UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
PRÍRODOVEDECKÁ FAKULTA

VPLYV ANTI-FORENZNÝCH TECHNÍK NA DIGITÁLNE FORENZNÉ VYŠETROVANIE

2023 **Zuzana HENNELOVÁ**

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
PRÍRODOVEDECKÁ FAKULTA

VPLYV ANTI-FORENZNÝCH TECHNÍK NA DIGITÁLNE FORENZNÉ VYŠETROVANIE

BAKALÁRSKA PRÁCA

Študijný program:	Informatika
Pracovisko (katedra/ústav):	Ústav informatiky
Vedúci bakalárskej práce:	Mgr. Eva Marková
Konzultant bakalárskej práce:	doc. RNDr. JUDr. Pavol Sokol, PhD.

Gelnica 2023 **Zuzana HENNELOVÁ**

Univerzita P. J. Šafárika v Košiciach
Prírodovedecká fakulta

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Zuzana Hennelová
Študijný program: informatika (jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: Informatika
Typ záverečnej práce: Bakalárska práca
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Vplyv anti-forenzných techník na digitálne forenzné vyšetrovanie

Názov EN: Impact of anti-forensic techniques on digital forensic investigation

Cieľ:
(1) Analýza existujúcich anti-forenzných techník
(2) Porovnanie vplyvu anti-forenzných techník na kvalitu forenzných artefaktova ich atribútov
(3) Otestovanie anti-forenzných techník a vyhodnotenie údajov pred a popoužití techník

Literatúra:
(1) Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations. arXiv preprint arXiv:2103.17028.
(2) Gül, M., & Kugu, E. (2017, September). A survey on anti-forensicstechniques. In 2017 International Artificial Intelligence and Data Processing Symposium (IDAP) (pp. 1-6). IEEE.
(3) Majed, H., Noura, H. N., & Chehab, A. (2020, June). Overview of DigitalForensics and Anti-Forensics Techniques. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.

Vedúci: Mgr. Eva Marková
Konzultant: doc. RNDr. JUDr. Pavol Sokol, PhD.
Oponent: RNDr. PhDr. Peter Pisarčík
Ústav : ÚINF - Ústav informatiky
Riaditeľ ústavu: doc. RNDr. Ondrej Krídlo, PhD.
Spôsob sprístupnenia elektronickej verzie práce: bez obmedzenia

Dátum schválenia: 15.05.2023

Poďakovanie

Týmto ďakujem vedúcej práce Mgr. Eve Markovej za cennú pomoc a podporu pri výskume a písaní, za odborné vedenie a za ochotu odpovedať na množstvo mojich otázok. Ďakujem aj konzultantovi doc. RNDr. JUDr. Pavlovi Sokolovi, PhD. za odborné rady a podporu.

Abstrakt v štátnom jazyku

Anti-forenzné techniky dokážu ovplyvniť forenznú analýzu vo viacerých smeroch. V tejto práci sa preto venujeme ohodnoteniu vplyvov anti-forenzných techník. Najskôr je potrebné pochopiť princíp ich fungovania, a preto sme v rámci splnenia prvého cieľa, analýzy existujúcich techník, popísali 11 rôznych anti-forenzných techník. Následne bolo možné jednotlivé techniky otestovať a sledovať, ako ovplyvňujú jednotlivé artefakty. Aby bolo určenie vplyvov jednotné, v práci sme navrhli tri spôsoby, ako na základe zistených poznatkov určiť výsledný vplyv anti-forenznej techniky. Pozreli sme sa na manuálnu forenznú analýzu, ako aj na automatizáciu hľadania podozrivých artefaktov. Tieto spôsoby sme následne aplikovali na určenie vplyvov vybraných anti-forenzných techník. Pri manuálnej forenznej analýze sme stanovili vplyvy siedmich anti-forenzných techník na dáta, časové pečiatky a logy, a určili sme najvplyvnejšie z nich. Pri automatizovanom hľadaní podozrivých artefaktov sme porovnali nájdené anomálie v neupravených dátach a v dátach s použitím štyroch rôznych anti-forenzných techník. Na základe výsledkov sme stanovili techniky s najväčším a najmenším vplyvom. Porovnania vplyvov môžu mať veľký význam pri oboch formách forenznej analýzy, pretože nie je možné sústrediť sa na všetky existujúce techniky. Je potrebné zvoliť si tie najvplyvnejšie, ktoré môžu vážne ohroziť aktíva a hľadať formy obrany primárne voči nim.

Kľúčové slová: forenzná analýza, artefakty, anti-forenzné techniky, vplyv

Abstrakt v cudzom jazyku

Anti-forensic techniques can impact forensic analysis in multiple ways. This work focuses on evaluating the effects of anti-forensic techniques. To do so, it is necessary to first understand the principles of their functioning. Therefore, as part of achieving the first objective, the analysis of existing techniques, we described 11 different anti-forensic techniques. Subsequently, it was possible to test and observe the effects of individual techniques on various artifacts. To ensure a uniform determination of the impacts, three methods were proposed in this work to assess the resulting impact of an anti-forensic technique based on the findings. We examined both manual forensic analysis and the automation of searching for suspicious artifacts. These methods were then applied to determine the impacts of selected anti-forensic techniques. In the manual forensic analysis, we identified the influences of seven anti-forensic techniques on data, timestamps, and logs, and determined the most influential anti-forensic techniques. In the automated search for suspicious artifacts, we compared the anomalies found in unmodified data with data modified using four different anti-forensic techniques. Based on the results, we determined the techniques with the greatest and least impact. Comparisons of impacts can be highly relevant in both aforementioned forms of forensic analysis, as it is not feasible to focus on all existing techniques. It is necessary to select the most influential ones that can pose a serious threat to assets and primarily seek defense measures against them.

Key words: forensic analysis, artifacts, anti-forensic techniques, impact

Obsah

Zoznam ilustrácií

Zoznam tabuliek

Úvod

S výraznými technologickými pokrokmi vzniká v kybernetickom priestore aj množstvo príležitostí pre útočníkov. Aby bolo možné eliminovať následky vzniknutého bezpečnostného incidentu a zabrániť vzniku ďalších, je potrebné zisťovať kto a akým spôsobom vykonal útok, aké zraniteľnosti zneužil, aké použil príkazy, s akými zariadeniami komunikoval a k akým dátam pristupoval. S cieľom odpovedať na tieto otázky vznikol odbor digitálnej forenznej analýzy, v rámci ktorého dochádza k zaisťovaniu digitálnych stôp, ich spracovaniu, analýze a vyhodnoteniu. Na druhej strane sú však útočníci, ktorí sa častokrát pokúšajú zahladiť za sebou stopy, ktoré zanechali v kompromitovaných systémoch. Za týmto účelom používajú rôzne anti-forenzné techniky na oklamanie rôznych automatizovaných nástrojov používaných na prevenciu či detekciu škodlivej aktivity a na spomalenie a zavádzanie forenzných vyšetrovateľov pri analýze digitálnych stôp.

Anti-forenzné techniky môžu do určitej miery ovplyvniť proces a výsledky forenznej analýzy, a preto je dôležité sa nimi zaoberať. Nie každá technika je rovnako efektívna a práve túto efektivitu, resp. vplyv skúmame v tejto práci. Väčšina výskumov anti-forenzných techník sa totiž zameriava na ich detekciu, no rozhodnutie, či je technika natoľko závažná, aby sa jej detekcia mala zahrnúť do procesov vo forenznej analýze, je ponechané na čitateľovi. Je však časovo nevýhodné riešiť pri každej forenznej analýze to, či nebola niektorá z techník použitá. V súčasnosti totiž existuje množstvo rôznych anti-forenzných techník, a kým niektoré z nich je možné rýchlo odhaliť, iné sú len ťažko detekovateľné. K rozhodovaniu pri výbere z techník by malo dopomôcť práve preskúmanie vplyvu anti-forenzných techník na forenzné vyšetrovanie, čo je jedným z cieľov tejto práce. Výsledky je potom možné vnímať ako odporúčania, na ktoré anti-forenzné techniky je potrebné dávať pozor, a aj keď ich detekcia môže byť náročná, tak má zmysel ju vykonať, pretože následky pri ich nedetegovaní by mohli byť signifikantné.

Literatúra týkajúca sa anti-forenzných techník sa najčastejšie zaoberá popisom, ako dané techniky fungujú (často s použitím konkrétnych nástrojov) a snažia sa poskytnúť čitateľovi istú formu mitigácie. Chýbajú však práce zaoberajúce sa vplyvom anti-forenzných techník na artefakty či forenzné vyšetrovanie. Nepodarilo sa nám nájsť relevantnú literatúru, v ktorej by boli vyhodnocované vplyvy anti-forenzných techník na

forenznú analýzu, iba zdroje popisujúce to, ktoré artefakty technika ovplyvní a akým spôsobom.

V rámci práce popíšeme nami navrhnuté spôsoby jednotného ohodnotenia, ktoré bude možné aplikovať na všetky existujúce, ale aj ešte nevymyslené anti-forenzné techniky. Takéto popísanie vplyvov anti-forenzných techník na forenzné vyšetrovanie by mohlo byť nápomocné pri manuálnej forenznej analýze, ako aj pri jej automatizácii. Vzhľadom na nárast anti-forenzných techník bude taktiež potrebné zahrnúť identifikáciu a ošetrenie anti-forenzných techník do postupov a procesov. Prihliadať by sa mohlo práve na vplyvy jednotlivých techník, keďže nie je možné zohľadňovať všetky techniky.

V práci uvádzame vlastné testovanie vybraných anti-forenzných techník (keďže nie všetky nástroje a spísané postupy musia byť funkčné či efektívne) a rozoberáme ovplyvnené artefakty. Zaoberáme sa aj vplyvom techník pri automatizácii, a to aplikáciou anti-forenzných techník na už zaistené a predspracované dáta, ktoré je možné použiť na automatizované vyhľadávanie anomálií (t.j. záznamov v dátach, ktoré môžu byť z pohľadu forenznej analýzy zaujímavé).

1 Úvod do digitálnej forenznej analýzy

Digitálna forenzná analýza (ďalej len forenzná analýza) sa zaoberá identifikáciou relevantných zdrojov digitálnych stôp, ich korektnou extrakciou, analýzou a interpretáciou výsledkov (Alazab et al., 2009). Cieľom forenznej analýzy je identifikovať neželané udalosti a ich vplyv na systémy, zaistiť všetky relevantné dôkazy v súlade so zákonom a zistiť akým spôsobom došlo k týmto neželaným udalostiam, aby bolo možné im zabrániť alebo znížiť ich výskyt.

Pre proces forenznej analýzy je dôležité dbať na tzv. auditovateľnosť (nezávislá kontrola dodržania predpísaných postupov), opakovateľnosť, reprodukovateľnosť a opodstatnenosť všetkých aktivít (Montasari, 2016).

Rozlišujeme viacero typov forenznej analýzy (podľa typu a zdroja dát): počítačová forenzná analýza, sieťová forenzná analýza, forenzná analýza mobilných zariadení, forenzná analýza škodlivého kódu, forenzná analýza vzdialeného úložiska, forenzná analýza pamäte, forenzná analýza e-mailov a iné (Yaacoub et al., 2021). V tejto práci sa zameriavame na počítačovú forenznú analýzu, konkrétne na počítače s operačným systémom Windows 10, ktorý využíva súborový systém NTFS.

1.1 Modely forenznej analýzy

Forenzná analýza je viacstupňový proces, ktorý zahŕňa množstvo úkonov a existuje viacero rôznych modelov, ktoré popisujú jednotlivé fázy procesu. Modely sa líšia počtom fáz, terminológiou, komplexnosťou či použiteľnosťou v praxi (Montasari, 2016), ako je možné vidieť pri dvoch nižšie popísaných modeloch. Ich diverzita vyplýva z rôznorodosti potrieb pri praktickej forenznej analýze rôznych zariadení a rôznych incidentov, ale aj z potreby popísať celý proces formálne. Vždy je však základnom celej forenznej analýzy **zaistenie** a **uchovanie** dát, ich **skúmanie**, **analýza** a následná **interpretácia** výsledkov. Fázy súvisiace s identifikáciou digitálnych stôp na potenciálnom mieste činu vynecháme – pracovať budeme iba s obrazom disku virtuálneho stroja (analyzovať ho a interpretovať výsledky).

