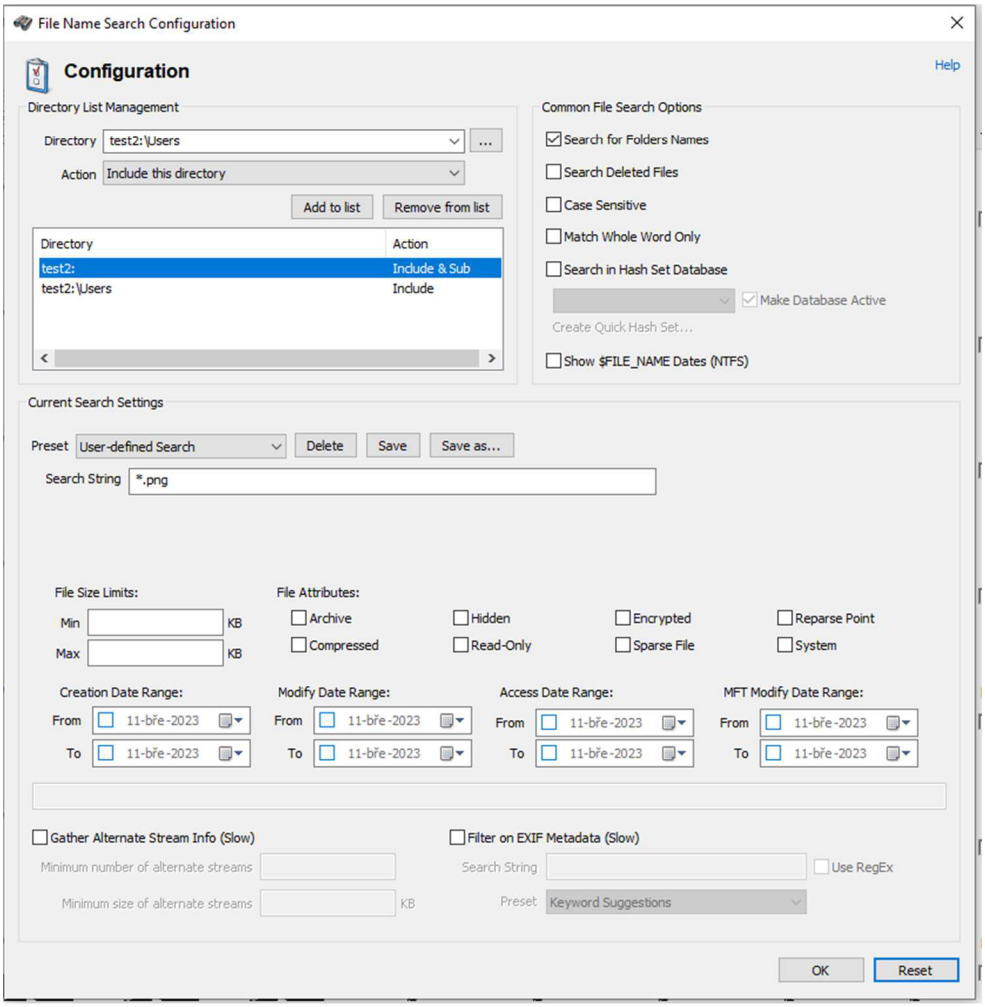
Retrieve Password with Rainbow Table

- Vygenerované tabulky lze využít pro obnovu hesla do čitelné podoby z hashe, který obdržíme i jiným způsobem, například z dat programu, který využívaný software nedokáže automaticky načíst. Limitujícím faktorem může být zejména omezený výčet podporovaných hashovacích funkcí, jelikož novější software často využívá SHA-2 nebo SHA-3, které již program nepodporuje. Dalším hlediskem je využívání soli (z ang. pojmu salt), což značí přidání dalšího řetězce několika bitů při hashování a tím přidání dalších teoreticky možných kombinací, pokud neznáme původní sůl (48).
- Je možné najednou obnovit více hesel při použití načítání z *.txt souboru.

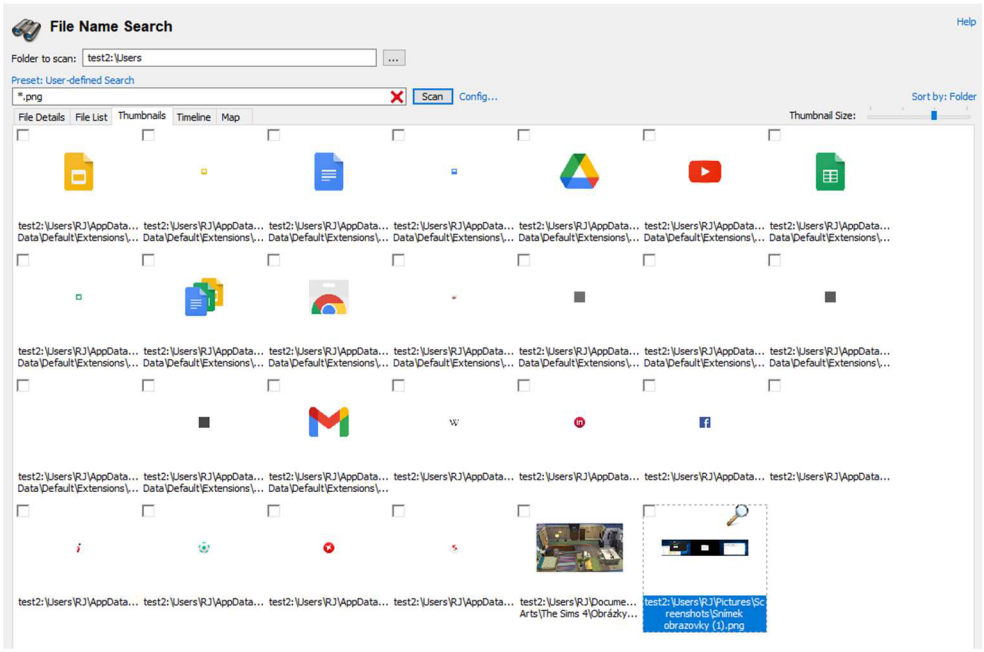



*Obrázek 45 - Obnova hesla z hashe.*
Zdroj: vlastní

a) File Name Search
Lze prohledat celý image disku pro hledané soubory na základě zvolených parametrů nebo atributů jako například rozsah velikosti, data, adresáři nebo formátu i mezi již smazanými soubory, které byly ale stále fyzicky uloženy na disku. V hledaném názvu lze využívat i nahrazovací znaky za libovolný znak nebo řetězec. Multimediální soubory je možné filtrovat dle EXIF metadat.

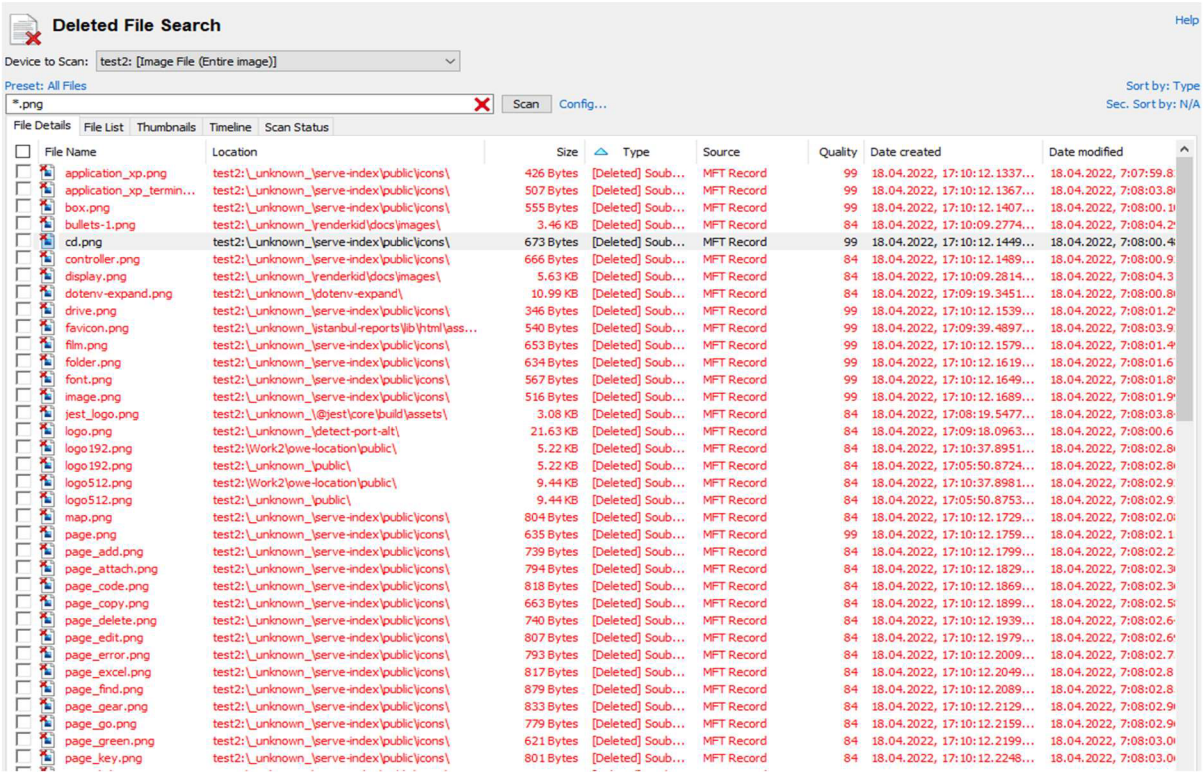



*Obrázek 46 - Hledání souborů hle parametrů a atributů.*
Zdroj: vlastní

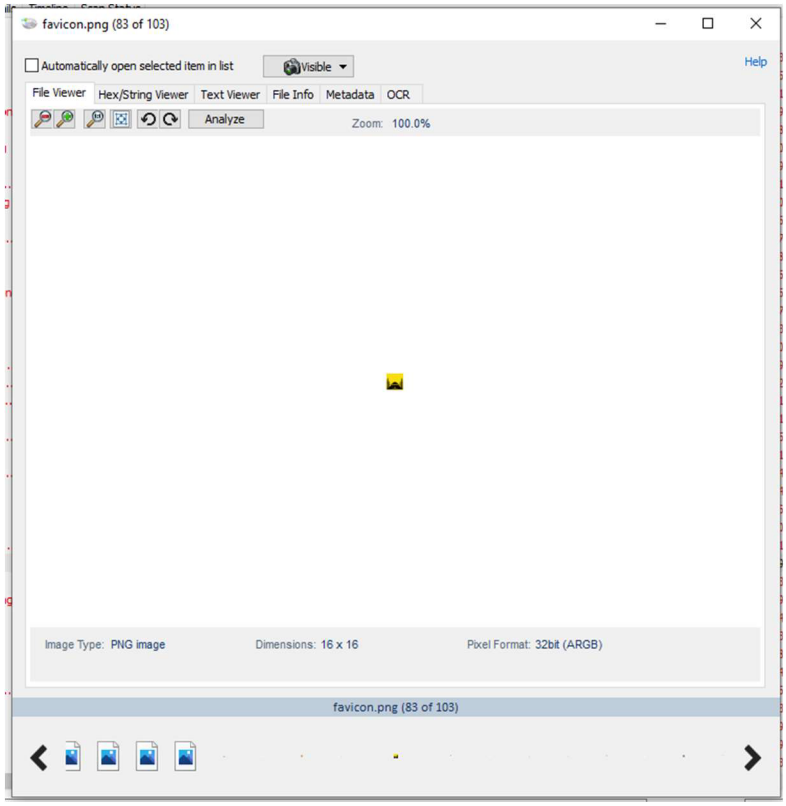



*Obrázek 47 - Příklad výsledků vyhledávání v podadresáři souborů s příponou PNG.*
Zdroj: vlastní

a) Deleted File Search
Funkce odpovídá názvu – slouží pro hledání již smazaných souborů. Program prohledá u disků s formátem dat NTFS tabulku MFT (49) (Master File Table), která ukládá informace o všech souborech na disku (název, datum vytvoření, atributy a velikost) a jejich fyzické adrese na disku. V případě, že je soubor uživatelem smazán, je odstraněna informace z tabulky a použitý adresní prostor označen jako volný. V případě, že není přepsán novým souborem, lze data stále přečíst, jen se uživateli nezobrazují. V závislosti na přepsání, může být čitelný celý soubor nebo jen jeho část (50; 51).