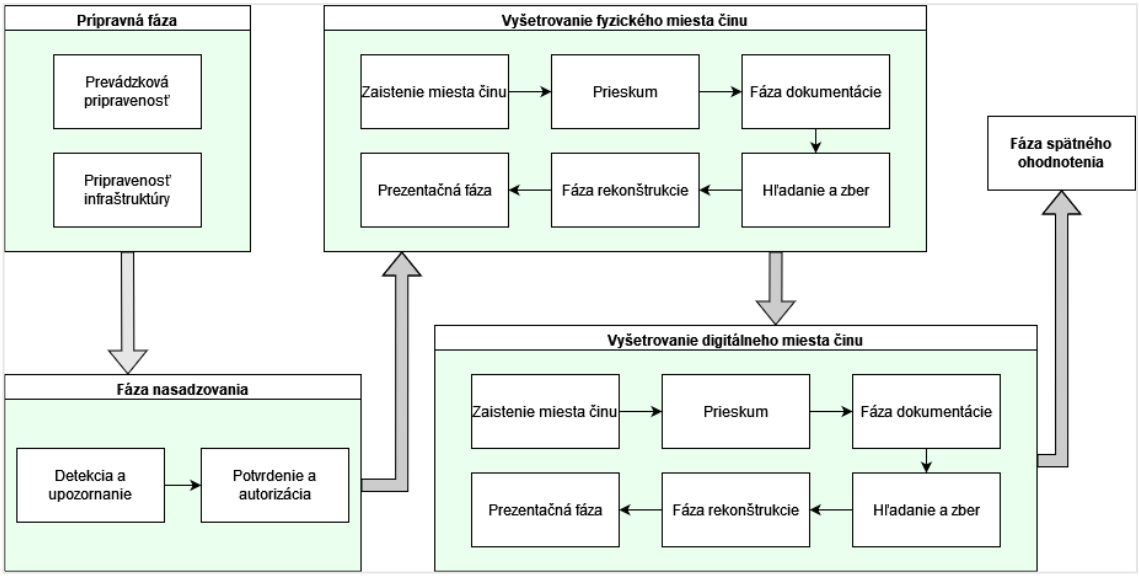
Abstraktný model

Tento model pozostáva z deviatich fáz. Prvou fázou je *identifikácia*, teda zistenie, že došlo k bezpečnostnému incidentu. Potom nasleduje *príprava* (potrebných nástrojov,

povolení, softvéru) a určenie *stratégie prístupu* pre zaistenie dôkazov. Potom prichádza *zachovanie* miesta činu a samotný *zber* dôkazov. Dôkazy sú skúmané vo fáze *vyšetrovania* a výsledky sa podrobujú *analýze*. Fáza analýzy zahŕňa rekonštrukciu dát, určovanie dôležitosti či formuláciu záverov. Nakoniec sa vo fáze *prezentácie* zhrnú a odôvodnia výsledky a môže nasledovať aj fáza *vrátenia dôkazov* vlastníkovi, ak boli zaistené fyzické dôkazy. (Kaur, Kaur, 2012)

Integrovaný model digitálneho vyšetrovania

Integrovaný model pozostáva z piatich fáz, ktoré majú vlastné vnútorné delenie (Obrázok 1). Niektoré z vnútorných fáz môžu byť vykonávané paralelne (prevádzková pripravenosť a pripravenosť infraštruktúry), niektoré môžu byť vynechané vzhľadom na charakter incidentu.



Obrázok 1: Integrovaný model digitálneho vyšetrovania

Prípravná fáza zabezpečuje *pripravenosť prevádzky a infraštruktúry* na vyšetrovanie. Potom nasleduje *fáza nasadzovania*, kde sa najprv deteguje incident a upozornia sa príslušné oddelenia/ľudia. Tí potom overia a potvrdia (resp. vyvrátia) vznik incidentu a získajú potrebné povolenia na ďalšie vyšetrovanie.

Potom dochádza k samotnému *vyšetrovaniu fyzického a digitálneho miesta činu*. Obe tieto fázy majú rovnaké vnútorné členenie, teda najprv sa zaistí miesto činu – zaznamená sa neporušený stav. Vo fáze prieskumu sa potom zabezpečujú prvé fyzické/digitálne stopy a celý proces ich zberu sa dokumentuje (fáza dokumentácie teda nasleduje po nájdení každej stopy).

V ďalšej fáze dochádza k podrobnejšiemu hľadaniu a zberu stôp. Pri fyzických stopách je to dôslednejšie prehľadanie miesta činu, pri digitálnych stopách je to použitie ďalšieho softvéru napr. na zotavenie vymazaných dát. Vo *fázach rekonštrukcie* sa potom jednotlivé dôkazy vyhodnocujú a zostavuje sa priebeh incidentu.

Výsledky sú následne prezentované v *prezentačnej fáze*. Po uzavretí incidentu nasleduje *fáza spätného ohodnotenia*, kde sú spätne prehodnotené vykonané kroky, postupy s cieľom identifikovať problémové miesta a navrhnúť zlepšenia pre ďalšie vyšetrovanie. (Kaur, Kaur, 2012)

1.2 Výzvy vo forenznej analýze

Forenzná analýza sa stretáva s viacerými výzvami, ktoré môžu ovplyvniť jej procesy. Patria tu **technické výzvy** ako šifrovanie dát, príliš veľké množstvo dát, či použitie anti-forenzných techník, čo môže viesť k mareniu alebo predĺženiu vyšetrovania, resp. k extrémnemu vyťaženiu zdrojov.

Ďalej sú to napr. **prevádzkové výzvy**, ku ktorým patrí nedostatočná prevencia a slabá detekcia vzniku incidentov, ale aj nedostatočné nastavenie procesov a nedostatočná príprava na vykonanie zberu digitálnych dát. Výzvou je aj **právna** stránka celého procesu, pretože je potrebné právne zabezpečiť napr. prístup k zbieraným digitálnym stopám ale hlavne mať v zákonoch podchytené trestné činy v digitálnom priestore. Forenzná analýza sa stretáva aj s **investigatívnymi výzvami**, ktoré súvisia s nedostatkom skúseností a vedomostí forenzných analytikov, s ich celkovým nedostatkom na trhu práce ale aj s nepostačujúcimi nástrojmi. (Yaacoub et al., 2021)

V *Challenges in digital forensics* (2016) sú medzi výzvami pre forenznú analýzu spomenuté aj výzvy analýzy rôznorodých zariadení, popularity využívania cloudov, či zachovanie súkromia používateľov.

2 Forenzné artefakty

Kým digitálny dôkaz je akákoľvek informácia uložená alebo prenášaná v binárnej podobe (Jansen, Ayers, 2004), forenzný artefakt (ďalej iba artefakt) je digitálna informácia, ktorá vypovedá o udalostiach, ktoré sa odohrali v minulosti (Forensics Wiki, n.d.). V procese forenznej analýzy slúžia artefakty na potvrdenie prítomnosti škodlivej aktivity (ale nie na jej vyvrátenie).

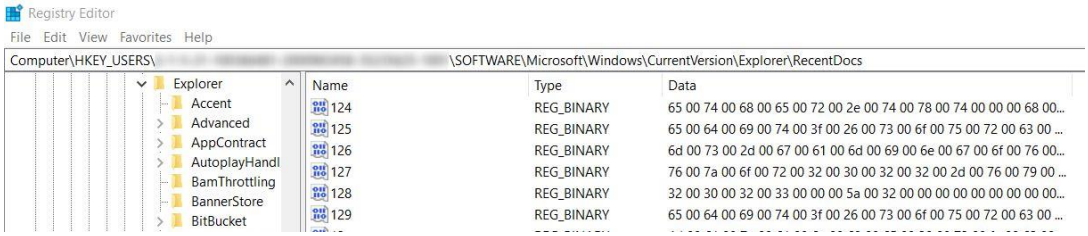
2.1 Súbory

Operačný systém Windows ukladá informácie o súboroch na rôznych miestach. Najčastejšie je odtiaľ možné získať metadáta (aj vymazaných) súborov ale aj samotný obsah, či aspoň miniatúru (viď. thumbnails).

Office Recent Files sú nedávno otvorené MS Office súbory, ktoré sú zaznamenávané aplikáciami MS Office ako súčasť funkcionality rýchleho prístupu pre používateľov. Zoznam týchto súborov sa nachádza v registri NTUSER.DAT\Software\Microsoft\Office\VERSION.

Prefetch súbory sa nachádzajú v priečinku C:\Windows\Prefetch a slúžia na zrýchlenie načítavania často používaných aplikácií. Tieto súbory obsahujú informácie o počte spustení aplikácií a čas posledného spustenia. Systém môže mať vytváranie prefetch súborov zakázané, povolené iba pre aplikácie, povolené iba pre štartovanie systému (booting) a povolené pre aplikácie aj booting. Tieto nastavenia je možné nájsť v registroch. (EC-Council ,2021)

Recent files sú záznamy o naposledy otvorených či modifikovaných súboroch. Záznamy sa nachádzajú v registri NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs (obrázok č. 2) a čas poslednej úpravy daného kľúča je aj časom úpravy prislúchajúceho súboru.

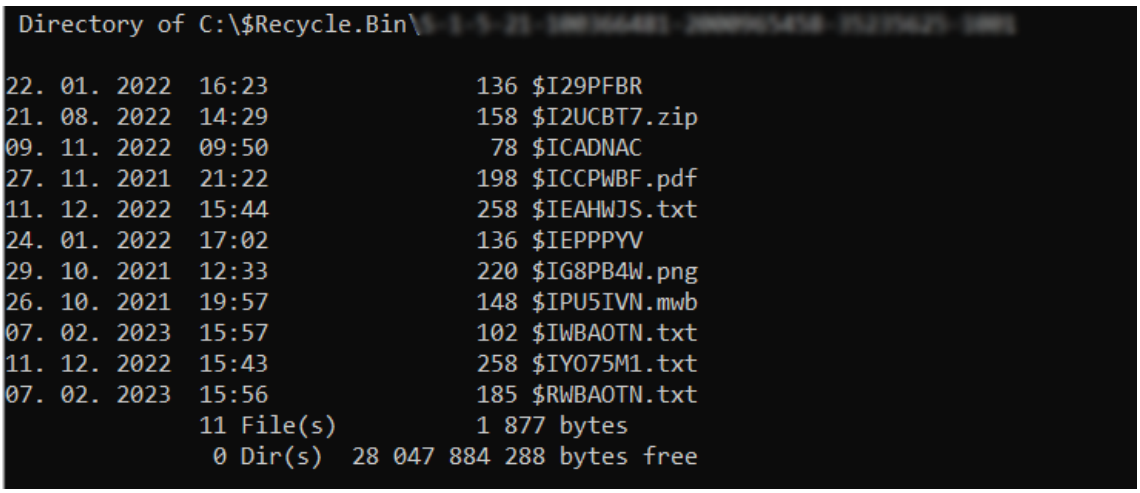


Obrázok 2: Nedávne súbory

Recycle Bin, teda odpadkový kôš je miesto, kde končia všetky súbory, ktoré sú odstránené „klasickým“ spôsobom – kliknutím na možnosť *Odstrániť*. Cesta k priečinku je C:\$Recycle.Bin\SID, kde SID je bezpečnostný identifikátor používateľa.

Pre každý odstránený súbor sú do koša pridané 2 položky, jedna začína znakom $I a obsahuje metadáta odstráneného súboru, druhá začína znakom $R a nesie v sebe samotný obsah. Zvyšok názvu je tvorený 6 náhodnými znakmi (písmenami a číslicami), za ktorými je pôvodná prípona súboru. (Senator Patrick Leahy Center for Digital Investigation 2015). Iba súbory, ktoré majú zachované svoje $R aj $I súbory (dáta aj metadáta) sú priamo viditeľné v koši a obnoviteľné.