*Obrázek 48 - Výpis nalezených smazaných souborů.*
Zdroj: vlastní

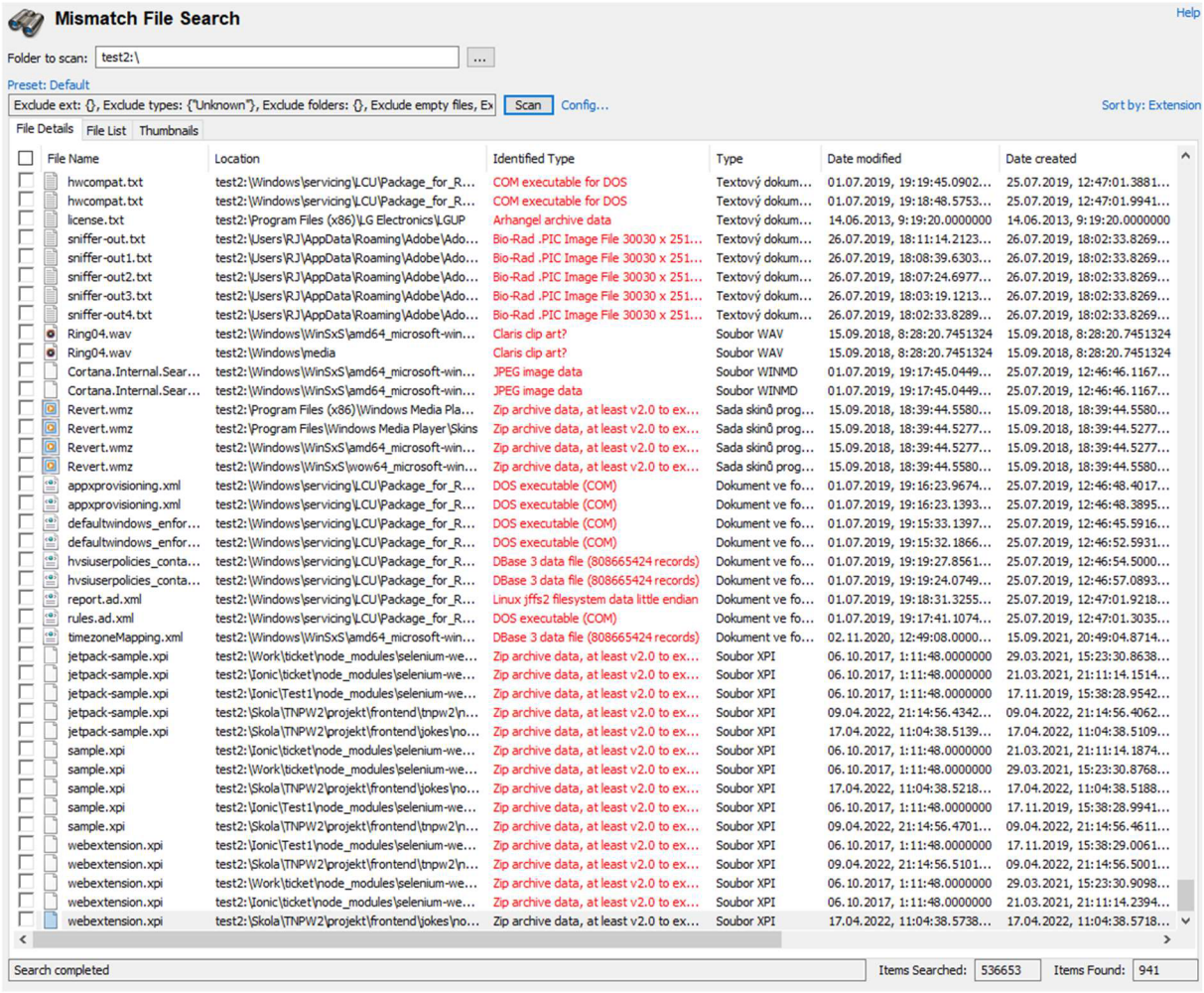



*Obrázek 49 - Příklad zobrazeného souboru.*
Zdroj: vlastní

a) Mischmatch File Search

Tato funkcionalita hledá soubory, které mají odlišný bitový formát od přípony souboru v názvu. To může značit, že se uživatel snažil skrýt soubor před nalezením při forenzní analýze změnou přípony. Je ale nutné odlišovat soubory dat programů, spousta programů si ukládá vlastní data v běžně používaném formátu, ale využívá například vlastní příponu pro jednoznačnou identifikaci programem.

Při hledání lze filtrovat hledání dle používaných přípon, typů souborů, podsložek, atributy nebo jednoduše předvolbou v programu vyloučit například známé soubory z OS Windows nebo cache internetových prohlížečů.



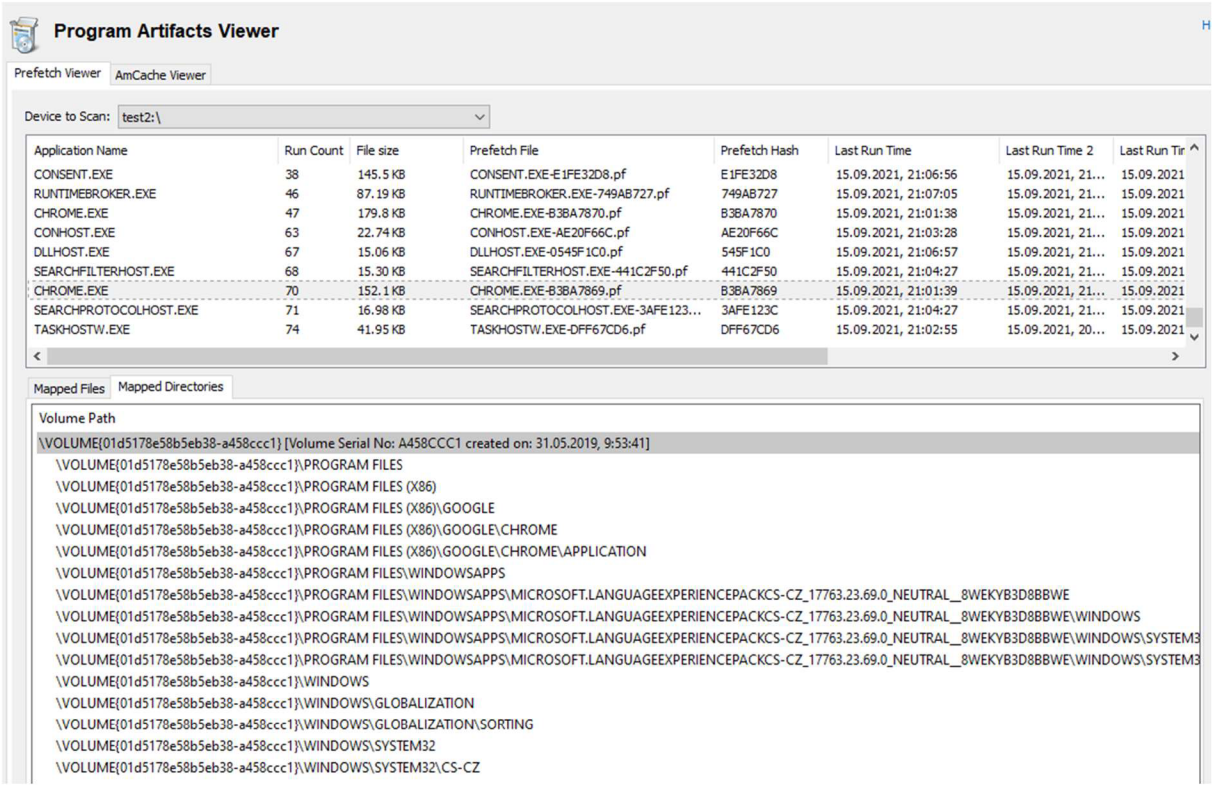

*Obrázek 50 - Příklady nalezených souborů s odlišnou datovou strukturou od přípony v názvu.*

Zdroj: vlastní

a) Program Artifacts

V sekci Prefetcher lze najít potencionálně zajímavé informace pro forenzní analýzu uložené v nástroji Prefetcher (52) OS Windows, ten často načítané soubory načte předem do paměti RAM pro rychlejší běh programu, v době využívání jako systémového disku SSD je reálný přínos v rychlosti minimální.

Pokud systém načte soubory určitého programu, uloží data s informacemi o programu a souborech, ke kterým přistupuje. Tímto způsobem lze odhalit poslední spuštěné programy nebo soubory, které uživatel naposledy otevřel. To může pomoci s určením, kterým směrem se dále může forenzní analýza zabývat.




*Obrázek 51 - Výpis programů se seznamem složek, ke kterým program přistupuje.*
Zdroj: vlastní

Druhou sekcí je AmCache Viewer, tento typ cache využívají OS Windows 7 a novější pro ukládání dat o přistupovaných souborech, použitých zástupcích, připojených zařízeních nebo ovladačích zařízení. Pro cache je využíván soubor C:\Windows\apcompat\Programs\Amchache.hve (53; 54).

Data v AmCache jsou rozdělena do následujících kategorií:

a) Application Files
   Ukládá informace o souborech, které otevřely spuštěné programy.

b) Application Programs
   Zde jsou uloženy informace o programech, které byly spuštěny.

c) Driver Binaries
   V této části jsou uloženy informace o ovladačích jako například certifikáty autority, službách a zařízeních na které jsou vázány apod.

d) Pnp Devices
   Sekce obsahuje informace o dříve připojených odpojitelných zařízeních jako jsou telefony, tiskárny, monitory, klávesnice apod.

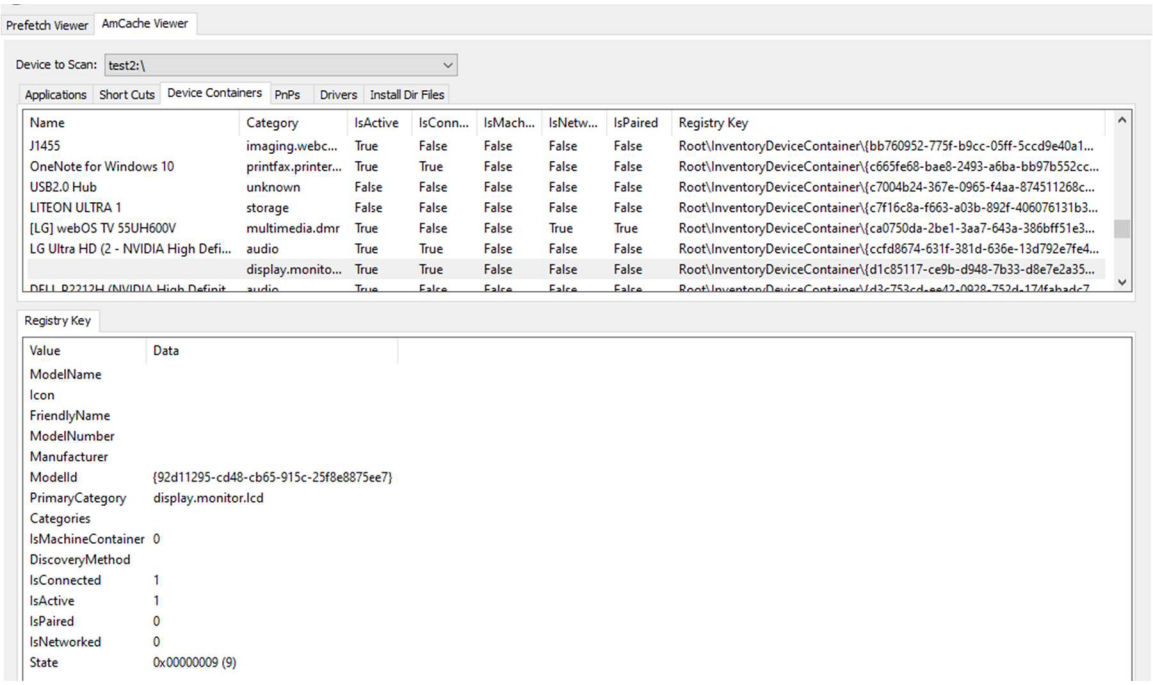
e) Driver Packages
   Souhrné podrobnosti o balíčcích ovladačů.

f) Device Containers
   Informace o zařízeních, které jsou registrovány v systému a nespadají pod obvykle odpojitelná zařízení.

g) Application Shortcuts
   Ukládá informace o zástupcích souborů jako jsou názvy, odkaz na cílový soubor nebo časovou značku posledního použití.

h) Files
   Podobná kategorie s Application Files, rozdílem je chybející USN atribut (Update Sequence Number), tím lze potencionálně nalézt další data na nealokované části disku.