Na obrázku č. 3 je obsah priečinku koša. Kôš bol vysypaný a následne bol dňa 07.02.2023 vymazaný jeden textový súbor. Tento jediný súbor je teda možné z koša obnoviť, keďže má uložené svoje dáta aj metadáta (na obrázku súbory $RWBAOTN.txt a $IWBAOTN.txt).



Obrázok 3: Obsah odpadkového koša

Príkazom napr. „type <názov súboru>.<prípona>“ je možné do konzoly priamo vypísať obsah súborov či metadáta. Použitím príkazu „copy <názov súboru>.<prípona> <cieľový priečinok>“ môžeme skopírovať obsah súborov začínajúcich na $R do priečinka – priradiť im cestu v súborovom systéme, kde si už dané súbory môžeme otvoriť (aj keď sú ich metadáta vymazané a teda nie je možné súbory priamo obnoviť z koša).

LNK (linkové) súbory resp. odkazy sú primárne ukladané v priečinku C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent a odkazy pre Office

súbory aj v priečinku C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Office\ Recent ale môžu sa nachádzať aj na rôznych iných miestach. Čas, ktorý sa pri linkových súboroch zobrazuje je vlastne časom prvého otvorenia súboru (kedy LNK súbor vzniká). Čas poslednej modifikácie odkazu je čas posledného otvorenia súboru. Odkaz obsahuje napr. aj cestu k súboru a jeho veľkosť. Tieto odkazy sa nezanikajú spolu so zánikom (vymazaním, premiestnením) súboru a preto môžu byť pri vyšetrovaní dôležité.(Hassan, 2019)

Thumbnails sú miniatúry súborov (obrázky, dokumenty), ktoré sa vo verzii Windows 10 vytvárajú automaticky pre každý súbor a zachovávajú sa aj po vymazaní samotného súboru. Sú umiestnené v databázových súboroch (prípona DB) v priečinku C:\Users\<USERNAME>\AppData\Local\Microsoft\Windows\Explorer. (Senator Patrick Leahy Center for Digital Investigation, 2015)

2.2 Metadáta

Metadáta sú dáta o dátach – údaje popisujúce jednotlivé súbory, priečinky, či aplikácie. Najbežnejšie metadáta sú napr. veľkosť súboru, názov, umiestnenie, dátum poslednej úpravy či vytvorenia a povolenia na čítanie a zapisovanie. Môže to však byť aj názov používateľa, ktorý vytvoril súbor, kategórie, verzie, typ súboru a ďalšie.

Časové pečiatky (MACB)

Časové pečiatky patria k najdôležitejším metadátam pre forenznú analýzu, pretože pomáhajú pri filtrovaní dát a vytváraní celkového obrazu o časovej postupnosti udalostí (počas útoku).

Rozlišujeme štyri časové pečiatky nazývané MACB. MACB je skratkou pre Modified, Accessed, Changed a Birth, teda časová pečiatka *M* zaznamenáva čas poslednej modifikácie súboru, *A* zaznamenáva čas posledného pristúpenia k súboru. Tieto dve pečiatky sú často rovnaké. Pečiatka *C* hovorí o poslednej zmene v Master File Tabuľke (MFT). Pečiatka *B* uchováva čas vzniku súboru. (Mohamed, Khalid, 2021). V tabuľke 1 uvádzame, ako základné operácie so súborom aktualizujú jednotlivé časové pečiatky.

	Modified	Accessed	Changed	Born
Upravený súbor	✓		✓	
Prístup k súboru		✓		
Premiestnenie súboru			✓	
Vytvorenie súboru	✓	✓	✓	✓

Tabuľka 1: Aktualizácia časovej pečiatky

Master File Tabuľka (MFT)

MFT je databáza všetkých priečinkov a súborov v súborovom systéme. Slúži na udržiavanie metadát spolu s umiestnením dát na disku. Metadáta v MFT zahŕňajú informácie o rodičovskom priečinku, veľkosti dát a i. Vzhľadom na časové pečiatky je však najdôležitejšie to, že obsahuje až 2 typy časových pečiatok pre daný súbor/priečinok.

Jeden typ sú pečiatky v tzv. štandardných informáciách *(Standard Information,* ozn. SI alebo 0x10), ktoré udržiavajú metadáta, ktoré bežne vidí používateľ napr. pri prezeraní podrobností súboru. Druhý typ časových pečiatok sa nachádza v atribúte *File Name* (ozn. FN alebo 0x30), ktorý okrem názvu obsahuje časové pečiatky, ktoré sa aktualizujú iba pri zmene iného údaja spadajúceho do FN, napr. pri premiestnení alebo premenovaní súboru. (Palmbach, Breitinger, 2020). Tento typ časových pečiatok je často označovaný aj ako *systémové časové pečiatky* a sú ťažšie manipulovateľné, pretože má k nim prístup iba jadro operačného systému.

MFT nie je priamou súčasťou súborového systému (nachádza sa spravidla na začiatku partície) a nie je možné si ju zobraziť. Je však možné ju extrahovať napr. pomocou nástroja KAPE a exportovať do formátu CSV.

Denník (Journal)

Denník je formou logovacieho súboru v NTFS, do ktorého sa zaznamenávajú zmeny vykonané na súboroch. Z denníka tak vieme vyčítať čas modifikácie súboru a najmä typ modifikácie (úprava metadát, obsahu, premiestnenie). Je súčasťou MFT tabuľky, konkrétne sa nachádza v premennej *$Extend.* V *$Extend* je uložený súbor, uchovávajúci samotné záznamy denníka: *$USNjrnl: $J,* aj súbor *$USNjrnl: $Max,* v ktorom sú všeobecné informácie o denníku, ako maximálna veľkosť denníka.

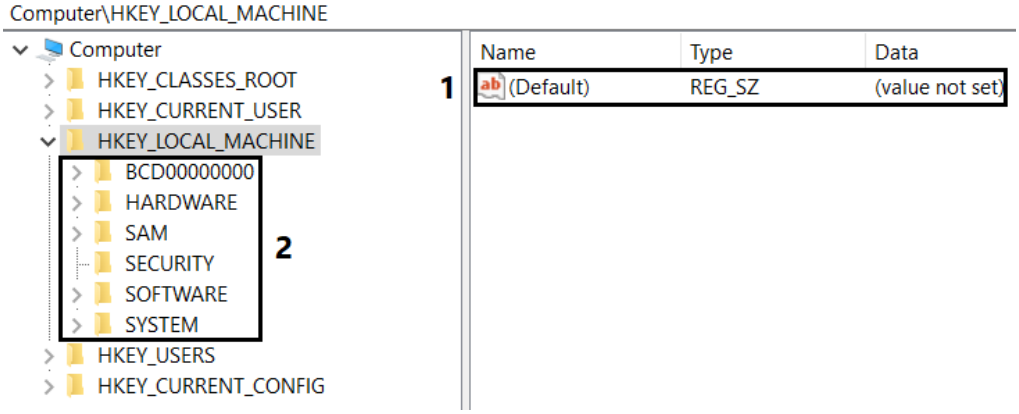
Na rozdiel od MFT tabuľky, s údajmi z denníka vieme pracovať cez príkazový riadok - pomocou príkazu *fsutil usn*. Príkaz umožňuje zobraziť základné informácie, vypísať záznamy ale aj vytvoriť, či vymazať denník (vymazanie generuje logovanú udalosť s ID 3079). (Palmbach, Breitinger, 2020). Na zobrazovanie dát je však omnoho prehľadnejšie použiť nástroj na extrahovanie a exportovanie, podobne ako pri MFT tabuľke.

2.3 Registre

Vo Windows registroch sa štruktúrovane ukladajú rôzne systémové a používateľské nastavenia operačného systému či aplikácií (Perlman, 2022). Samotný register obsahuje 5 hlavných priečinkov, tzv. kľúčov (často nazývaných aj Hives):

- HKEY_CLASSES_ROOT (ozn. HKCR) – informácie o softvéri a používateľskom prostredí,
- HKEY_CURRENT_USER (ozn. HKCU) – nastavenia aktuálne prihláseného používateľa,
- HKEY_LOCAL_MACHINE (ozn. HKLM) – informácie o hardvéri zariadenia,
- HKEY_USERS (ozn. HKU) - konfigurácie všetkých používateľov,
- HKEY_CURRENT_CONFIG (ozn. HKCC) – momentálne systémové nastavenia. (Singh et al., 2018).

Každý kľúč môže obsahovať hodnoty (obrázok č. 4, označenie 1). aj ďalšie kľúče (obrázok.. číslo 2), tzv. podkľúče. Podkľúče ďalej rozvetvujú štruktúru registra, kým hodnoty už obsahujú konkrétne nastavenia či informácie.



Obrázok 4: Štruktúra registra

Najvýznamnejšie podkľúče sú SYSTEM, SOFTWARE, SECURITY, SAM a HARDWARE. SYSTEM a SOFTWARE obsahujú konfigurácie ovládačov, služieb a aplikácií. Podkľúč SAM drží informácie o manažérovi bezpečnostných účtov (Security Accounts Manager), SECURITY obsahuje bezpečnostné nastavenia systému a siete. Obe tieto kľúče sú pre bežných používateľov neprístupné. HARDWARE obsahuje informácie o externých zariadeniach, ktoré boli od posledného spustenia zariadenia pripojené. (Forensic Focus, 2019).

2.4 Logy

Logy sú záznamy, ktoré vytvára operačný systém pri dôležitých udalostiach (prihlásenia, spustenia programov, príkazového riadku, inštalácie a iné), ktoré nastali v systéme, aplikáciách alebo iných službách. Logy dokážu poslúžiť administrátorom, vývojárom aj forenzným analytikom. Pri riešení bezpečnostného incidentu je možné v logoch vidieť, čo predchádzalo útoku a ako asi útok prebiehal. (Hassan, 2019). Samotný proces vytvárania logov sa nazýva *logovanie*.

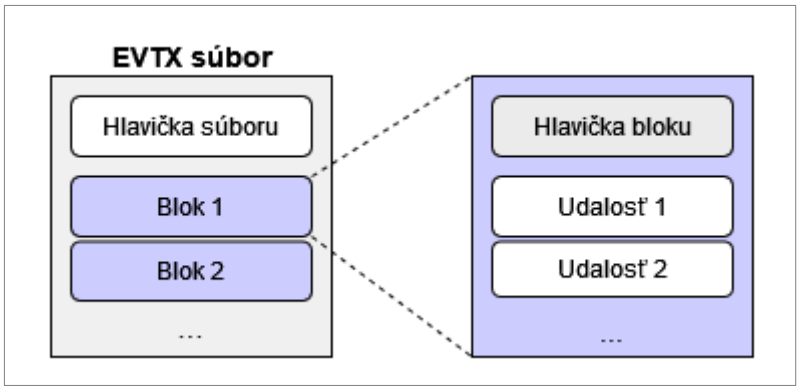
Windows Event Logy

V operačnom systéme Windows 10 sa využívajú tzv. EVTX logy, teda event logy vo formáte XML. Štandardne sú tieto logy uložené v priečinku C:\Windows\System32\winevt\Logs a za ich zaznamenávanie zodpovedá služba s názvom EventLog. Každý log má svoj unikátny identifikátor. Ďalej obsahuje čas zaznamenania udalosti, ID a typ udalosti, zdroj udalosti, používateľa a ďalšie podrobnosti.

Logy sú organizované podľa ich významu do EVTX súborov. K najdôležitejším EVTX súborom patria aplikačné (Application), systémové (System) a bezpečnostné (Security). Aplikačné logy súvisia s nainštalovanými aplikáciami a ich udalosťami, systémové sa týkajú zmien hardvéru, ovládačov a systémových činností. Bezpečnostné logy zachytávajú prihlásenia do zariadenia a ďalšie udalosti súvisiace so zabezpečením.