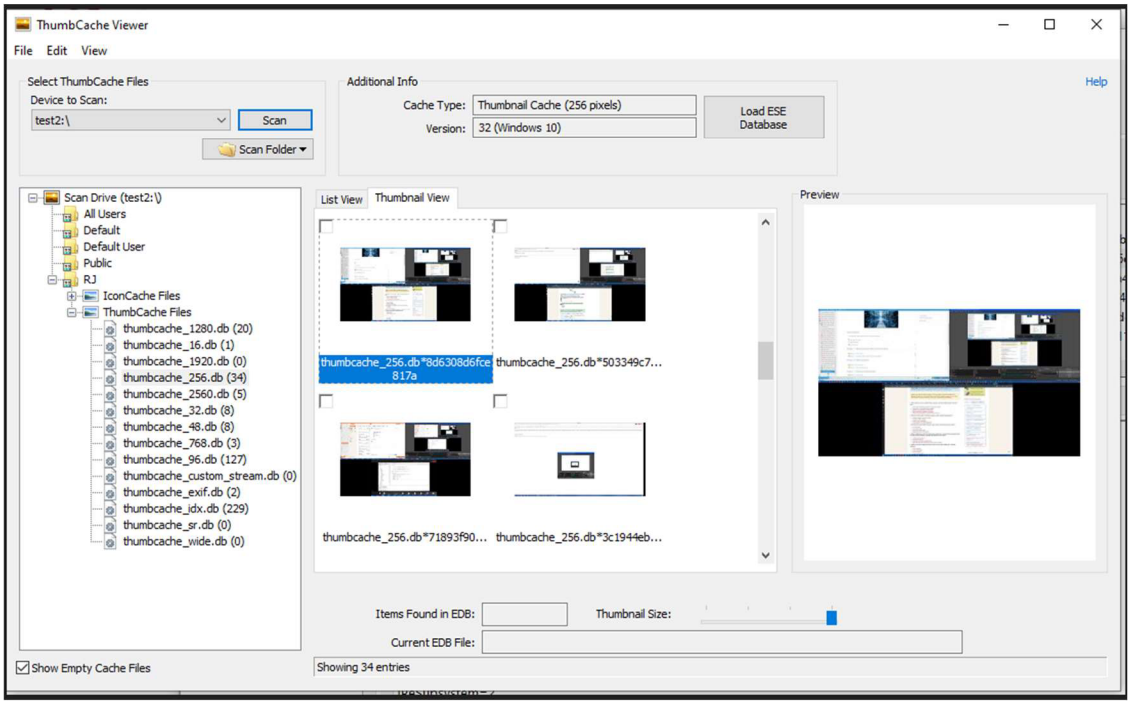
i) Programs
   Uchovává informace i o již odinstalovaných programech.




*Obrázek 52 - Příklad výpisu dříve připojených zařízení.*
Zdroj: vlastní

a) Raw Disk Viewer

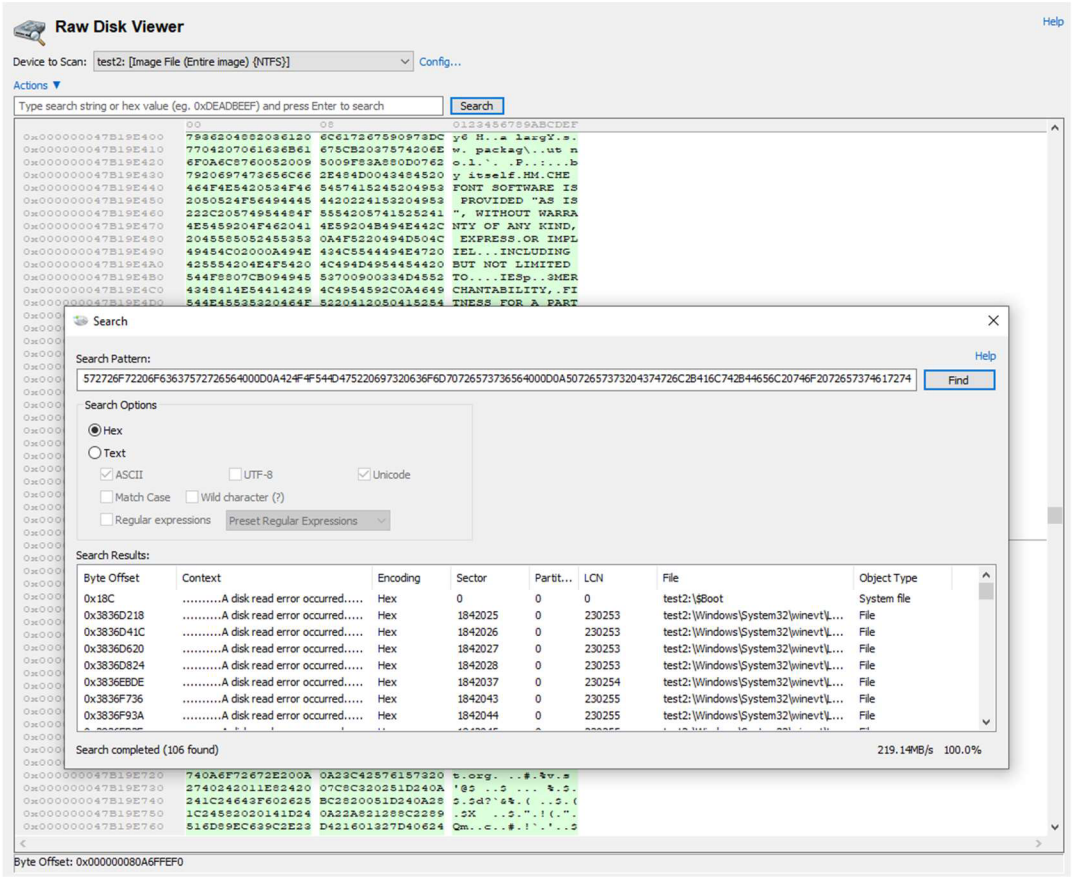
V této kategorii lze načíst uložené náhledy multimediálních souborů. Obecně jde tedy o obrázky, videa nebo i ikony složek, kde je možné na základě náhledu částečně rozpoznat o jaký typ obsahu se jednalo. V určitých případech je možné tímto způsobem najít náhledy již smazaných souborů nebo souborů na dříve připojených externích úložištích.




*Obrázek 53 - Náhledy (některých již smazaných) multimediálních souborů.*
Zdroj: vlastní

a) Raw Disk Viewer

Prostřednictvím procházení bitových dat disku lze hledat konkrétní řetězce buď v hexadecimálním formátu nebo jako textový řetězec. Pro takové hledání je obvykle mít předem daná data, která chceme ověřit, se že na disku nacházejí. Druhým případem je hledání dat, která mohou být uložena mimo obvykle dostupný prostor jako jsou například volné clustery po smazaných souborech nebo data ukrytá v prostoru nevyužitých celých sektorů (pokud má soubor velikost 1 KB, je využit 4 KB sektor a 3 KB prostoru zbývá nevyužito, tzv. free slack space). Lze tedy najít části i dlouhou dobu smazaných dat, zejména na koncích adresního prostoru jednotlivých sektorů.




*Obrázek 54 - Příklad hledání hexadecimálního řetězce.*
Zdroj: vlastní

a) Signatures

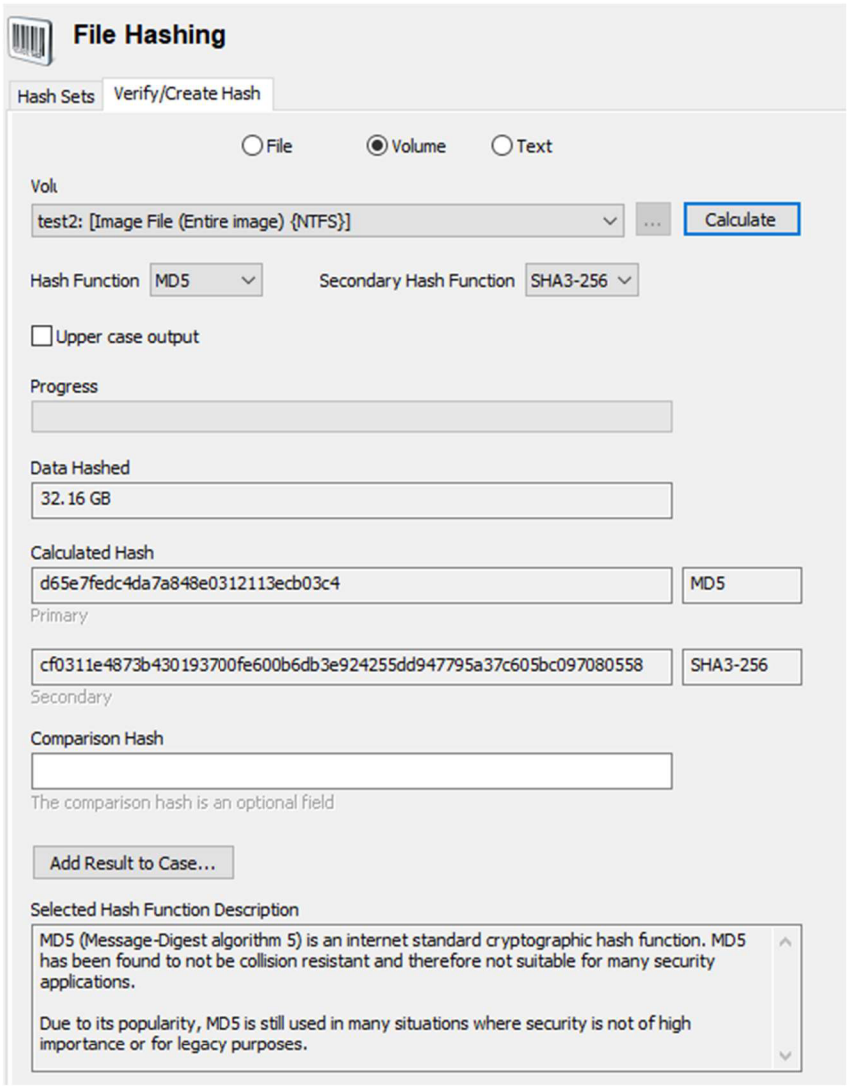
Tato část aplikace slouží pro jednoznačné porovnání informací o všech uložených souborech mezi dvěma kopiemi a případně vypíše změněné soubory. Je vhodné využít například po delším zkoumání pro ověření, že nedošlo ať už úmyslné nebo neúmyslné změně dat.

b) File Hasning

Hash dat funguje jako jednoznačný otisk unikátnosti, jelikož malá změna vstupních dat značně ovlivní výsledný hash a vzhledem k počtu kombinací (v případě MD5 32 hexadecimálních znaků, tedy 16^32, což je přibližně 3,4×10^38 kombinací) je velmi malá šance, že by výsledný hash mohl být shodný, nicméně šance existuje.

Z takového důvodu je vhodné použít buď hashovací funkci o delším řetězci (například SHA3-512 – 128 hexadecimálních znaků, tedy přibližně 1,3×10^154 různých kombinací) nebo dvě různé hashovací funkce. Tím je

přidáno více teoreticky možných kombinací a zároveň naprosto minimalizována šance, že by oba kontrolní řetězce byly v obou případech stejné při změně souboru. Pro základní kontrolu shodného souboru nicméně obvykle dostačuje i MD5.




*Obrázek 55 - Vytvoření a provnání hashe souboru.*
Zdroj: vlastní

### 6.2.1 Shrnutí programu

Nástroj OSForensics nabízí spoustu základních forenzních nástrojů pro analýzu „živého stroje“, vytvoření bitové kopie disku a jeho analýzu nebo základní rozbor dumpu paměti RAM. Také nabízí možnost ukládat veškerá data pod založené případy pro jednodušší dohledání dříve zjištěných informací. Oproti jiným nástrojům ve většině případů příliš

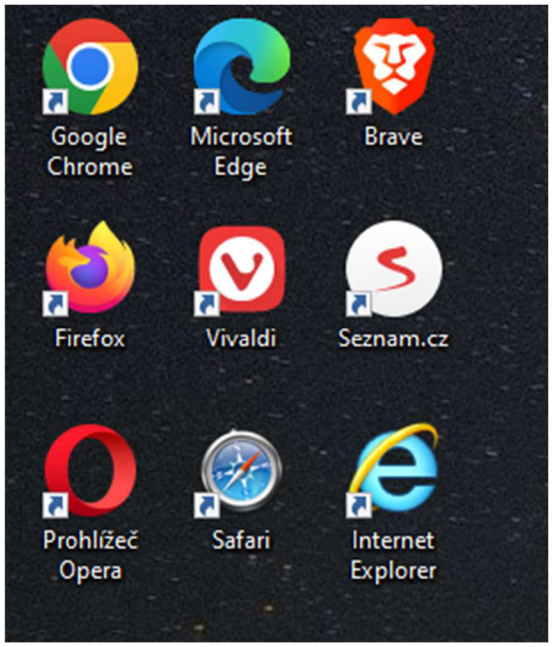
neinterpretuje zjištěná data, samotná interpretace je tak na uživatelovi. Výjimkou je zejména kategorie User Activity, kde data třídí například i podle nainstalovaných programů.

### 6.2.2 Podrobná analýza historie webových prohlížečů

Jelikož spousta uživatelů na počítači používá zejména internetový prohlížeč a zároveň se jedná o aspekt, který lze najít na prakticky jakémkoli počítači, budu se tedy podrobněji věnovat této části.