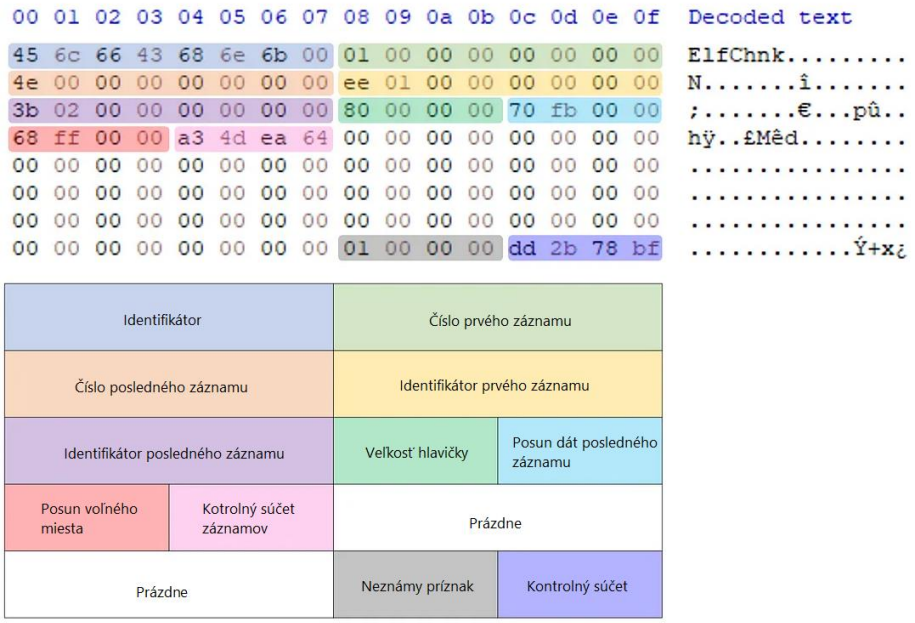
Štruktúra EVTX súboru

Každý EVTX súbor je tvorený hlavičkou samotného súboru a aspoň jedným blokom dát (chunk). Každý blok má svoju vlastnú hlavičku a dáta náležiace jednotlivým logovaným udalostiam (obrázok 5), ktoré sú tiež štruktúrované. Hlavička súboru má 4096 bajtov, obsahuje identifikátor začiatku súboru (ElfFile), informácie o prvom a poslednom bloku, kontrolný súčet a ďalšie, menej významné informácie.



Obrázok 6: Štruktúra EVTX súboru

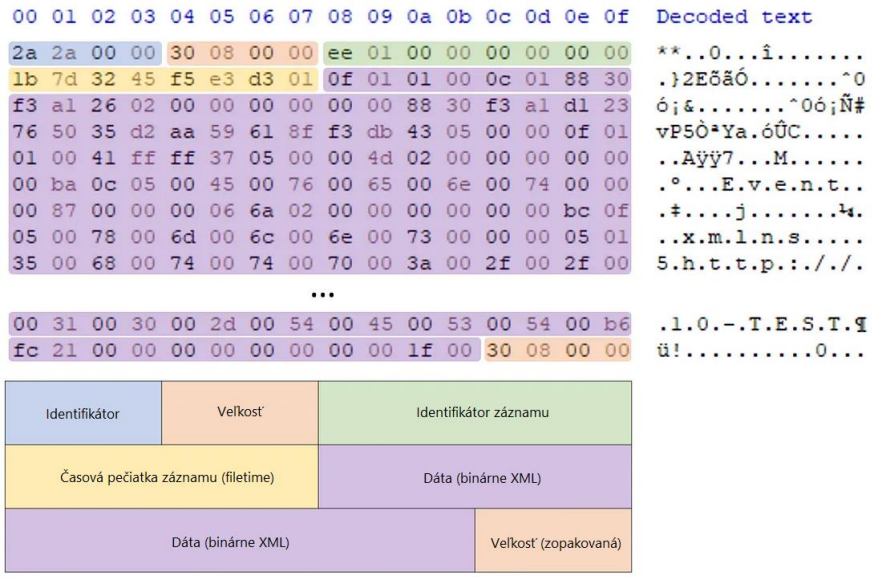
Každý blok začína identifikátorom bloku (ElfChnk). V hlavičke bloku sú ďalej informácie o prvom a poslednom zázname pre daný blok či veľkosť hlavičky a až dva kontrolné súčty (obrázok 6). *Kontrolný súčet dát* je počítaný ako CRC32 všetkých udalostí patriacich do daného bloku, *kontrolný súčet hlavičky* sa počíta ako CRC32 celej hlavičky, okrem bajtov 120 až128, kde sa nachádza počítaný kontrolný súčet. (Xu et al., 2018).



Obrázok 5: Štruktúra záznamu (svch0st, 2020)

Samotný log začína identifikátorom ** a veľkosťou logu a končí sa zopakovaním veľkosti. Samotný obsah logu je písaný vo formáte binárneho

XML. (Xu et al., 2018). Každý log má svoj vlastný identifikátor a časovú pečiatku zaznamenania udalosti (obrázok 7).



Obrázok 7: Štruktúra EVTX bloku (svch0st, 2020)

3 Anti-forenzné techniky

Po vzniku digitálnej forenznej analýzy útočníci vyvinuli anti-forenzné techniky, aby sa dokázali rôznymi spôsobmi brániť voči nástrojom a postupom používaným vo forenznej analýze. Tie cielia na zistenie príčin, ktoré umožnili vykonanie útoku a prípadne aj na získanie dostatočných dôkazov použiteľných na súdnom konaní.

Anti-forenzné techniky sú rôzne postupy aplikovateľné na digitálne dáta či hardvér, na ktorom sú dáta umiestnené. K ich hlavným cieľom patrí: vyhnutie sa detekcii udalosti, narušenie procesu zhromažďovania informácií, predĺženie doby vyšetrovania incidentu a spochybnenie výsledkov forenznej analýzy (Liu, Brown, 2006).

V literatúrach sa vyskytujú odlišné kategorizácie anti-forenzných techník. Príkladom je článok *A survey on anti-forensics techniques* (2017), kde sa rozlišuje až 6 hlavných kategórií, a navrhujú sa odporúčania na mitigáciu techník. My budeme vychádzať z kategorizácie uvedenej v *Overview of Digital Forensics and Anti-Forensics* (2020). V ňom autori rozlišujú 4 kategórie a popisujú princípy fungovania vybraných anti-forenzných techník.

Z hľadiska spôsobu manipulácie s dátami (vrátane artefaktov) budeme rozlišovať kategórie mazania, ukrývania, obfuskácie a zmeny dát. Špeciálnou kategóriou sú útoky voči forenzným technikám a nástrojom, ktorých hlavným cieľom nie je manipulovať dáta.

Dostupná literatúra sa zaoberá prevažne detekciou anti-forenzných techník. V článku *Detection and Mitigation of Anti-Forensics* (2020) je popis vybraných anti-forenzných techník spolu s odporúčaniami na ich mitigáciu. *Anti-forensics techniques: An analytical review* (2014) je zameraný najmä na dostupné nástroje, pomocou ktorých sa anti-forenzné techniky vykonávajú.

Snahy o popísanie konkrétnych vplyvov anti-forenzných techník sú uvedené v *A Conceptual Framework for Database Anti-forensics Impact Mitigation* (2020), avšak práca je zameraná iba na forenznú analýzu databáz a poskytuje iba všeobecné odporúčania ako je zlepšenie pripravenosti na analýzu databáz. Článok *Forensic exploration on windows File History* (2021) sa venuje vplyvu anti-forenzných techník, ktoré môže nechcene vykonať používateľ. Jednotné popísanie a porovnanie vplyvov na manuálnu ani automatizovanú forenznú analýzu však nie sú priamo popisované.

V tabuľke č. 2 uvádzame vyznačené anti-forenzné techniky, ktorými sa zaoberajú jednotlivé zdroje. Techniky, ktoré skúmame v tejto práci, sú popísané v nasledujúcich podkapitolách. Vybrané techniky spadajú do kategórie mazania, ukrývania aj obfuskácie a zmeny dát.

Zdroj/Technika	**Timestomping**	**Šifrovanie**	**Steganografia**	**Falošné stopy**	**Ukrývanie v ADS**	**Ukrývanie v slack space**	**Manipulácia logov**	**Mazanie súborov**	**Deštrukcia disku**
A survey on anti-forensics techniques (2017)	✓			✓					
Anti-forensics techniques: An analytical review (2014)	✓		✓		✓	✓		✓	
Computer anti-forensics methods and their impact on computer forensic investigation (2009)	✓	✓	✓			✓		✓	
Data Hiding Under Windows OS File Structure (2017)					✓	✓			
Detection and Mitigation of Anti-Forensics (2020)		✓	✓			✓		✓	✓
Overview of Digital Forensics and Anti-Forensics Techniques (2020)	✓	✓	✓				✓	✓	

Tabuľka 2: Prehľad anti-forenzných techník v literatúre

Podrobnejšie sa v práci venujeme mazaniu a šifrovaniu súborov a šifrovaniu disku, keďže sú to veľmi často používané techniky. Ďalej sa venujeme ukrývaniu v ADS, čo síce nie je až tak bežná technika, ale je veľmi jednoducho použiteľná. Steganografiu ani deštrukciu disku sme netestovali, pretože v nami zvolenom postupe nie sú tieto techniky aplikovateľné. Bližšie sa však venujeme mazaniu logov, ktoré sú základom pri analýze mnohých bezpečnostných incidentov. Detailnejšie sa zaoberáme aj vytváraniu falošných stôp, ktoré môžu ovplyvniť výsledky forenznej analýzy, či predĺžiť čas potrebný na analýzu.

3.1 Mazanie

Mazanie patrí k najčastejšie používaným technikám. Spočíva v bezpečnom odstránení požadovaných dát (súbory, logy, nastavenia, história a pod.). Pri správnom vymazaní je výhodou, že dané dáta už nebude možné získať, avšak môže to v systéme zanechať stopy po mazaní. Tieto stopy indikujú, že sa v systéme pravdepodobne dialo niečo podozrivé a je potrebné to preskúmať podrobnejšie.

3.1.1 Mazanie súborov

Technika mazania súborov patrí k najprirodzenejším spôsobom, ako odstrániť zo systému stopy po útoku. V prípade bežného odstránenia súboru, je daný súbor premiestnený do koša, odkiaľ je možné súbor obnoviť. V súborovom systéme sa takéto odstránenie prejavuje tým, že miesta v pamäti, kde bol súbor uložený sa označia ako nealokované. Samotné dáta súboru však ostávajú v pamäti, kým nie sú prepísané. Takéto dáta je potom možné vyextrahovať z pamäte, a to aj v prípade, keď súbory odstránime z koša.

Za účelom bezpečného odstránenia súborov boli vyvinuté viaceré nástroje (výber niektorých z nich uvádzame v tabuľke č. 3). Prítomnosť takýchto nástrojov v zariadení však nemusí znamenať aktivitu útočníka. Tieto nástroje totiž môžu byť používané v bežnom živote, napr. pri práci s citlivými, dôvernými údajmi, ktoré je potrebné zlikvidovať podľa stanovených štandardov. Operačný systém Windows neponúka štandardné metódy odporúčané na odstraňovanie citlivých dát ako sú DoD či Gutmann.