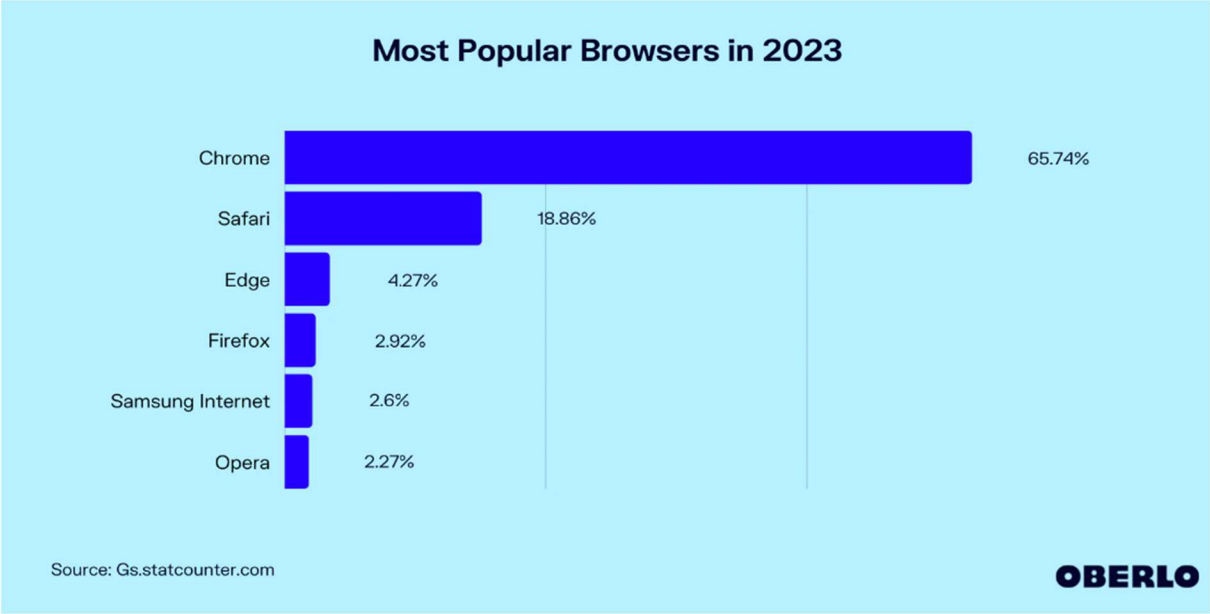
V práci využiji tyto prohlížeče:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Vivaldi
- Safari
- Seznam.cz prohlížeč
- Opera
- Brave
- Internet Explorer




*Obrázek 56 - Přehled vyzkoušených webových prohlížečů.*
Zdroj: vlastní

Tyto prohlížeče byly vybrány, jelikož se jedná o všechny aktuálně používané prohlížeče i s těmi, které již mají minimální tržní podíl. Výjimkou je prohlížeč Safari, který je pro ve verzi pro Windows od roku 2015 neaktualizovaný (55). Podobně sporadické je reálné využití prohlížeče Internet Explorer na Windows 10 a novější, jelikož standardně po načtení webové stránky ji otevře znovu v Microsoft Edge, nicméně na starších verzích Windows se zřejmě ještě najde část uživatelů, kteří jej budou využívat.



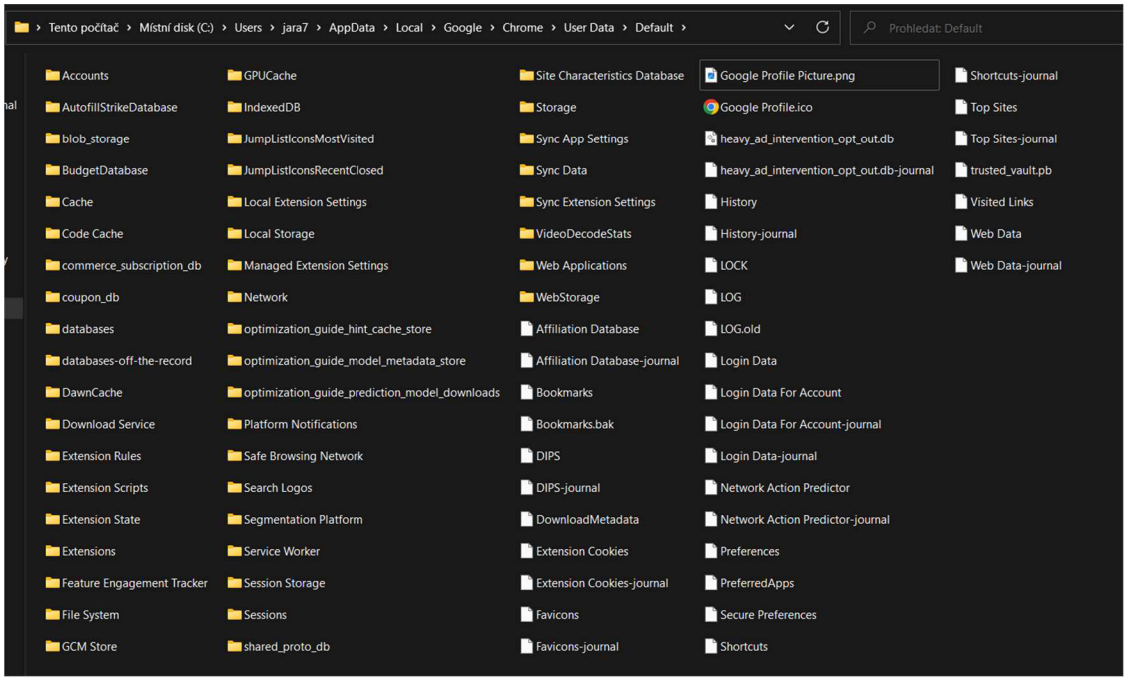

Obrázek 57 - Graf podílů webových prohlížečů **(56)**.

Jelikož v tuto chvíli naprostá většina prohlížečů je založena na jádru Chromium (57), princip ukládání dat prohlížečů je velmi podobný a tak pro vývojáře software pro interpretaci dat prohlížečů je jednoduché přidat podporu pro další prohlížeč.

Zároveň pro účely forenzní analýzy může být vhodné využít uložené přihlašovací údaje do webových služeb nebo session klíče přihlášení, viz. podrobněji výše, nicméně konkrétními podrobnostmi využití a zpracování těchto dat se rozsah této práce nezabývá.

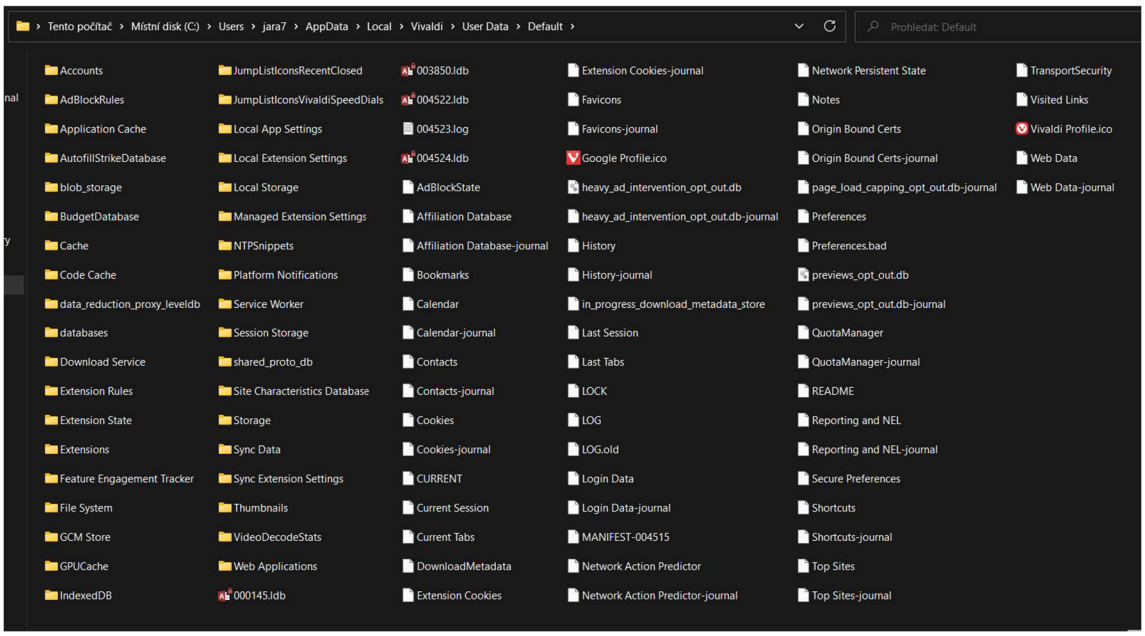
Datová struktura

Data prohlížeče Chrome je uložena v OS Windows 7 a novější v adresáři C:\Users\[USERNAME]\AppData\Local\Google\Chrome\User Data\Default (Google Chrome verze 109), ve starších verzích prohlížeče může být umístění konkrétních dat odlišné (58).



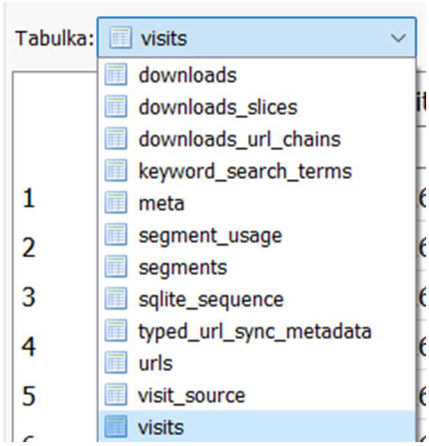

*Obrázek 58 - Uživatelská data prohlížeče Chrome.*
Zdroj: vlastní

V jiných prohlížečích je struktura dat podobná, liší se zejména na základě specifických funkcí daných prohlížečů.

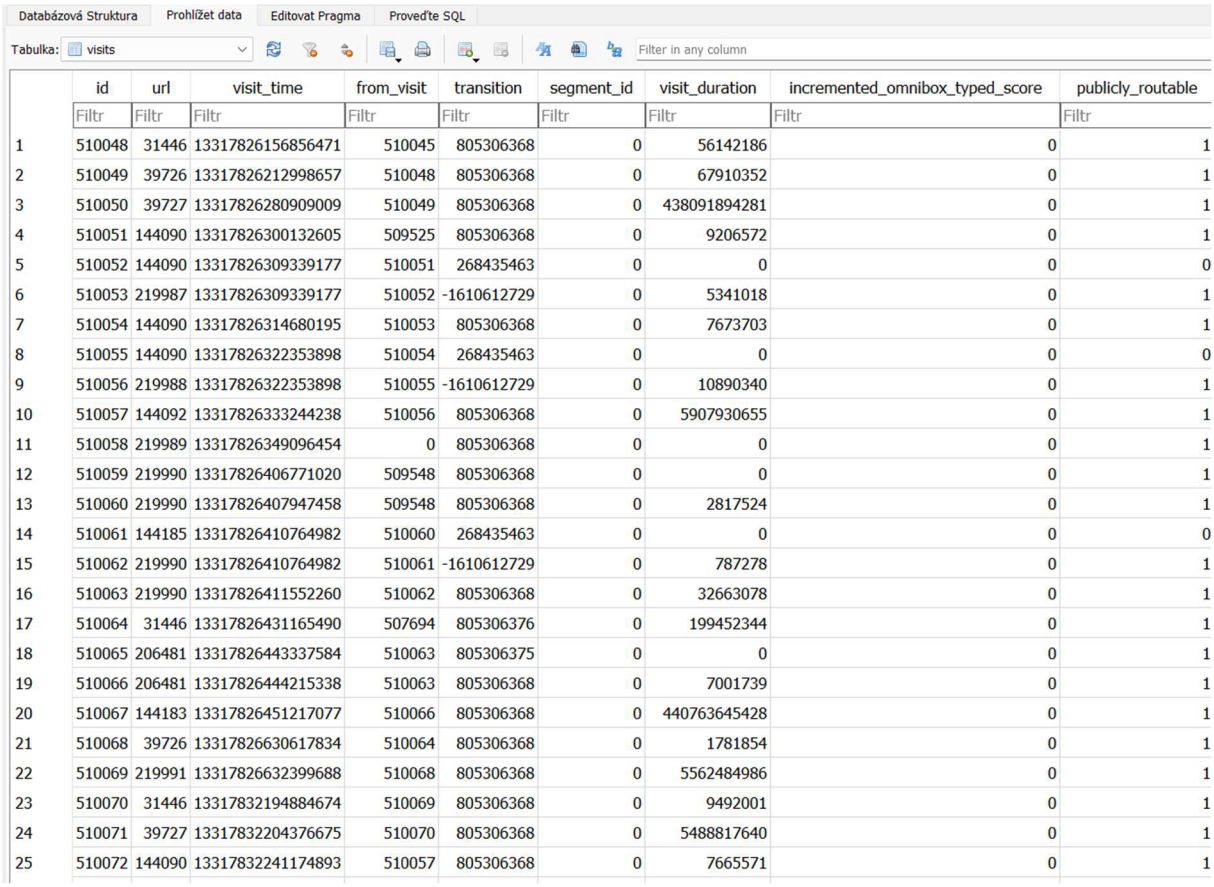



*Obrázek 59 - Uživatelská data prohlížeče Vivaldi.*
Zdroj: vlastní

Na screenshotu výše lze porovnat stejnou složku a její obsah v jiném prohlížeči založeném na jádru Chromium – Vivaldi. Data historie procházení jsou uložena v tomto adresáři v souboru History (bez přípony) ve formátu SQLite v tabulce visits, konkrétní adresa v tabulce urls. Po aktualizaci ze starší verze chrome je soubor historie procházení přejmenován na Archived History (opět stejný formát SQLite), v takovém případě je tedy starší historie procházení uložena v separátním souboru.