Nástroj	Dostupnosť	Najnovšie vydanie	Poznámky	Odkazy
BitKiller	zdarma	2015	jednoduché použitie, 5 módov	sourceforge.net
CBL Data Shredder	zdarma	neznáme	vyžaduje e-mailovú adresu	cbldatarecovery.com
DP Secure Wiper	zdarma	2008		softpedia.com
Eraser	zdarma	2021	13 módov, menej intuitívne	eraser.heidi.ie
Hardwipe	zdarma	2022	pochybný inštalačný súbor	hardwipe.en.softonic.com
Remo File	zdarma/pro	neznáme	neplatená verzia	remosoftware.com

Eraser	verzia		nepodporuje Gutmann metódu	
Sdelete	zdarma	2020	súčasť Windows Sysinternals	learn.microsoft.com

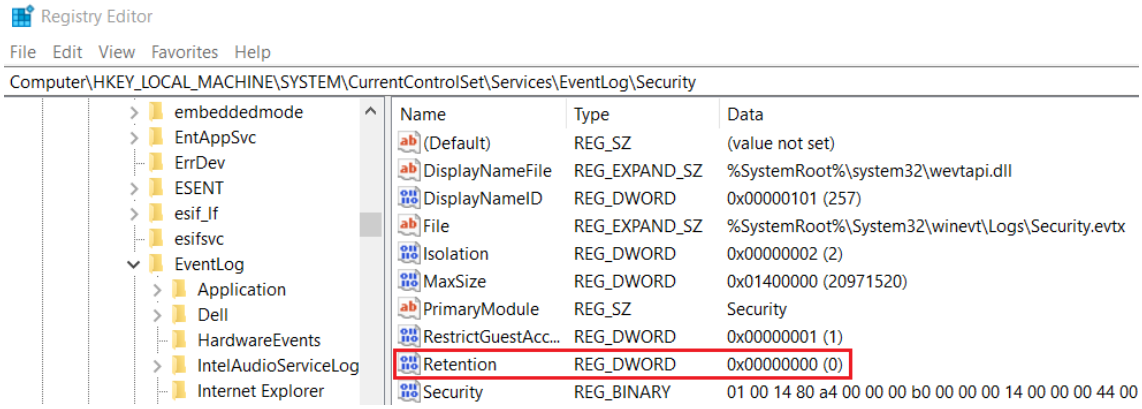
Tabuľka 3: Nástroje na mazanie súborov

Po použití nástrojov na odstraňovanie súborov v systéme ostávajú stopy po spustení aplikácie v prefetch súboroch (medzi spustenými programami). V prípade že súbory boli na danom zariadení otvorené, tak je možné nájsť aj linkové súbory, z ktorých sa dá vyčítať aspoň názov odstráneného súboru a jeho pôvodné umiestnenie.

3.1.2 Mazanie logov

Keďže logy zaznamenávajú všetky dôležité udalosti a poskytujú tak forenznému analytikovi podstatné informácie, vymazanie takýchto logov môže spomaliť proces analýzy zaistených stôp. Najčastejšie sú mazané hlavné kategórie logov: *Security*, *System* a *Application*, pretože obsahujú najviac významných udalostí. V prípade vymazania logu kategórie Security sa vygeneruje nový Security log s ID 1102. Pri vymazaní akéhokoľvek iného logu sa vygeneruje nový log s ID 104 v kategórii System.

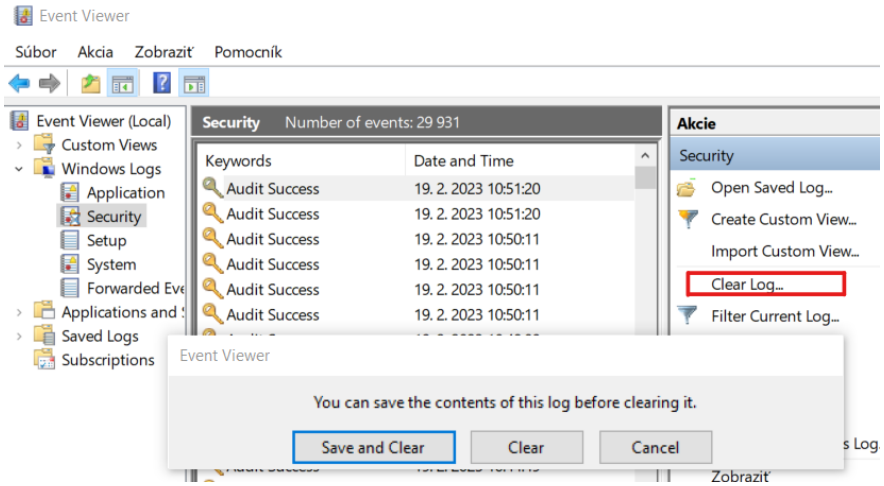
Generovanie logov o vymazaní môže útočník obísť zmenou tzv. *retention hodnoty* (obrázok 8) z 0 na akúkoľvek inú hodnotu, čo spôsobí, že pri dosiahnutí maximálnej veľkosti logov nebudú staré logy nahradzované novými ale nové logy sa prestanú zapisovať, kým sa miesto neuvoľní manuálne. Taktiež je možné zastaviť službu „Windows Event Log“, čím sa zaznamenávanie logov úplne zastaví. (Perlman, 2022).



Obrázok 8: Retention hodnota v registri

Ďalší, menej nápadný spôsob na zabránenie vygenerovania nových logov, spočíva v identifikácii procesu Windows Event Log a jeho zastavení, resp. v identifikácii všetkých jeho vlákien, ktoré sa prerušia, čo umožní odstraňovať logy bez vygenerovania nových logov, pričom samotný proces Windows Event Log naďalej beží (MITRE ATT&CK®, n.d.).

Všetky logy vybranej kategórie sa dajú odstrániť priamo vo vstavanej aplikácii Event Viewer kliknutím na „*Clear Log...*“ (viď. obrázok 9). Ďalšia, pre útočníka prívetivejšia možnosť, je vymazanie príkazom v PowerShelli. Použiť sa dá príkaz „Clear-EventLog“ alebo „Remove-EventLog“.

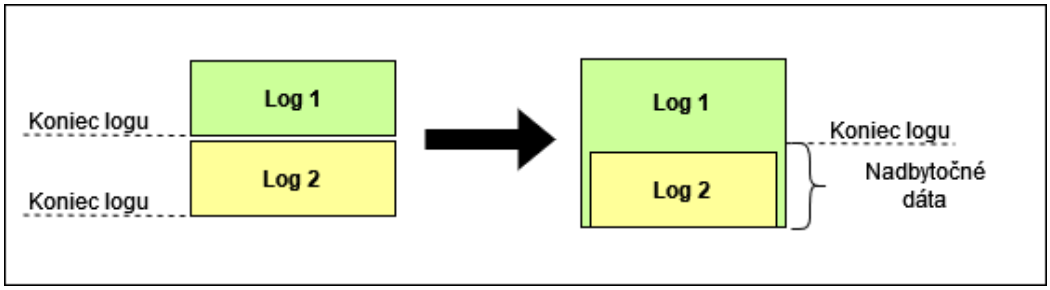


Obrázok 9: Odstránenie záznamov

Pri odstraňovaní konkrétnych logov vznikajú medzery v identifikátoroch logov, ktoré sa pre každý nový log zvyšujú o 1. To by umožňovalo jednoduchú detekciu odstránenia logov hľadaním chýbajúcich identifikátorov, avšak aj tento indikátor mazania je možné obísť prepísaním identifikátorov všetkých predchádzajúcich logov (svch0st, 2020). Modifikáciu logov popisujeme kapitole 3.3.1.

Logy je možné naoko odstrániť pri zobrazovaní v Event Vieweri, a to tak, že sa daný log zlúči s predchádzajúcim logom. Hlavička predchádzajúceho logu sa zväčší o veľkosť logu, ktorý má byť odstránený, čo spôsobí, že pri interpretácii logov je odstraňovaný log považovaný za nadbytočné dáta, keďže sa nachádza za označením konca dát logu (obrázok 10). Na takúto úpravu je možné použiť nástroj *eventlogedit* z frameworku DanderSpritz od NSA. Zároveň už však existuje aj implementácia

skriptu, ktorý dokáže tieto úpravy rozpoznať a extrahovať takto ukryté záznamy. (Jansen, 2017).



Obrázok 10: Zlúčenie logov

3.1.3 Mazanie z registrov

Mazanie hodnôt z registrov môže útočník využiť pri odstraňovaní stôp po útoku. Z pohľadu útočníka môžu byť dôležité hodnoty týkajúce sa napr. nimi vytvorených registrov (na získanie perzistencie) či pozostatkov odstránených aplikácií.

Jednotlivé hodnoty ale aj kľúče sa dajú odstrániť priamo v Registry Editore kliknutím pravým tlačidlom na požadovanú položku, kliknutím na „Odstrániť“ a potvrdením upozornenia, ktoré sa zobrazí.

Alternatívou sú príkazy „reg delete“ v príkazovom riadku cmd alebo „Remove-ItemProperty“ v PowerShelli. Príkazy je potrebné spustiť s administrátorskými privilégiami.

Po vymazaní kľúča môžu ostať zachované stopy v rovnomennom kľúči s príponou LOG, do ktorého sa z dôvodu konzistencie zapisujú hodnoty ešte pred ich vložením do požadovaného registra (Perlman, 2022).

3.2 Ukrývanie dát

Pre útočníka môže byť v niektorých prípadoch výhodné ukrývať dáta, aby sa vyhol detekcii, či už počas inicializácie útoku, získavania perzistencie, vykonávania škodlivej činnosti, či exfiltrácie údajov.

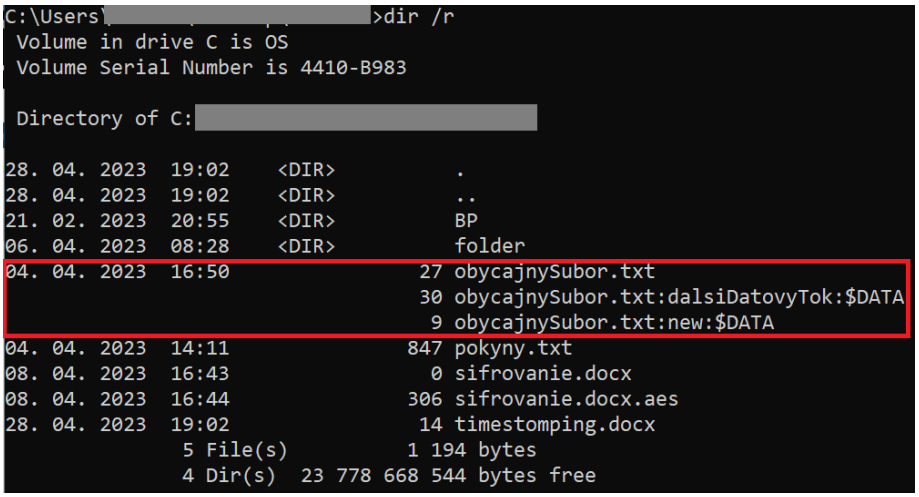
3.2.1 Alternatívne dátové toky

V súborovom systéme NTFS môžu súbory obsahovať viaceré dátové toky. Základný dátový tok obsahuje samotné dáta súboru a zobrazuje sa vtedy, keď nie je

špecificky požadovaný iný, tzv. alternatívny dátový tok (ADS). Každý súbor môže mať viacero ADS.

Hlavným významom ADS je zaznamenanie dodatočných informácií. Používa sa to napr. pri sťahovaní súborov z nedôveryhodného zdroja na označenie, že daný súbor môže byť škodlivý. Microsoft Word súbor si do ADS môže uložiť metadáta ako autor či počet strán, môžu sa tam ukladať informácie o oprávneniach a pod.

Dôležitá je informácia, že pridanie ADS vôbec nemení veľkosť súboru, teda aj v zdanlivo obyčajnom súbore môže byť ukrytý celý zdrojový kód malvéru, škodlivý spustiteľný súbor a i. Avšak stačí v príkazovom riadku pri vypisovaní obsahu priečinka použiť príkaz *dir /r* a zobrazia sa aj všetky ADS (obrázok č. 11). Je možné vypísať ich obsah napr. príkazom *more < obycajnySubor.txt:dalsiDatovyTok*.



Obrázok 11: Porovnanie veľkosti po pridaní ADS

Pomocou ADS tak môžu útočníci ukryť škodlivý kód v legitímnom programe, čím docielia to, že sa ich program bude vykonávať pod názvom legitímneho procesu, pričom neovplyvnia veľkosť ani funkčnosť tohto procesu. (Hassan, Hijazi, 2017).

3.2.2 Slack space

Pojmom slack space je označovaná nevyužitá časť klastra (t.j. najmenšia časť disku, ktorá musí byť alokovaná pre uloženie dát), ktorý je vyhradený pre nejaký súbor. Klaster môže byť naraz využívaný iba jedným súborom. Je teda menšie riziko toho, že daná časť disku bude prepísaná inými dátami (to sa aj naďalej môže udiať v prípade zväčšenia súboru) a preto je slack space vhodný na ukrytie iných dát.