*Obrázek 60 - Tabulky v souboru History.*
Zdroj: vlastní



Databázová Struktura | Prohlížet data | Editovat Pragma | Proveďte SQL

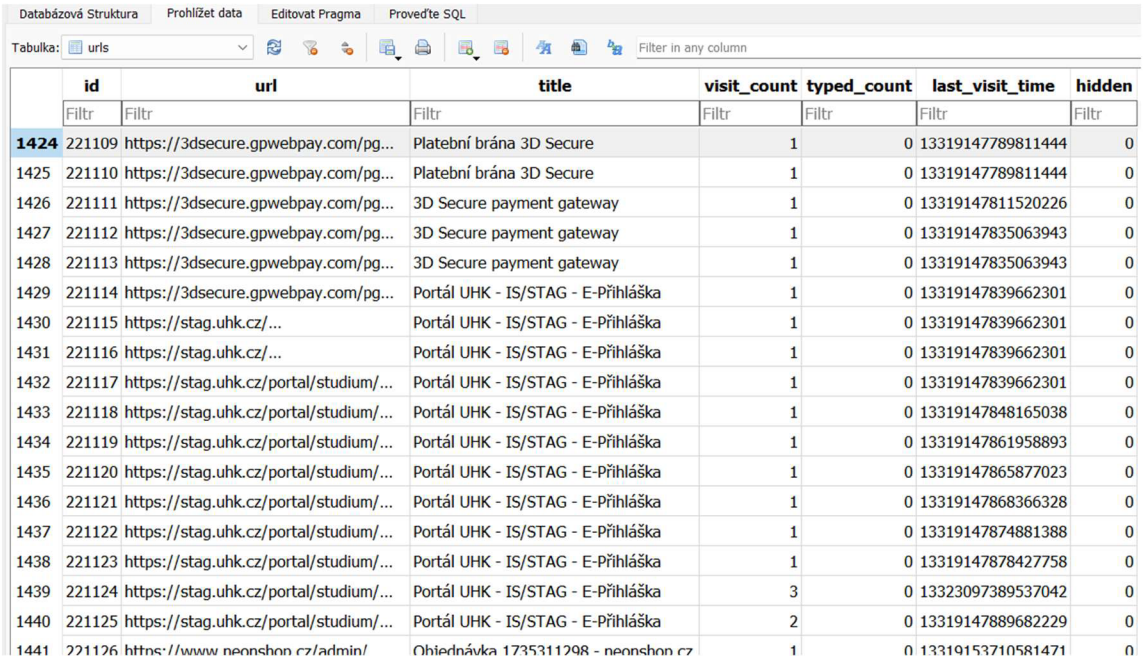
Tabulka: visits — Filter in any column

| | id | url | visit_time | from_visit | transition | segment_id | visit_duration | incremented_omnibox_typed_score | publicly_routable |
|---|---|---|---|---|---|---|---|---|---|
| | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr |
| 1 | 510048 | 31446 | 13317826156856471 | 510045 | 805306368 | 0 | 56142186 | 0 | 1 |
| 2 | 510049 | 39726 | 13317826212998657 | 510048 | 805306368 | 0 | 67910352 | 0 | 1 |
| 3 | 510050 | 39727 | 13317826280909009 | 510049 | 805306368 | 0 | 438091894281 | 0 | 1 |
| 4 | 510051 | 144090 | 13317826300132605 | 509525 | 805306368 | 0 | 9206572 | 0 | 1 |
| 5 | 510052 | 144090 | 13317826309339177 | 510051 | 268435463 | 0 | 0 | 0 | 0 |
| 6 | 510053 | 219987 | 13317826309339177 | 510052 | -1610612729 | 0 | 5341018 | 0 | 1 |
| 7 | 510054 | 144090 | 13317826314680195 | 510053 | 805306368 | 0 | 7673703 | 0 | 1 |
| 8 | 510055 | 144090 | 13317826322353898 | 510054 | 268435463 | 0 | 0 | 0 | 0 |
| 9 | 510056 | 219988 | 13317826322353898 | 510055 | -1610612729 | 0 | 10890340 | 0 | 1 |
| 10 | 510057 | 144092 | 13317826333244238 | 510056 | 805306368 | 0 | 5907930655 | 0 | 1 |
| 11 | 510058 | 219989 | 13317826349096454 | 0 | 805306368 | 0 | 0 | 0 | 1 |
| 12 | 510059 | 219990 | 13317826406771020 | 509548 | 805306368 | 0 | 0 | 0 | 1 |
| 13 | 510060 | 219990 | 13317826407947458 | 509548 | 805306368 | 0 | 2817524 | 0 | 1 |
| 14 | 510061 | 144185 | 13317826410764982 | 510060 | 268435463 | 0 | 0 | 0 | 0 |
| 15 | 510062 | 219990 | 13317826410764982 | 510061 | -1610612729 | 0 | 787278 | 0 | 1 |
| 16 | 510063 | 219990 | 13317826411552260 | 510062 | 805306368 | 0 | 32663078 | 0 | 1 |
| 17 | 510064 | 31446 | 13317826431165490 | 507694 | 805306376 | 0 | 199452344 | 0 | 1 |
| 18 | 510065 | 206481 | 13317826443337584 | 510063 | 805306375 | 0 | 0 | 0 | 1 |
| 19 | 510066 | 206481 | 13317826444215338 | 510063 | 805306368 | 0 | 7001739 | 0 | 1 |
| 20 | 510067 | 144183 | 13317826451217077 | 510066 | 805306368 | 0 | 440763645428 | 0 | 1 |
| 21 | 510068 | 39726 | 13317826630617834 | 510064 | 805306368 | 0 | 1781854 | 0 | 1 |
| 22 | 510069 | 219991 | 13317826632399688 | 510068 | 805306368 | 0 | 5562484986 | 0 | 1 |
| 23 | 510070 | 31446 | 13317832194884674 | 510069 | 805306368 | 0 | 9492001 | 0 | 1 |
| 24 | 510071 | 39727 | 13317832204376675 | 510070 | 805306368 | 0 | 5488817640 | 0 | 1 |
| 25 | 510072 | 144090 | 13317832241174893 | 510057 | 805306368 | 0 | 7665571 | 0 | 1 |

*Obrázek 61 - Příklad struktury tabulky visits.*
Zdroj: vlastní

Na screenshotu výše lze zmínit zejména následující:

- url – ID je cizí klíč do tabulky urls
- visit_time – timestamp data a času návštěvy webové stránky (počet sekund od 1. ledna 1970 v časovém pásmu UTC+0, konvertovat hodnoty lze jednoduše například na webu https://www.unixtimestamp.com/)
- from_visit – předchozí url adresa, pokud uživatel proklikl na adresu z jiné webové stránky



Databázová Struktura | Prohlížet data | Editovat Pragma | Proveďte SQL

Tabulka: urls — Filter in any column

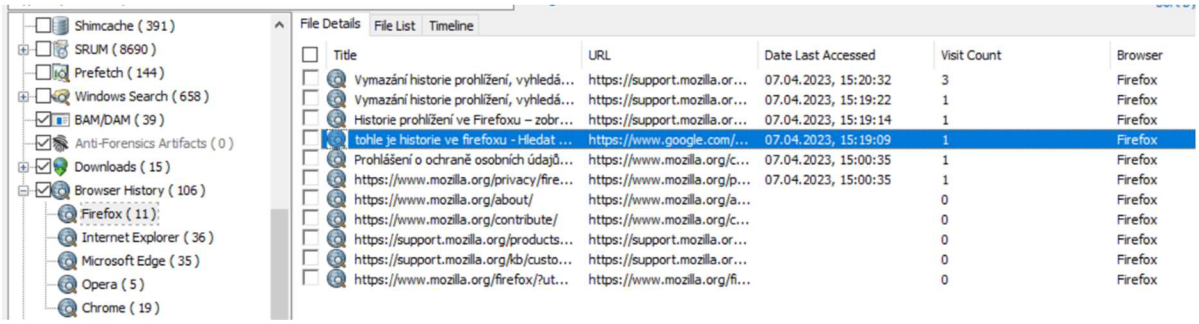
| | id | url | title | visit_count | typed_count | last_visit_time | hidden |
|---|---|---|---|---|---|---|---|
| | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr |
| 1424 | 221109 | https://3dsecure.gpwebpay.com/pg... | Platební brána 3D Secure | 1 | 0 | 13319147789811444 | 0 |
| 1425 | 221110 | https://3dsecure.gpwebpay.com/pg... | Platební brána 3D Secure | 1 | 0 | 13319147789811444 | 0 |
| 1426 | 221111 | https://3dsecure.gpwebpay.com/pg... | 3D Secure payment gateway | 1 | 0 | 13319147811520226 | 0 |
| 1427 | 221112 | https://3dsecure.gpwebpay.com/pg... | 3D Secure payment gateway | 1 | 0 | 13319147835063943 | 0 |
| 1428 | 221113 | https://3dsecure.gpwebpay.com/pg... | 3D Secure payment gateway | 1 | 0 | 13319147835063943 | 0 |
| 1429 | 221114 | https://3dsecure.gpwebpay.com/pg... | Portál UHK - IS/STAG - E-Přihláška | 1 | 0 | 13319147839662301 | 0 |
| 1430 | 221115 | https://stag.uhk.cz/... | Portál UHK - IS/STAG - E-Přihláška | 1 | 0 | 13319147839662301 | 0 |
| 1431 | 221116 | https://stag.uhk.cz/... | Portál UHK - IS/STAG - E-Přihláška | 1 | 0 | 13319147839662301 | 0 |
| 1432 | 221117 | https://stag.uhk.cz/portal/studium/... | Portál UHK - IS/STAG - E-Přihláška | 1 | 0 | 13319147839662301 | 0 |
| 1433 | 221118 | https://stag.uhk.cz/portal/studium/... | Portál UHK - IS/STAG - E-Přihláška | 1 | 0 | 13319147848165038 | 0 |
| 1434 | 221119 | https://stag.uhk.cz/portal/studium/... | Portál UHK - IS/STAG - E-Přihláška | 1 | 0 | 13319147861958893 | 0 |
| 1435 | 221120 | https://stag.uhk.cz/portal/studium/... | Portál UHK - IS/STAG - E-Přihláška | 1 | 0 | 13319147865877023 | 0 |
| 1436 | 221121 | https://stag.uhk.cz/portal/studium/... | Portál UHK - IS/STAG - E-Přihláška | 1 | 0 | 13319147868366328 | 0 |
| 1437 | 221122 | https://stag.uhk.cz/portal/studium/... | Portál UHK - IS/STAG - E-Přihláška | 1 | 0 | 13319147874881388 | 0 |
| 1438 | 221123 | https://stag.uhk.cz/portal/studium/... | Portál UHK - IS/STAG - E-Přihláška | 1 | 0 | 13319147878427758 | 0 |
| 1439 | 221124 | https://stag.uhk.cz/portal/studium/... | Portál UHK - IS/STAG - E-Přihláška | 3 | 0 | 13323097389537042 | 0 |
| 1440 | 221125 | https://stag.uhk.cz/portal/studium/... | Portál UHK - IS/STAG - E-Přihláška | 2 | 0 | 13319147889682229 | 0 |
| 1441 | 221126 | https://www.neonshop.cz/admin/ | Objednávka 1735311298 - neonshop.cz | 1 | 0 | 13319153710581471 | 0 |

*Obrázek 62 - Tabulka urls*
Zdroj: vlastní

V tabulce urls jsou uloženy konkrétní url adresy s textovým titulkem a timestamp údajem poslední návštěvy. Nicméně pro pohodlnější prohlížení je vhodné využít externí software, druhým možným způsobem prohlížení včetně dalších dat prohlížeče je zkopírování celé složky s datami prohlížeče do čisté instalace daného prohlížeče na našem počítači, nicméně takové použití pro forenzní analýzu nemusí být jasně průkazné, jelikož může jednoduše dojít ke změně dat.