Na takéto ukrytie je možné použiť voľne dostupný nástroj *Slacker.exe*[1] od Metasploitu, ktorý umožňuje ukrývanie aj extrakciu a podporuje aj zabezpečenie ukrytých dát heslom. Veľkosť využiteľného priestoru na ukrytie však nemusí byť vôbec veľká (napr. v porovnaní s ADS). (Hassan, Hijazi, 2017).

3.2.3 Šifrovanie

Šifrovanie je veľmi účinná metóda zaisťujúca dôvernosť dát. Používa sa v každodennom živote a za účelom ukrytia dát pred nepovolanými osobami ju používajú aj útočníci. Šifrované môžu byť jednotlivé súbory, priečinky alebo partície. V prípade zašifrovania celého zariadenia môže byť úplne znemožnená forenzná analýza.

Súčasným štandardom na šifrovanie dát je symetrický algoritmus AES s použitím aspoň 128-bitového šifrovacieho kľúča (Barker, 2020). V tabuľke č. 4 uvádzame výber nástrojov, ktoré je možné použiť za účelom šifrovania. Prítomnosť šifrovaných súborov detegujú niektoré nástroje používané vo FA na základe entropie. Zašifrovanie ovplyvní časové pečiatky šifrovaných súborov, resp. vytvorí nový šifrovaný súbor (v závislosti od použitej aplikácie), kde veľkosť súboru môže byť voči originálu pozmenená.

Nástroj	Použitie	Dostupnosť	Najnovšie vydanie	Poznámky	Odkazy
AES Crypt	súbory	zdarma	2013	AES, aj cez príkazový riadok	aescrypt.com
AxCrypt	súbory	skúšobná verzia/platené	2023	AES	axcrypt.net
BestCrypt Container Encryption	súbory, priečinky	skúšobná verzia/platené	2022	AES, Blowfish, CAST, GOST 28147-89, Twofish, Camellia	jetico.com
BestCrypt Volume Encryption	disk	skúšobná verzia/platené	2023	AES, ARIA, Camellia, Serpent, Twofish	jetico.com
BitLocker	disk	zdarma	neznáme	AES	microsoft.com

[1] https://github.com/codejanus/ToolSuite/blob/master/slacker.exe

NordLocker	lokálny/cloud trezor	zdarma s obmedzením/ platené	neznáme	AES	nordlocker.com
VeraCrypt	disk	zdarma	2022	AES, Camellia, Kuznyechik, Serpent, Twofish a ďalšie	veracrypt.fr

Tabuľka 4: Nástroje na šifrovanie

3.2.4 Steganografia

Dáta je možné ukrývať v iných digitálnych médiách, tzv. *nosných médiách*, ktorými sú najčastejšie obrázky, ale aj videá či zvukové nahrávky. Vkladanie skrytých dát do digitálnych médií nazývame steganografia. Používa sa napr. na nenápadné vynášanie informácií, keďže funkčnosť a vzhľad nosných médií nie sú nijak ovplyvnené. Steganografia je zároveň vhodná alternatíva ukrývania dát šifrovaním, pretože jej detekcia je omnoho náročnejšia. Môže sa používať aj v prípadoch spywaru (keylogger), kde je dôležité, aby si antimalvérový softvér ani používateľ nič podozrivé nevšimol.

Existuje množstvo nástrojov, ktoré je možné použiť na ukrytie dát do digitálnych médií (prehľad niektorých z nich je v tabuľke č. 5). Líšia sa podporovanými médiami, maximálnou veľkosťou vkladaných dát, niektoré najprv vkladané dáta šifrujú. Nástroje zároveň podporujú jednoduché spätné získanie dát (po zadaní hesla použitého na šifrovanie).

Nástroj	Podporované formáty	Dostupnosť	Najnovšie vydanie	Poznámky	Odkazy
Hide'N'Send	JPEG	nedostupný	2012	algoritmy - F5 and LSB, matrix coding	download.cnet
OpenPuff	obrázky, PCX, MP3, WAV, 3GP, MP4, SWF, PDF a ďalšie	zdarma	2018	prenosný nástroj	embeddedsw.net
Our Secret	obrázky, zvuk	skúšobná verzia	neznáme		downloadsource.net
rSteg	obrázky, export do	zdarma	2010	prenosný nástroj,	softpedia.com

	PNG			vyžaduje Javu	
Ssuite Picsel	obrázky (vrátane BMP, WMF)	zdarma	neznáme	kľúč pre zašifrovanie je obrázok, prenosný, neintuitívny	ssuitesoft.com
SteganoG	BMP	zdarma	2017	prenosný nástroj	softpedia.com
Steganography Online Codec	JPG, PNG, GIF, BMP	zdarma, online	neznáme	na výstupe je PNG, algoritmus LSB	pelock.com
SteganPEG	JPG	zdarma	2011	iba obrázky	softpedia.com
StegOnline	obrázky	zdarma, online	2020	LSB	stegonline.georgeom

Tabuľka 5: Výber nástrojov na steganografiu

Od vzniku steganografie boli navrhnuté a implementované viaceré spôsoby, ako zakomponovať požadované dáta do dát iného média. Najbežnejšie sú algoritmy upravujúce najmenej významné bity (Least Significant Bits) nosného súboru. Sú to napr, algoritmy **LSB replacing** a **LSB matching**. Využívajú to, že zmena posledného bitu označenia farby pixelu nespôsobuje pri pozorovaní voľným okom žiadne viditeľné rozdiely. (Hassaballah, 2020). Pre ukrytie väčšieho objemu dát je potrebné modifikovať nie len posledný najmenej významný bit ale aj druhý od konca, prípadne tretí atď. To však spôsobuje viditeľnejšie zmeny v grafických súboroch a preto je veľkosť ukrývaných dát obmedzená. Ďalšou nevýhodou je poškodenie ukrytých dát v prípade úpravy nosného súboru (orezanie, pridanie efektov, zmena veľkosti).

K ďalším spôsobom vkladania dát patrí **manipulácia funkcie diskrétnej kosínusovej transformácie** (Discrete Cosine Transform), ktorá sa používa na kódovanie a dekódovanie napr. JPEG formátu a technika **vkladania na koniec súboru** (Asawaree; Goldman et al., 2009).

Pri použití steganografie dochádza k vzniku stôp po inštalácii/spustení aplikácie na vykonanie steganografie, resp. môžu vznikať generické dáta (história vyhľadávania v prehliadači) pri hľadaní online nástroja. Po vykonaní steganografie vzniká nový súbor obsahujúci ukryté dáta, teda je možné hľadať artefakty súvisiace s vznikom nových súborov. Taktiež existujú nástroje, ktoré hľadajú možné použitie steganografie na základe entropie, pri čom teda analyzujú obsah všetkých súborov, čo môže byť časovo

náročné. Preto je najdôležitejšie identifikovať použitie aplikácie na vkladanie súborov do nosného média.

3.2.5 Ukrývanie v registroch

Útočníci môžu použiť registre na ukrytie škodlivého kódu. Malvér sa teda nemusí vôbec nachádzať na disku a vykonáva sa vkladaním do iných procesov. Ukrývanie je možné vykonať manuálne – vytvorením novej hodnoty v registri. Veľkosť jednej hodnoty je 64 KB, avšak podľa Hassana a Hijaziho (2017) je tam možné bez problémov ukryť aj 50 strán ASCII textu.

Detekcia takéhoto bezsúborového útoku antimalvérovou aplikáciou je prakticky nemožná. Pomocou dostupných nástrojov je možné hľadať napr. hodnoty v registroch, ktoré obsahujú viac dát ako ostatné. Získané výsledky je však potom potrebné manuálne skontrolovať, keďže vyhľadávanie na základe veľkosti nemusí byť vôbec spoľahlivé. Ani žiadna detekcia takýmito nástrojmi nemusí znamenať, že v registroch nie je ukryté niečo škodlivé. (Hassan, Hijazi, 2017).

3.3 Obfuskácia a zmena dát

Obfuskácia je forma zahmlievania alebo falšovania informácií. Používa sa teda s cieľom zavádzať pri vyšetrovaní, predĺžiť vyšetrovanie a odkláňať forenzných analytikov od skutočných problémov. Obfuskácia je veľmi často aplikovaná pri škodlivom kóde, kedy útočník prevedie funkčný kód na veľmi ťažko čitateľný kód tým, že použije iné kódovanie textu, nič nehovoriace názvy premenných a funkcií, pridajú sa funkcie, ktoré nič nerobia a pod. Tým sa docieli zdĺhavá analýza samotného kódu. Podobne pri forenznej analýze zariadenia je možné vytvoriť napr. logy, ktoré nie sú skutočné, prepísať dáta tak, aby boli ťažko čitateľné, vytvoriť množstvo podozrivo vyzerajúcich a zároveň nič nerobiacich súborov, či upraviť artefakty, aby bola analýza náročná a zdĺhavá.

Vytváraniu súborov s cieľom zvýšenia počtu dát, ktoré je potrebné analyzovať, sa budeme venovať aj v kapitole 5 a popíšeme vplyv pri automatizovanom vyhodnocovaní záznamov.

3.3.1 Modifikácia logov

Cieľom niektorých útočníkov môže byť spomalenie vyšetrovateľov, zavádzanie, či spochybnenie dôveryhodnosti zaistených dôkazov. K dosiahnutiu týchto cieľov im môže dopomôcť práve modifikácia logov. Modifikácia je potrebná aj pri mazaní logov, ak chce útočník zakryť fakt, že boli niektoré logy odstránené, teda že v postupnosti identifikačných čísel logov niektoré čísla chýbajú.

Základom modifikácie je znalosť štruktúry EVTX logov (popísaná v kapitole 2.4). Je totiž nevyhnutné nie len identifikovať konkrétnu udalosť, ktorú chceme pozmeniť, ale aj prepočítať všetky relevantné kontrolné súčty, ktoré sa menia so zmenou dát v EVTX súbore. V opačnom prípade by sa vyskytla chyba pri otváraní EVTX súboru.

Modifikácia sa dá vykonať manuálne – otvorením EVTX súboru v nástroji na prácu s hexadecimálnymi súbormi. Následne sa manuálne upravia požadované polia a prepočítajú sa kontrolné súčty pomocou algoritmu CRC32. (svch0st, 2020). Je to však veľmi zdĺhavý proces a vyžaduje si veľkú presnosť. Zároveň to v systéme zanecháva stopy po pristupovaní a upravovaní EVTX súborov. Efektívnejšie je celý tento proces zautomatizovať vytvorením nástrojov a pre lepší výsledok pridať aj zamedzenie logovania.

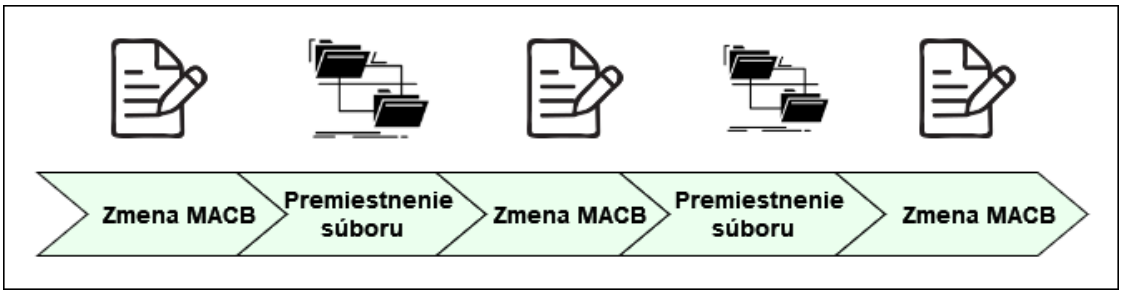
3.3.2 Timestomping

Timestomping - modifikácia časových pečiatok, dokáže malou zmenou ovplyvniť zaužívané procesy FA. V praxi nie je vždy čas na analýzu všetkých zaistených súborov a dát a preto sa často analýza vykonáva iba v rámci určitého časového úseku. Zmena časových pečiatok tak môže spôsobiť vynechanie dôležitých stôp.

Časové pečiatky (MACB) sa v systéme Windows ukladajú v MFT tabuľke. Niektoré môžu byť uložené aj v denníku a môžu byť získané aj z iných artefaktov ako sú nedávne súbory, v prípade že boli tieto súbory nedávno otvorené.