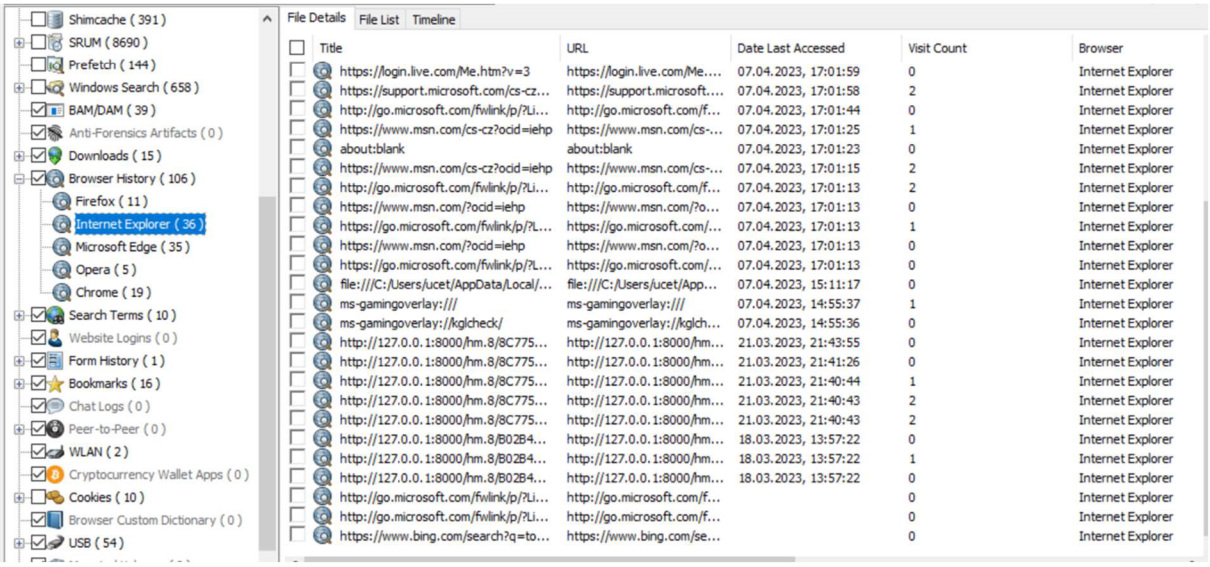
Konkrétní data z image disku lze prohlížet strukturovaně prostřednictvím výše zmíněného software OSForensics. Interpretovaná data lze zobrazit následovně.

### 6.2.2.1 Firefox




*Obrázek 63 - Historie prohlížeče Firefox (verze 111).*
Zdroj: vlastní

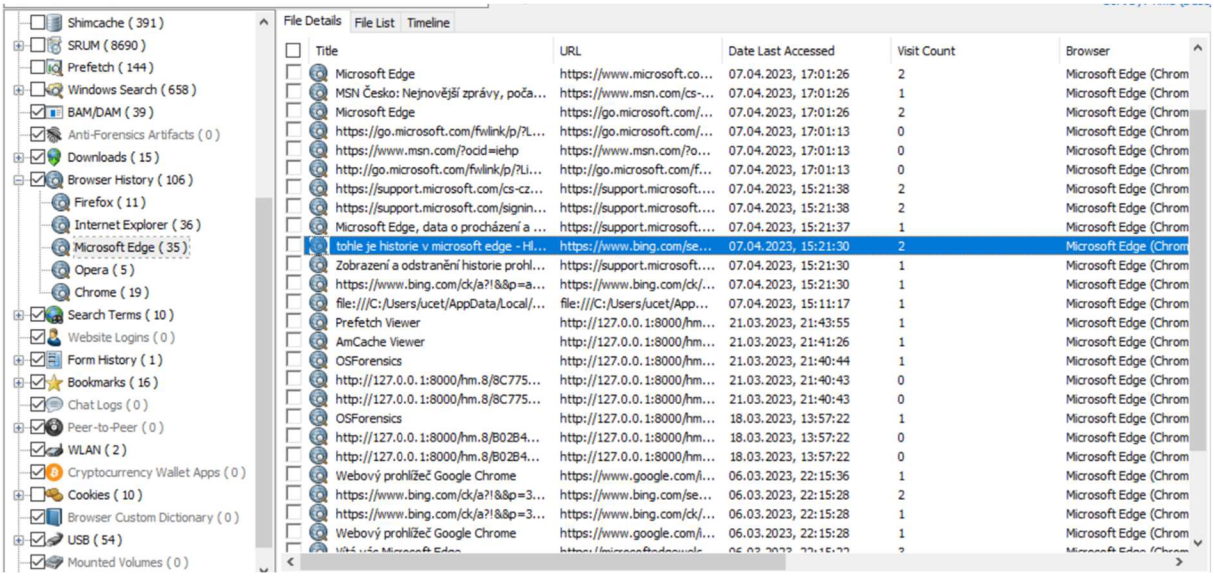
### 6.2.2.2 Internet Explorer




*Obrázek 64 - Historie prohlížeče Internet Explorer (verze 11).*
Zdroj: vlastní

Na screenshotu výše lze pozorovat, že jej jako vykreslovací engine využívají i další programy, které spustí lokální web server. Na základě titulků tedy můžeme zjistit o jaký program se mohlo jednat a případně tak tyto informace dále využít při forenzní analýze. Jelikož již ale není podporován, při pokusu o načtení webové stránky pouze otevře Microsoft Edge (pouze Windows 10 a novější) a načte požadovanou webovou stránku tam, zde se tedy tento pokus neobjeví.

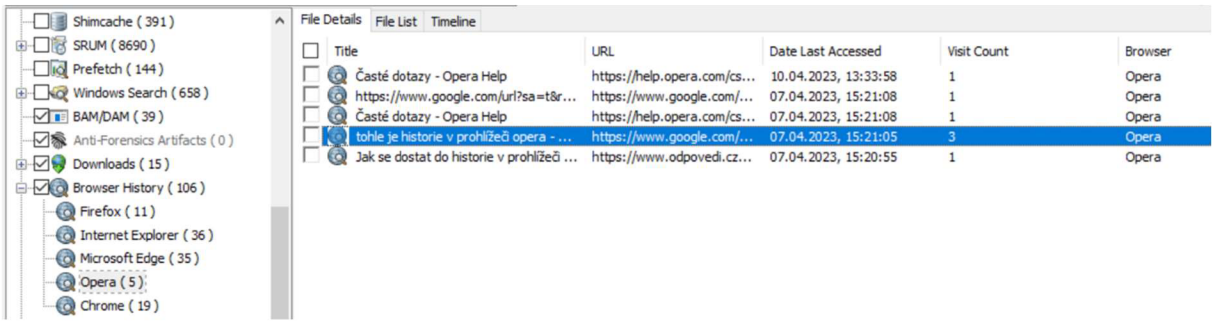
### 6.2.2.3 Microsoft Edge




*Obrázek 65 - Historie v prohlížeči Microsoft Edge.*
Zdroj: vlastní

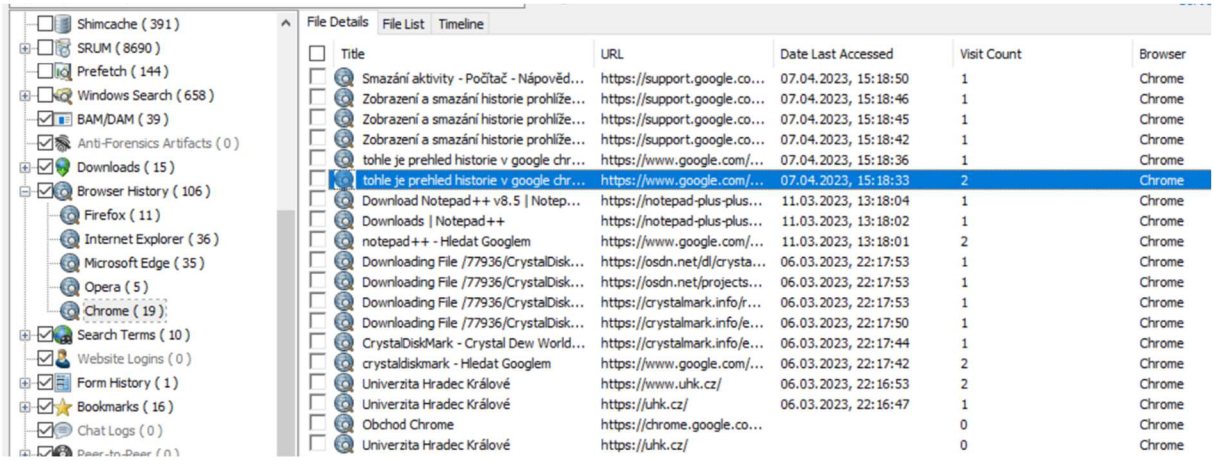
Podobně jako v Internet Exploreru prohlížeč Microsoft Edge je využíván jako vykreslovací engine a tak tam lze najít v titulcích další potencionální informace.

### 6.2.2.4 Opera




*Obrázek 66 - Historie v prohlížeči Opera (verze 97).*
Zdroj: vlastní

### 6.2.2.5 Google Chrome




*Obrázek 67 - Historie v prohlížeči Google Chrome (verze 111).*
Zdroj: vlastní

### 6.2.2.6 Ostatní prohlížeče

Další testované prohlížeče se v tomto výpisu v programu OSForensics nezobrazí, opět se jedná o podobnou strukturu adresářů.

#### *6.2.2.6.1 Vivaldi*

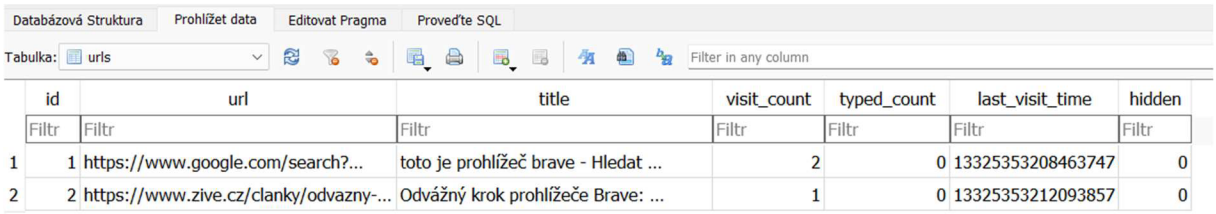
- Adresář C:\Users\[USERNAME]\AppData\Local\Vivaldi\User Data\Default
- Soubor History (bez přípony) ve formátu SQLite.
- Struktura uložených dat stejná jako prohlížeč Google Chrome, jelikož využívá jádro Chromium.

| | id | url | title | visit_count | typed_count | last_visit_time | hidden |
|---|---|---|---|---|---|---|---|
| | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr |
| 1 | 1 | https://vivaldi.com/newfeatures?... | What's new in Vivaldi \| Vivaldi Browser | 1 | 0 | 13325345860444333 | 0 |
| 2 | 2 | https://vivaldi.com/new/ | What's new in Vivaldi \| Vivaldi Browser | 1 | 0 | 13325345860444333 | 0 |
| 3 | 3 | https://vivaldi.com/cs/new/ | What's new in Vivaldi \| Vivaldi Browser | 1 | 0 | 13325345860444333 | 0 |
| 4 | 4 | https://search.yahoo.com/search?... | Yahoo is part of the Yahoo family of ... | 1 | 0 | 13325347323331130 | 0 |
| 5 | 5 | https://guce.yahoo.com/consent?... | Yahoo is part of the Yahoo family of ... | 1 | 0 | 13325347323331130 | 0 |
| 6 | 6 | https://consent.yahoo.com/v2/... | Yahoo is part of the Yahoo family of ... | 1 | 0 | 13325347323331130 | 0 |
| 7 | 7 | https://guce.yahoo.com/copyConsen... | tohle je historie v prohlížeči vivaldi - ... | 1 | 0 | 13325347326675988 | 0 |
| 8 | 8 | https://search.yahoo.com/search?... | tohle je historie v prohlížeči vivaldi - ... | 1 | 0 | 13325347326675988 | 0 |
| 9 | 9 | https://help.vivaldi.com/desktop/... | History \| Vivaldi Browser Help | 1 | 0 | 13325347331345271 | 0 |

*Obrázek 68 - Tabulka urls souboru History v prohlížeči Vivaldi (verze 5.7).*
Zdroj: vlastní

#### 6.2.2.6.2 Brave

- Adresář C:\Users\[USERNAME]\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default
- Soubor History (bez přípony) ve formátu SQLite.
- Struktura uložených dat stejná jako prohlížeč Google Chrome, jelikož využívá jádro Chromium.




| | id | url | title | visit_count | typed_count | last_visit_time | hidden |
|---|---|---|---|---|---|---|---|
| | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr |
| 1 | 1 | https://www.google.com/search?... | toto je prohlížeč brave - Hledat ... | 2 | 0 | 13325353208463747 | 0 |
| 2 | 2 | https://www.zive.cz/clanky/odvazny-... | Odvážný krok prohlížeče Brave: ... | 1 | 0 | 13325353212093857 | 0 |

*Obrázek 69 - Tabulka urls souboru History v prohlížeči Brave (verze 1.50).*
Zdroj: vlastní

#### 6.2.2.6.3 Seznam.cz prohlížeč

- Adresář C:\Users\[USERNAME]\AppData\Local\Seznam.cz\User Data\Default
- Soubor History (bez přípony) ve formátu SQLite.
- Struktura uložených dat stejná jako prohlížeč Google Chrome, jelikož využívá jádro Chromium.
- Odlišností oproti ostatním prohlížečům využívající stejné jádro je to, že do tabulky neukládá titulky webových stránek i když má sloupec vygenerovaný.
- Historii ukládá i dusplicitně s dalšími informacemi s mírně odlišnou strukturou do adresáře C:\Users\[USERNAME]\AppData\Local\Seznam.cz\SznDatabases\history do souboru 5.db, v tomto případě i s titulky webových stránek. Podobným způsobem duplicitně ukládá i cache webových stránek.

Tabulka: urls

Filter in any column

| | id | url | title | visit_count | typed_count | last_visit_time | hidden |
|---|---|---|---|---|---|---|---|
| | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr |
| 1 | 1 | https://notepad-plus-plus.org/... | | 1 | 0 | 13325346619676539 | 0 |
| 2 | 2 | https://notepad-plus-plus.org/... | | 1 | 0 | 13325346619676907 | 0 |
| 3 | 3 | https://www.google.com/search?... | | 2 | 0 | 13325346619677312 | 0 |
| 4 | 4 | https://osdn.net/projects/... | | 1 | 0 | 13325346619677479 | 0 |
| 5 | 5 | https://crystalmark.info/en/software... | | 1 | 0 | 13325346619677676 | 0 |
| 6 | 6 | https://www.google.com/search?... | | 2 | 0 | 13325346619678340 | 0 |
| 7 | 7 | https://www.uhk.cz/ | | 2 | 0 | 13325346619678924 | 0 |
| 8 | 8 | https://search.seznam.cz/?... | | 1 | 0 | 13325353245821692 | 0 |
| 9 | 9 | https://www.cistepc.cz/novy-... | | 1 | 0 | 13325353262124133 | 0 |

*Obrázek 70 - Tabulka urls souboru History v prohlížeči Seznam.cz (verze 6.19).*
Zdroj: vlastní

| | id | url | urlNorm | title | titleNorm | protocol | idDomain | pathname |
|---|---|---|---|---|---|---|---|---|
| | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr | Filtr |
| 1 | 1 | https://notepad-plus-plus.org/... | notepad plus plus org download... | Download Notepad++ v8.5 \| Notepa... | download notepad v8 5 notepad | https: | 1 | /downloads/v8.5/ |
| 2 | 2 | https://notepad-plus-plus.org/... | notepad plus plus org downloads | Downloads \| Notepad++ | downloads notepad | https: | 1 | /downloads/ |
| 3 | 3 | https://www.google.com/search?... | www google com search | notepad++ - Hledat Googlem | notepad hledat googlem | https: | 2 | /search |
| 4 | 4 | https://osdn.net/projects/... | osdn net projects crystaldiskma... | Downloading File /77936/... | downloading file 77936 ... | https: | 3 | /projects/crystaldiskmark/downloads... |
| 5 | 5 | https://crystalmark.info/en/software... | crystalmark info en software ... | CrystalDiskMark - Crystal Dew World ... | crystaldiskmark crystal dew world en | https: | 4 | /en/software/crystaldiskmark/ |
| 6 | 6 | https://www.google.com/search?... | www google com search | crystaldiskmark - Hledat Googlem | crystaldiskmark hledat googlem | https: | 2 | /search |
| 7 | 7 | https://www.uhk.cz/ | www uhk cz | Univerzita Hradec Králové | univerzita hradec kralove | https: | 5 | / |
| 8 | 8 | https://search.seznam.cz/?... | search seznam cz | toto je prohlížeč seznam – Seznam.cz | toto je prohlizec seznam – seznam cz | https: | 6 | / |
| 9 | 9 | https://www.cistepc.cz/novy-... | www cistepc cz novy internetov... | Nový internetový prohlížeč od ... | novy internetovy prohlizec od seznam... | https: | 7 | /novy-internetovy-prohlizec-od-... |

*Obrázek 71 - Tabulka HistoryUrls souboru 5.db v prohlížeči Seznam.cz.*
Zdroj: vlastní

### *6.2.2.6.4 Safari*

- Adresář C:\Users\[USERNAME]\AppData\Local\Apple Computer\Safari\History
- Soubor segments (bez přípony) ve formátu SQLite (ve verzích 3 až 8) (59), nicméně se mi jej nepodařilo otevřít. Je možné, že se jedná o nějaký vlastně upravený formát. Při otevření jako text neobsahuje žádná čitelná data.
- V adresáři ...\Safari\Webpage Previews ukládá ve formátu PNG a JPEG (pro každou webovou stránku vytvoří oba formáty) náhledy načtených webových stránek.
- Náhledy mají rozlišení 496×826 px (JPEG) a 991×1652 px. (PNG).
- Jedná se o poslední verzi pro Windows s datem vydání 20. března 2015.


*Obrázek 72 - Uložený náhled webové stránky v prohlížeči Safari (verze 5.1.7 pro Windows).* Zdroj: vlastní

### 6.2.2.7 Shrnutí analýzy historie webových prohlížečů

Naprostá většina používaných webových prohlížečů ukládá historii prohlížení ve stejném formátu SQLite, který lze načíst různými programy pro správu databázových tabulek, v mém případě například DB Browser for SQLite. Pro jednodušší uživatelské rozhraní je možné použít různé programy, které jsou schopny data zobrazit bez znalostí struktury tabulek a adresářů, kde jsou data uložena, nicméně obvykle v základu neobsahují podporu pro méně používané prohlížeče.

Nepodařilo se mi ale načíst data z prohlížeče Safari pro Windows, nicméně veškeré načtené webové stránky byly ale uloženy i jako náhled ve formátu obrázku.

V každém případě není problém v případě fyzického přístupu k disku a bez šifrování dat poměrně jednoduše data analyzovat v čitelném formátu pro následnou interpretaci v rámci forenzní analýzy.

# 7 Shrnutí výsledků

V praktické části byla provedena forenzní analýza, kterou bylo demonstrováno, jaká data lze získat z disku počítače s nainstalovaným OS Windows verze 10 za využití extrakčních nástrojů a programů. Byly identifikovány důležité informace jako uživatelské účty, nainstalované programy, případy hledání souborů dle parametrů nebo textových řetězců a uložená hesla pro přihlášení do webových služeb.

Ve druhé části praktické části byl podrobněji znázorněn způsob ukládání dat devíti webových prohlížečů jako je Google Chrome, Microsoft Edge, Opera a další s konkrétními příklady na základě získání historie procházení. Důkladné porozumění těmto adresářům a jejich obsahu je klíčové pro úspěšnou forenzní analýzu webových prohlížečů, a tak získání důkazů z počítače.

Celkově tedy byla praktická část zaměřena na ukázku směrů, kam forenzní analýza disku může dále směřovat s podrobnější ukázkou webových prohlížečů s popsáním adresářů a struktury, kde jsou tato data ukládána.

# 8 Závěry a doporučení

Digitální forenzní analýza je velmi rozsáhlý obor, který se zabývá mnoha podobory. Tato práce je zaměřena na úzkou část analýzy, v teoretické části je rozebrán způsob ukládání dat na disková úložiště typu HDD a SSD, jelikož se jedná o nejčastěji využívaný typ úložišť pro počítače, popisuje jejich základní rozdíly a vlastnosti a dále pokračuje do praktické části s ukázkou, která data lze prostřednictvím vybraného programu OSForensics načíst s krátkou ukázkou a popisem získaných dat, následná interpretace a využití v rámci dalšího šetření je poté na konkrétním vyšetřovateli.

Praktická část je dále zaměřena na analýzu způsobu získání dat o historii procházení ve webových prohlížečích, jelikož s obvyklým využíváním počítače jako prostředníka pro procházení internetu mohou poskytnou cenná data. Praktická část se zaměřuje na prohlížeče Google Chrome, Microsoft Edge, Opera, Mozilla Firefox a některé další, které mají menší tržní podíl. Jelikož většina webových prohlížečů využívá jádro Chromium, jsou mezi nimi malé rozdíly. V této části bylo splněno původní ukázkové zadání mimo prohlížeč Safari, kde se nepodařilo získat navštívené odkazy. Mimo prohlížeč Safari byla data uživatelsky čitelná bez nutnosti je dešifrovat nebo jiným způsobem transformovat. Praktickou část práce doplňují video tutoriály s názornou ukázkou práce s daty.

Nicméně je třeba mít na paměti, že dostupnost dat může velmi ovlivnit mnoho faktorů, může tím být nastavení prohlížeče, různé ochranné mechanismy a programy, které mohou data za uživatele mazat nebo šifrování dat, proto je vhodné, aby měl vyšetřovatel rozsáhlé znalosti v dalších aspektech, které mohou vstupní data ovlivnit a následně tak změnit způsob práce s daty.

Případné rozšíření práce by se mohlo zabývat v práci zmíněnými konkrétními sektory analýzy více podrobně, například analýza dat v AmCache nebo v nástroji Prefetcher ve Windows, které mohou poskytnout přehled o používaných programech, případně možnosti získání šifrovaných dat nebo analýza dat z mobilních telefonů.

Digitální forenzní analýza se neustále vyvíjí podobným tempem jako vývoj hardware a software počítačů a z toho důvodu bude do budoucna stále více potřeba dostatek vyšetřovatelů s vyspělými znalostmi a dovednostmi v rámci daného forenzního vyšetřování, kteří budou schopni se přizpůsobit vzniklým situacím a výzvám.

# 9 Seznam použitých zdrojů

1. Klein, Andy. Are SSDs Really More Reliable Than Hard Drives? *The Best Unlimited Online Backup and Cloud Storage Services.* [Online] 30. Září 2021. https://www.backblaze.com/blog/are-ssds-really-more-reliable-than-hard-drives/.

2. Smith, Tyan. Western Digital's Advanced Format: The 4K Sector Transition Begins. *AnandTech: Hardware News and Tech Reviews Since 1997.* [Online] 18. Prosinec 2009. [Citace: 16. Duben 2023.] https://www.anandtech.com/show/2888.

3. LSoft Technologies Inc. Hard Disk Drive Basics - NTFS.com. [Online] 2023. [Citace: 16. Duben 2023.]

4. EDN. Hard disk drive read channels " a must for perpendicular recording. *EDN.com.* [Online] 20. Květen 2004. [Citace: 16. Duben 2023.] https://www.edn.com/hard-disk-drive-read-channels-a-must-for-perpendicular-recording/.

5. ISO/IEC JTC 1 Information Technology. ISO/IEC 9293:1994. *Volume and file structure of disk cartridges for information interchange.* [Online] Listopad 1994. [Citace: 16. Duben 2023.] https://www.iso.org/standard/21273.html.

6. How to recover bad sectors and fix HDD errors. *Recover files deleted from hdd with hard disk drive recovery software.* [Online] 2006. [Citace: 16. Duben 2023.] https://recoverhdd.com/blog/how-to-recover-bad-sectors-and-fix-hdd-errors.html.

7. Bell, Donald. Apple iPod Classic review: The iPod that holds it all. *CNET: Product reviews, advice, how-tos and the latest news.* [Online] 3. Prosinec 2012. [Citace: 16. Duben 2023.] https://www.cnet.com/reviews/apple-ipod-classic-7th-generation-review/.

8. ADRECA. Top 7 Causes Of Hard Disk Failure - My Data Recovery Lab. *My Data Recovery Lab - The Data Recovery eZine.* [Online] 5. Srpen 2015. [Citace: 16. Duben 2023.] https://mydatarecoverylab.com/top-7-causes-of-hard-disk-failure/.

9. Seagate Technology LLC. Hard disk drive reliability and MTBF / AFR. *Support Seagate US. The Leader in Mass Data Storage Solutions | Seagate US.* [Online] [Citace: 16. Duben 2023.] https://www.seagate.com/support/kb/hard-disk-drive-reliability-and-mtbf-afr-174791en/.

10. TechJunkie. How Long Does Backup Media Last? *Tech Junkie.* [Online] [Citace: 16. Duben 2023.] https://www.techjunkie.com/how-long-does-backup-media-last/.

11. Randy, Kenny. How Long Does a Hard Drive Last If Not Used? (Explained) | WhatsaByte. *Whatsabyte: Your Source for Computer Issues & Fixes.* [Online] [Citace: 16. Duben 2023.] https://whatsabyte.com/hard-drive-last-not-used.

12. Olson, Alan a Lanlois J., Denis. Solid State Drives Data Reliability and Lifetime. [Online] 7. Duben 2008. [Citace: 16. Duben 2023.] https://www.researchgate.net/publication/265286222_Solid_State_Drives_Data_Reliability_and_Lifetime.
13. ATP Inc. What is Error detection correction, LDPC, BCH, Reed-Solomon Algorithm? *ATP Electronics. Industrial SSD storage & DRAM memory solutions.* [Online] 6. Červen 2019. [Citace: 16. Duben 2023.] https://www.atpinc.com/blog/ldpc-ssd-low-density-parity-check-ecc-algorithm.
14. Larrivee, Steve. Solid State Drive Primer # 9 - Controller Architecture - Controller Block Diagram. *Industrial Solid State Storage, Flash Memory Storage Devices - Cactus .* [Online] 8. Červen 2015. [Citace: 16. Duben 2023.] https://www.cactus-tech.com/resources/blog/details/solid-state-drive-primer-9-controller-architecture-controller-block-diagram/.
15. Focus Technology Co., Ltd. Image | Made-in-China.com - Manufacturers, Suppliers & Products in China. [Online] [Citace: 16. Duben 2023.] https://image.made-in-china.com/44f3j00aJhtKiVFLbqS/128GB-Internal-M-2-2280-Interface-Ngff-SATA-SSD-Laptop-Solid-State-Drive.jpg.
16. Kingston Technology Europe Co LLP. Difference between SLC, MLC, TLC and 3D NAND in USB flash drives, SSDs and Memory cards - Kingston Technology. [Online] 21. Duben 2021. [Citace: 16. Duben 2023.] https://www.kingston.com/en/blog/pc-performance/difference-between-slc-mlc-tlc-3d-nand.
17. —. KC3000 PCIe 4.0 NVMe M.2 SSD High-performance for desktop and laptop PCs - Kingston Technology. [Online] [Citace: 16. Duben 2023.] https://www.kingston.com/en/ssd/kc3000-nvme-m2-solid-state-drive.
18. Fulltext Media AB. Fastest SSDs in 2023: Best SATA & PCIe SSDs. *GPCB. Gaming PC Builder – Gaming Hardware Reviews & Guides.* [Online] 2023. [Citace: 16. Duben 2023.]
19. Max | Nitemedia s.r.o. SSD a zničení běžným používáním? Možná to jde.... AbcLinuxu.cz. *Linux na stříbrném podnose.* [Online] 24. Květen 2021. [Citace: 16. Duben 2023.] https://www.abclinuxu.cz/blog/Max_Devaine/2021/4/ssd-a-zniceni-beznym-pouzivanim-mozna-to-jde.
20. Sliwa, Carol. What is SSD TRIM? | Definition from TechTarget. *Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget.* [Online] Únor 2018. [Citace: 16. Duben 2023.] https://www.techtarget.com/searchstorage/definition/TRIM.