Modifikácia je možná prostredníctvom príkazového riadku, v ktorom je možné nastaviť zobrazované časové pečiatky, avšak systémové časové pečiatky ostanú nezmenené.

Tým, že sa systémové časové pečiatky aktualizujú pri premiestnení súboru, je možné ich upraviť krokmi znázornenými na obrázku 12 (Palmbach, Breitinger, 2020). Druhé premiestnenie súboru slúži iba na jeho uloženie na pôvodné miesto, nie je to potrebné na zmenu systémovej pečiatky.



Obrázok 12: Timestomping systémových pečiatok (Palmbach, Breitinger 2020)

Taktiež sú dostupné nástroje, ktoré je možné použiť za účelom timestompingu. Najviac spomínané nástroje sú nTimestopm[2], Timestomp[3] a SetMACE[4].

3.4 Útoky voči forenzným technikám a nástrojom

Kým predchádzajúce kategórie sa zameriavali na vykonanie techník s cieľom zanechať v systémoch čo najmenej dát, resp. zmanipulovať alebo zakryť možné stopy, táto kategória anti-forenzných techník sa zameriava na narušenie priebehu forenznej analýzy, a to útokmi voči zaužívaným technikám a procesom alebo útokmi voči nástrojom, ktoré forenzní vyšetrovatelia používajú.

Je verejne známe, aké postupy a najmä nástroje sa najčastejšie používajú na forenznú analýzu. Útočníci tak môžu skúmať zraniteľnosti používaných nástrojov a hľadať, ako tieto zraniteľnosti zneužiť v ich prospech. Docieliť by mohli napr. spochybnenie dôveryhodnosti zaistených dôkazov, ktoré by tým boli na súde nepoužiteľné.

Pri forenznej analýze môžu niektoré nástroje čerpať z online zdrojov, resp. sa môžu použiť iba online verzie niektorých nástrojov. V tomto prípade by mohol útočník vykonať útok na tieto online zdroje a spôsobiť ich nedostupnosť.

[2] https://github.com/limbenjamin/nTimetools
[3] https://github.com/jackson5sec/timestomp
[4] https://github.com/jschicht/SetMace

Ďalšia možnosť útoku na nástroje forenznej analýzy sú tzv. kompresné bomby. Sú to malé komprimované súbory, ktoré však po dekompresii naberajú obrovskú veľkosť, na ktorú nástroje nemusia byť stavané a dôjde k ich zlyhaniu. Kompresné bomby môžu byť tvorené napr. ďalšími komprimovanými súbormi, ktoré obsahujú ďalšie komprimované súbory. Príkladom je kompresná bomba 42.zip[5], ktorá má 42 bytov a po úplnom rozbalení je jej veľkosť až 4,5 PB.

Ďalšia forma nedostupnosti je Regular Expression Denial of Service (REDoS). Využíva to, že pri analýze sa hľadajú rôzne vzorce v dátach a názvoch pomocou regulárnych výrazov, a niektoré špeciálne vstupy môžu spôsobiť nárast časovej zložitosti vyhľadávania z lineárnej na exponenciálnu (vzhľadom na dĺžku vstupu). (Jain, Chhabra, 2014).

Vzhľadom na charakter týchto techník sa však touto kategóriu nebudeme bližšie zaoberať. Útokom na nástroje a procesy sa nie je možné vyhnúť a nie vždy je možné ich včas odhaliť a zabrániť im. Ich vplyv na samotné forenzné artefakty je zanedbateľný, ide skôr o dĺžku a dôveryhodnosť vyšetrovania, ktoré sú týmito technikami ohrozené.

[5] https://www.unforgettable.dk/

4 Popis datasetu

V ďalšej kapitole budeme pri zisťovaní vplyvu anti-forenzných techník používať existujúci dataset, nad ktorým budeme vyhľadávať anomálie. Dataset pochádza z portálu DFIR Madness z prípadu Case001 – The Stolen Szechuan Sauce[6]. K tomuto prípadu existuje viacero popisov a dokonca ho používajú aj výskumné články.

Budeme vychádzať z článku Detection of relevant digital evidence in the forensic timelines (2022), ktorý skúma viaceré metódy hľadania anomálií nad prípadom ukradnutej sečuánskej omáčky, konkrétne nad dátami získanými z obrazu disku servera.

Kým v článku je vyhodnocovaná efektívnosť a presnosť pri aplikácii rôznych algoritmov a ich nastaveniach, my sa budeme pozerať iba na sumárne výsledky pre Empirical-Cumulative-distribution-based Outlier Detection (ECOD), keďže cieľom práce nie je hľadanie najvhodnejších nastavení či najpresnejších algoritmov. ECOD sme zvolili s ohľadom na zložitosť algoritmu (*O(n*d),* kde *n* je počet riadkov dát a *d* je počet dimenzií) a počet vstupných parametrov.

Počas behu programu na hľadanie anomálií sa testujú všetky kombinácie pre 7 hodnôt kontaminácie, 4 agregačné funkcie a všetky kombinácie logických skupín atribútov (t.j. nie každý beh programu je nad všetkými dostupnými atribútmi). Taktiež sa rozlišuje metóda vyhľadávania anomálií na základe názvov súborov a na základe tzv. inodov. Pojem inode označuje číslo, ktoré slúži ako jednoznačný identifikátor súboru v súborovom systéme NTFS (Carrier, 2005).

Rovnako ako v spomínanom článku, použijeme predspracované dáta vyextrahované z obrazu disku, konkrétne dáta týkajúce sa súborov, v ktorých je identifikovaných 17 anomálnych názvov súborov a 15 anomálnych inodov a ECOD vykonáme nad dátami z času útoku a pozrieme sa na sumárne výsledky. Samotné dáta sú súčasťou prílohy A spolu s kódom na hľadanie anomálií pomocou ECOD. Dáta sú uložené v CSV formáte a každý riadok má 60 atribútov. Atribúty, s ktorými sa pracuje sú binárne (napr. ak má záznam časovú pečiatku M, tak je atribút M nastavený na 1) a sú združené do 8 logických skupín.

[6] https://dfirmadness.com/the-stolen-szechuan-sauce/

5 Vplyv anti-forenzných techník

V tejto kapitole uvedieme prístupy k stanoveniu vplyvu anti-forenznej techniky na konkrétne artefakty, ako aj na výsledky algoritmického vyhľadávania anomálií. Následne tieto prístupy využijeme pre ohodnotenie konkrétnych techník a ich vplyvov na vybrané artefakty a precíznosť vyhľadávania anomálií.

5.1 Prístupy k určovaniu vplyvu

Na stanovenie miery vplyvu anti-forenznej techniky na artefakt sme definovali 2 spôsoby (úrovne vplyvu a matica vplyvu). Kým prvý neberie do úvahy žiadne okolnosti, druhý zohľadňuje aj náročnosť detekcie použitej techniky. Na vyhodnotenie vplyvu pri detekcii anomálií použijeme ohodnotenie precíznosti.

5.1.1 Úrovne vplyvu

Vplyv anti-forenznej techniky na kvalitu artefaktu bez prihliadnutia na iné okolnosti (náročnosť detekcie, dôležitosť artefaktu) je možné charakterizovať nasledujúcimi 4 úrovňami vplyvu:

- **Žiadny vplyv:** anti-forenzná technika artefakt neovplyvňuje.
- **Malý vplyv:** technika mení umiestnenie artefaktu a/alebo vytvára falošné artefakty
- **Stredný vplyv:** technika čiastočne mení obsah a/alebo modifikuje metadáta artefaktu.
- **Vysoký vplyv:** technika zatají existenciu daného artefaktu, odstráni artefakt (a stopy po jeho existencii) a/alebo ho nenávratne prepíše.

5.1.2 Matica vplyvu

Ako jednu z možností pre porovnávanie vplyvu rôznych techník na artefakty sme navrhli maticu vplyvu anti-forenznej techniky na artefakt (tabuľka 6). Matica berie do úvahy náročnosť detekcie použitia danej anti-forenznej techniky a stav artefaktu. Na výstupe sú 3 úrovne vplyvu na artefakt:

- **Malý vplyv** značí to, že daná anti-forenzná technika sa zameriava na artefakty, ktoré je možné nahradiť inými alebo sú artefakty čiastočne zotaviteľné a samotná detekcia použitia techniky je triviálna, pretože v systéme zanecháva očividné stopy. Malý vplyv má aj kombinácia náročne detekovateľnej techniky spolu s nahraditeľným artefaktom, keďže po zistení použitia danej techniky stačí nahradiť ovplyvnený artefakt iným.
- **Stredný vplyv** zodpovedá buď takmer nemožnej detekcii ale nahraditeľnému artefaktu, alebo čiastočne zotaviteľnému artefaktu a náročnej detekcii, resp. nezotaviteľnému artefaktu ale triviálnej detekcii.
- **Vysoký vplyv** budú mať techniky, ktoré úplne znehodnotia artefakt a ich detekcia je náročná alebo takmer nemožná. Veľký vplyv má aj takmer nedetekovateľná technika, ktorá ovplyvňuje čiastočne nahraditeľný artefakt. Takéto techniky budú mať veľký význam pri automatizácii procesov forenznej analýzy, ako aj pri manuálnej analýze.

Vplyv anti-forenznej techniky na artefakt		stav artefaktu		
		je nahraditeľný	dá sa čiastočne zotaviť	nedá sa zotaviť ani nahradiť
detekcia	takmer nemožná			**vysoký vplyv**
	náročná		**stredný vplyv**	
	triviálna	**malý vplyv**		

Tabuľka 6: Matica vplyvu

V tabuľke nie je uvedená možnosť, kde artefakt je síce technikou ovplyvnený, ale nie je relevantný pre forenznú analýzu, pretože takéto artefakty nebudeme ohodnocovať. Rovnako neuvádzame možnosť nemožnej detekcie, pretože aj techniky, ktoré sú na teoretickej úrovni nedetekovateľné, môžu mať nedokonalú praktickú aplikáciu (ľudský faktor), ktorá predsa len zanechá v systéme stopy.

5.1.3 Hodnotiace techniky

- *Presnosť (precision):* slúži na ohodnotenie miery správne identifikovaných anomálií (True Positive, ozn. TP) k všetkým identifikovaným anomáliám, teda tým správne identifikovaným ale aj nesprávne identifikovaným (False Positive, ozn. FP).

$$Presnosť = \frac{TP}{TP + FP}$$

- *Senzitivita (recall):* meria počet správne identifikovaných anomálií (TP) vzhľadom na všetky anomálie, ktoré by reálne mali byť označené. Je to teda podiel TP a súčtu TP a nesprávne neidentifikovaných anomálií (False Negative, ozn. FN).

$$Senzitivita = \frac{TP}{TP + FN}$$

- *F1-skóre (F1-Score):* kombinuje presnosť a senzitivitu, najlepšia výsledná hodnota je 1, počíta sa nasledovným vzorcom:

$$F1 - skóre = 2 * \frac{presnosť * senzitivita}{presnosť + senzitivita}$$

Maximálna možná hodnota pre všetky tieto ohodnotenia je 1. (Kanstrén, 2020). Najväčšiu váhu budeme pri určovaní vplyvu prikladať práve F1-skóre, keďže je kombináciou predchádzajúcich dvoch hodnôt. Aj presnosť a senzitivita ako také sú však dôležité.

Na vyhodnotenie použijeme jednak súčet nájdených anomálií za všetky behy programu a ich ohodnotenie precíznosti ako aj priemerné hodnoty pre 5 nastavení, ktoré dávajú pre originálne dáta najlepšie výsledky.

5.2 Vplyv mazania súborov

Vplyv na artefakty

Na testovanie sme použili 2 nástroje určené na mazanie: BitKiller verzie 2.0 a Eraser. Autorom nástroja BitKiller je Hasan N. Genc a z priloženej dokumentácie vyplýva, že BitKiller najprv prepíše zvolený súbor podľa vybranej metódy a potom

zmenší veľkosť súboru na 0. Ďalej je súbor 10-krát náhodne premenovaný a vymaže sa. (obrázok nástroja). Postup použitý nástrojom Eraser nie je popísaný.