21. Sliwa, Carol a Sheldon, Robert. What is NAND flash wear-out? *Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget .* [Online] Březen 2022. [Citace: 16. Duben 2023.] https://www.techtarget.com/searchstorage/definition/NAND-flash-wear-out.

22. Datarecovery.com, Inc. SSD Lifespans: How Long Can You Trust Your Solid-State Drive? *Datarecovery.com. Data Recovery Services and Distribution | RAID HDD NAS | Datarecovery.com .* [Online] 27. Červenec 2021. [Citace: 16. Duben 2023.] https://datarecovery.com/rd/ssd-lifespans-how-long-can-you-trust-your-solid-state-drive/.

23. Cox, Alvin. JEDEC SSD Specifications. *JEDEC SSD Standards.* [Online] [Citace: 16. Duben 2023.] https://www.jedec.org/sites/default/files/Alvin_Cox%20%5BCompatibility%20Mode%5D_0.pdf.

24. Paganini, Pierluigi. Flaws in several self-encrypting SSDs allows hackers to decrypt dataSecurity Affairs. *Security Affairs - Read, think, share ... Security is everyone's responsibilitySecurity Affairs.* [Online] 6. Listopad 2018. [Citace: 16. Duben 2023.] https://securityaffairs.co/77735/hacking/self-encrypting-ssds-flaws.html.

25. Meijer, Carlo a Gastel, van Bernard. Self-encrypting deception: weaknesses in the. [Online] 5. Listopad 2018. [Citace: 16. Duben 2023.] https://www.ru.nl/publish/pages/909275/draft-paper_1.pdf.

26. Rajeev, Kumar, a další. Computer Forensic Investigation on Hard Drive Data Recovery. [Online] Září 2016. [Citace: 16. Duben 2023.] https://www.researchgate.net/publication/308171031_Computer_Forensic_Investigation_on_Hard_Drive_Data_Recovery_A_Review_Study.

27. BASIS Technology Corporation. Autopsy | Fast, Thorough, and Efficient Investigations | Datasheet. [Online] 2018. [Citace: 16. Duben 2023.] https://s3.amazonaws.com/resources.autopsy.com/datasheets/Autopsy-EN.pdf.

28. Valich, Theo. Microsoft's new product goes against crime: Meet (Hot) COFEE. [Online] 7. Květen 2008. [Citace: 16. Duben 2023.] https://web.archive.org/web/20080517070103/http://www.tgdaily.com/content/view/37305/108/.

29. Goodin, Dan. Hackers declare war on international forensics tool. *Microsoft's COFEE decaffeinated.* [Online] 14. Prosinec 2009. [Citace: 16. Duben 2023.] https://www.theregister.com/2009/12/14/microsoft_cofee_vs_decaf/.
30. WikiLeaks. Microsoft COFEE (Computer Online Forensics Evidence Extractor) tool and documentation, Sep 2009 - WikiLeaks. [Online] [Citace: 16. Duben 2023.] https://wikileaks.org/wiki/Microsoft_COFEE_(Computer_Online_Forensics_Evidence_Extractor)_tool_and_documentation,_Sep_2009.
31. Ardi, Sam. Komputer Forensik: Computer Online Forensic Evidence Extractor (COFEE). [Online] 16. Září 2009. [Citace: 16. Duben 2023.] https://samardi.wordpress.com/2009/09/16/cofee/.
32. Exterro, Inc. FTK® Forensic Toolkit - Exterro. Exterro - E-Discovery & Information Governance Software. [Online] [Citace: 16. Duben 2023.] https://www.exterro.com/forensic-toolkit.
33. PassMark Software. PassMark OSForensics - Digital investigation. PassMark OSForensics - Digital investigation. [Online] [Citace: 16. Duben 2023.] https://www.osforensics.com/osforensics.html.
34. Oxygen Forensics. Oxygen Forensic® Detective - Oxygen Forensics. [Online] [Citace: 16. Duben 2023.] https://oxygenforensics.com/en/products/oxygen-forensic-detective/.
35. H-11 Digital Forensics. Oxygen Forensic Detective – H-11 Digital Forensics. H-11 Digital Forensics. *Cybersecurity, Mobile Forensics, Incident Response, Digital Forensic Training.* [Online] [Citace: 16. Duben 2023.] https://h11dfs.com/oxygen-forensic-detective/.
36. AION CS, s.r.o. 89/2012 Sb. Občanský zákoník (nový). Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění . [Online] 3. Únor 2012. [Citace: 16. Duben 2023.] https://www.zakonyprolidi.cz/cs/2012-89#cast3.
37. —. 141/1961 Sb. Trestní řád. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění. [Online] 29. Listopad 1961. [Citace: 16. Duben 2023.] https://www.zakonyprolidi.cz/cs/1961-141.
38. JUDr. Souček, Josef, Csc. N320077: Trestní právo . E-learning VŠCHT Praha. [Online] 2015. [Citace: 16. Duben 2023.] https://e-learning.vscht.cz/mod/resource/view.php?id=1562.

39. AION CS, s.r.o. 99/1963 Sb. Občanský soudní řád. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění . [Online] 4. Prosinec 1963. [Citace: 16. Duben 2023.] https://www.zakonyprolidi.cz/cs/1963-99.
40. —. 150/2002 Sb. Soudní řád správní. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění. [Online] 21. Březen 2002. [Citace: 16. Duben 2023.] https://www.zakonyprolidi.cz/cs/2002-150.
41. CRU Data Security Group, LLC. Forensic UltraDock FUDv6.0 | WiebeTech. WiebeTech | Digital Forensics. [Online] [Citace: 16. Duben 2023.] https://wiebetech.com/products/forensic-ultradock-fudv6-0/.
42. National Institute of Standards and Technology. Hardware Write Blocker (HWB) Assertions and Test Plan. [Online] 21. Březen 2005. [Citace: 16. Duben 2023.] https://www.nist.gov/system/files/documents/2017/05/09/hwb-atp-19.pdf.
43. U.S. Department of Homeland Security. Tableau Forensic SATA/IDE Bridge T35u. *Test Results for Hardware Write Block Device - Federated Testing Suite.* [Online] 17. Říjen 2018. [Citace: 16. Duben 2023.] https://www.dhs.gov/sites/default/files/publications/Test%20Report_NIST_HWB_Tableau%20Forensic%20SATA-IDE%20Bridge%20T35u_Firmware%20Version%20Sep%2015%202015%2011.19.41_October%202018.pdf.
44. National Institute of Standards and Technology. Hardware Write Block | NIST. National Institute of Standards and Technology. [Online] 31. Leden 2023. [Citace: 16. Duben 2023.]
45. U.S. Department of Homeland Security. Test Results for Hardware Write Block Device: Coolgear SS-127ASD USB 3.0 to SATA/IDE Adapter with Write-Protection. [Online] Březen 2020. [Citace: 16. Duben 2023.] https://www.dhs.gov/sites/default/files/publications/testresults_for_cool_gear_sata-ide_adapter_windows.pdf.
46. SOFTCOM Group, spol. r. o. IcyBox External enclosure for M.2 NVMe SSD, USB 3.1 Type-C, Grey. [Online] [Citace: 16. Duben 2023.] https://www.softcom.cz/eshop/icybox-external-enclosure-for-m-2-nvme-ssd-usb-3-1-type-c-grey_d227313.html.
47. Distributed Rainbow Table Project. Free Rainbow Tables. [Online] [Citace: 16. Duben 2023.] https://freerainbowtables.com/.

48. Rosulek, Mike. Hash Functions. [Online] 3. Leden 2021. [Citace: 16. Duben 2023.] https://joyofcryptography.com/pdf/chap11.pdf.
49. LSoft Technologies Inc. NTFS Master File Table (MFT) - NTFS.com. [Online] [Citace: 16. Duben 2023.] http://ntfs.com/ntfs-mft.htm.
50. Pittman, D. Ryan a Shaver, Ryan. Handbook of Digital Forensics and Investigation | Chapter 5 - Windows Forensic Analysis. [Online] 2010. [Citace: 16. Duben 2023.] https://www.sciencedirect.com/science/article/pii/B9780123742674000057.
51. Gurkok, Cem. Computer and Information Security Handbook. [Online] 2017. [Citace: 16. Duben 2023.] https://www.sciencedirect.com/science/article/pii/B9780128038437000417.
52. Russinovich, Mark E. a Solomon, David A. *Windows internals.* místo neznámé : Redmond, Wash. : Microsoft Press, 2005.
53. Ummulkulthum, Wambai. Investigating AmCache. [Online] 22. Duben 2022. [Citace: 16. Duben 2023.] https://forensafe.com/blogs/AmCache.html.
54. Count Upon Security. DIGITAL FORENSICS – PLUGX AND ARTIFACTS LEFT BEHIND. [Online] 20. Červen 2018. [Citace: 16. Duben 2023.] https://countuponsecurity.com/tag/amcache/.
55. Apple Inc. Update to the latest version of Safari. *Apple Support. Official Apple Support.* [Online] [Citace: 16. Duben 2023.] https://support.apple.com/en-us/HT204416.
56. Oberlo. Most Popular Web Browsers in 2023. [Online] Únor 2023. [Citace: 16. Duben 2023.] https://www.oberlo.com/statistics/browser-market-share.
57. Wabuge, Daniel. 5 Chromium Based Browsers [With Additional Features]. [Online] 10. Listopad 2022. [Citace: 16. Duben 2023.] https://techjury.net/blog/chromium-based-browsers/#gref.
58. Foxton Software Ltd. Browser History Examiner — User Guide. [Online] [Citace: 16. Duben 2023.] https://www.foxtonforensics.com/browser-history-examiner/chrome-history-location.
59. McLeod, Sally. Apple Safari Analysis - Browser Forensics - Digital Detective Knowledge Base. [Online] 12. Březen 2015. [Citace: 16. Duben 2023.] https://kb.digital-detective.net/display/BF/Apple+Safari+Analysis.
60. Mathawan, Rohan. What Is The Lifespan of a USB Flash Drive? - TechStory. *Everything about tech entrepreneurs , startups, businesses and more!* [Online] 14. Červenec 2020.

[Citace: 16. Duben 2023.] https://techstory.in/what-is-the-lifespan-of-a-usb-flash-drive/.

# 10 Přílohy

Video tutoriály

- Dostupné jako playlist na YouTube.
- https://www.youtube.com/watch?v=eSTyFDxFvzc&list=PLmH3EA29WUHXAJUkRE0SQwFHj8cHO3k7o&pp=gAQB

*Oskenované zadání práce*

Univerzita Hradec Králové
Fakulta informatiky a managementu

# Zadání bakalářské práce

**Autor:** **Jaromír Bobek**

Studium: I1900149

Studijní program: B1802 Aplikovaná informatika

Studijní obor: Aplikovaná informatika

**Název bakalářské práce:** **Forenzní analýza diskových uložišť - video tutoriály**

Název bakalářské práce AJ: Forensic analysis of disk storage - video tutorials

**Cíl, metody, literatura, předpoklady:**

Cílem bakalářské práce je vytvořit podpůrné materiály v oblasti forenzní analýzy v podobě video tutoriálů. V teoretické části autor představí a podrobně popíše postupy a řešení dílčích úloh forenzní analýzy diskových uložišť. V paktické části pak autor vytvoří praktická řešení dílčích úloh ve formě video tutoriálů.

NIKKEL, Bruce. *Practical Linux forensics: a guide for digital investigators.* San Francisco: No Starch Press, [2022]. ISBN 978-1-7185-0196-6

Zadávající pracoviště: Katedra informačních technologií,
Fakulta informatiky a managementu

Vedoucí práce: Ing. Tomáš Svoboda, Ph.D.

Datum zadání závěrečné práce: 15.10.2021