Oboma nástrojmi sme zopakovali rovnaký postup odstraňovania (PDF súborov) a v prípade BitKillera sme vyskúšali všetkých 5 ponúkaných metód. Potom sme vytvorili obraz disku pomocou Access Data FTK Imager[7] verzie 7.4.1 a nahrali ho do nástroja Autopsy[8] verzie 4.19.3. Tam sa nám podarilo v oboch prípadoch nájsť linkové súbory odstránených súborov s ich pôvodným názvom a umiestnením, ako aj záznam o spustení nástroja na mazanie v prefetch súboroch. Detekcia mazania súboru je jednoduchá.

V logoch neboli nájdené žiadne relevantné záznamy a taktiež sa v žiadnom prípade nepodarilo extrahovať z pamäte odstránené súbory. Extrakcia PDF súborov pomocou nástroja Bulk Extractor [9] verzie 5.1 aj scalpel 2.0 [10] bola neúspešná.

Mazanie súboru má vplyv iba na samotné dáta súboru, ktoré sa nepodarilo vôbec zotaviť a na ostatné artefakty technika nemá **žiadny vplyv**. Úroveň vplyvu (5.1.1) na dáta súboru je síce **vysoká**, ale po prihliadnutí na jednoduchosť detekcie techniky je vplyv na dáta podľa matice vplyvu (5.1.2) **stredný**.

Vplyv na hľadanie anomálií

V predspracovaných dátach sme simulovali mazania súboru NoJerry.txt štyrmi rôznymi spôsobmi. Prvé 2 spôsoby simulujú obyčajné odstránenie súboru a to nastavením veľkosti súboru (a jeho prislúchajúceho LNK súboru) na 0 a jeho označením ako nealokovaný. To sa v porovnaní so simuláciou použitia aplikácie na mazanie ukázalo ako menej efektívne a ďalej to nebudeme brať do úvahy.

Simulácia kompletného vymazania sa v dátach prejavila ako odstránenie relevantných záznamov z dát, teda odstránením záznamu o NoJerry.txt (resp. aj NoJerry.lnk) zo súborového systému. Záznamy súvisiace s MFT a denníkom sme neodstraňovali, keďže ani aplikácie do týchto záznamov nezasahujú.

V tabuľke 7 uvádzame rozdiel počtu určených anomálií oproti pôvodným výsledkom. Všetky počty sú výsledkom sčítania všetkých anomálií nájdených počas celého behu určovania anomálií na základe rôznych kritérií.

[7] https://www.exterro.com/ftk-imager
[8] https://www.autopsy.com/
[9] https://downloads.digitalcorpora.org/downloads/bulk_extractor/
[10] https://github.com/machn1k/Scalpel-2.0

Pri odstránení textového súboru a jeho odkazu bol počet správne identifikovaných anomálií na základe agregácie podľa názvu súborov vo všetkých behoch o 190 menší oproti originálu. Pre forenzného analytika to znamená **menšiu presnosť výsledkov**. Počet nesprávne identifikovaných anomálií sa naopak zvýšil o 528, čo je najväčšie z navýšení a prináša **veľa nesprávne určených anomálií**, ktoré by musel forenzný analytik preskúmať.

Pri identifikácii anomálií na základe agregácie podľa inodov a odstránení iba súboru sa počet správne určených anomálií znížil najmenej. Pri odstránení súboru aj jeho odkazu sa počet nesprávne určených anomálií dokonca znížil, teda forenzný analytik by musel preskúmať o 6 nepodstatných záznamov menej.

V tabuľke 7 uvádzame porovnanie hodnôt z kapitoly 5.1.3. Ukázalo sa, že odstránenie súboru (aj jeho odkazu) vylepšuje senzitivitu a teda aj F1 skóre, hoci sme predpokladali presný opak. Príčinou môže byť menší počet záznamov, ktoré musí algoritmus vyhodnotiť.

	Presnosť		**Senzitivita**		**F1 skóre**	
	názov	inode	názov	inode	názov	inode
Originál	0,1859	0,2830	0,0761	0,0220	0,1080	**0,0409**
Odstránenie súboru	0,1787	0,2733	0,0789	0,0229	0,1094	0,0422
Odstránenie súboru aj LNK	0,1758	0,2819	0,0827	0,0237	0,1125	0,0438

Tabuľka 7: Porovnanie hodnotiacich techník (mazanie súborov)

Ak porovnáme odstránenie súboru a odstránenie súboru aj jeho odkazu, prvá možnosť dosahuje nižšiu celkovú presnosť, pravdepodobne preto, že neodstránené LNK súbory bez samotného súboru, na ktorý odkazujú, môžu pôsobiť výstrednejšie.

Na porovnanie sme zisťovali aj priemer najlepších 5 nastavení pre výsledky v originálnych dátach. Priemerné hodnoty sú uvedené v tabuľke č. 8. Je vidieť, že pre hľadanie anomálií podľa názvu je najhoršie F1 skóre pre zmazanie súboru aj jeho odkazu. Pri hľadaní podľa inodu sú výsledky menej jednoznačné, avšak aj tu dosiahlo zmazanie súboru aj jeho odkazu najhoršie F1 skóre.

		TP	FP	Presnosť	Senzitivita	F1 skóre
názov	**Originál**	14,0	57,2	0,1967	0,8235	0,3175
	Zmazaný súbor	14,0	57,2	0,1967	0,8235	0,3175
	Zmazaný súbor a odkaz	13,0	57,6	0,1842	0,7647	**0,2969**
inode	**Originál**	12,0	10,2	0,5513	0,8000	0,6483
	Zmazaný súbor	11,6	10,2	0,5434	0,8286	0,6521
	Zmazaný súbor a odkaz	11,4	10,4	0,5354	0,8143	0,6419

Tabuľka 8: Priemer piatich najlepších nastavení (mazanie súborov)

5.3 Vplyv mazania logov

Vplyv na artefakty

Vieme, že odstránenie celého EVTX súboru generuje nové logy s ID 1102 alebo 104. V prípade bežiacej logovacej služby je detekcia mazania logov jednoduchá. Vtedy je síce vplyv na logy **vysoký** (predpokladáme, že logy nie sú pravidelne zálohované), no s prihliadnutím na jednoduchú detekciu dostávame podľa matice vplyvu **stredný** dopad.

Ak chceme zabrániť vzniku logov zastavením služby Windows Event Log, vzniká nový log o zastavení služby s ID 1100 (navyše je potrebné zrušiť automatické spúšťanie služby). Po jej opätovnom spustení je však vygenerované množstvo chybových logov.

Dohľadali sme ID procesu, pod ktorým bežala logovacia služba. Tento proces sme zrušili bez vypnutia samotnej služby, avšak proces bol hneď obnovený (aj keď bolo jeho automatické spúšťanie vypnuté). Tento spôsob manuálneho vypínania služieb sa ukázal ako nefunkčný, keďže sa služba aj po zakázaní naďalej automaticky spustila. Na pozastavenie logovacej služby sme vyskúšali nástroje SuspendorResumeTid.exe a SuspendoerResumeTidEx.exe[11]. Nástroje sa síce tvárili, že vypínajú vlákna logovacej služby (viď. obrázok 13), ale nové logy vznikali aj naďalej. Za rovnakým účelom sme otestovali aj nástroj Phant0m[12]. Ten bol blokovaný vstavaným antimalvérovým riešením Windows Defender, ale ani po jeho vypnutí a spustení programu sa nepodarilo úspešne zastaviť logovanie. Navyše všetky tieto nástroje potrebovali na spustenie administrátorské privilégiá.

[11] https://github.com/3gstudent/Eventlogedit-evtx--Evolution
[12] https://github.com/hlldz/Phant0m

```
C:\Users\IEUser\Downloads>SuspendorResumeTid.exe suspend
[+]PID:756
[*]Try to EnableDebugPrivilege... Done
[+]Tid:884 suspend success
[+]Tid:1112 suspend success
[+]Tid:1116 suspend success
[+]Tid:1120 suspend success
```

Obrázok 13: Spustenie nástroja SuspendoerResumeTid.exe

Vplyv na hľadanie anomálií

V datasete sme simulovali vymazanie celej kategórie logov nastavením veľkosti a s ňou súvisiacich atribútov na 0. Pri vymazaní aplikačných logov nedošlo k žiadnym výrazným zmenám v sledovaných hodnotách (presnosť, senzitivita, F1 skóre). Niektoré z hodnôt sa líšili až od piateho desatinného miesta. To sa týka sumárnych výsledkov pre všetky behy hľadania anomálií ako aj priemerných výsledkov pre 5 najlepších nastavení.

V tomto prípade mazanie logov **nemá vplyv** na hľadanie anomálií. Toto hľadanie však prebieha iba nad súborovým systémom a nepozerá sa na obsah EVTX súborov. V prípade hľadania anomálií priamo nad obsahom EVTX logov môže byť vplyv mazania výraznejší.

5.4 Vplyv ukrývania v ADS

Vytvorili sme textový súbor, do ktorého sme vložili ADS. Vloženie spôsobilo aktualizáciu časových pečiatok zobrazovaného súboru a záznamy o zmenách je možné vidieť aj v denníku (obrázok 14), kde sa ako dôvod aktualizácie metadát uvádza „StreamChange“, teda zmena dátového toku. V prípade otvorenia dátového toku dokonca vzniká nový odkaz (zaznamenaný aj v denníku). Zároveň je možné všetky ADS jednoducho vypísať príkazom (viď. 3.2.1).

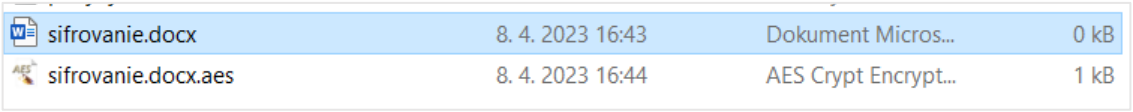
Name	UpdateTimestamp	UpdateReasons
obycajnySubor.txt	4.4.2023 14:50	StreamChange
obycajnySubor.txt	4.4.2023 14:50	NamedDataExtend|StreamChange
obycajnySubor.txt	4.4.2023 14:50	NamedDataExtend|StreamChange|Close
obycajnySubor.txt.lnk	4.4.2023 14:51	DataExtend|FileCreate|Close
obycajnySubor.txt.lnk	4.4.2023 14:51	DataExtend|FileCreate
obycajnySubor.txt.lnk	4.4.2023 14:51	FileCreate

Obrázok 14: Pridanie ADS v denníku

ADS má podľa kapitoly 5.1.1 **vysoký vplyv** na samotné dáta, keďže ich ukrýva, ale zároveň je detekcia ADS pomerne triviálna a dáta neodstraňuje ani nemodifikuje, teda podľa matice vplyvu (5.1.2) majú alternatívne dátové toky iba **malý vplyv** na dáta.

5.5 Vplyv šifrovania

Použili sme nástroj AES Crypt na zašifrovanie samostatného súboru. Nástroj je možné použiť cez príkazový riadok a zároveň sa zobrazuje ako možnosť pri kliknutí pravým tlačidlom na súbor. Po spustení nad konkrétnym súborom sa po zadaní hesla vytvorí nový rovnomenný súbor s príponou *.aes* a pôvodný súbor ostane nezmenený, viď. obrázok X. Prvým problémom šifrovania súborov je teda samotná existencia pôvodného súboru. Ten musí byť dôkladne odstránený, inak by šifrovanie nemalo význam.



Obrázok 15: Pôvodný a zašifrovaný súbor

Samotný zašifrovaný súbor nie je možné priamo otvoriť bez zadania správneho hesla. Pri zobrazení textu je možné vidieť v hlavičke názov šifrovacieho algoritmu aj názov použitého programu. Zvyšok dát je nečitateľný (viď. obrázok 16). Navyše je v systéme logovaná aj inštalácia samotného programu.

```
AES...&CREATED_BY.aescrypt (Windows GUI)
3.10.....................................................................
.....................................................MÒ..F¸àz.î.hùkÙÆ."wËéÝèhZ.êj.ï55
uR.6 zªCµ,\>.v1^E.÷ç°'íýÙX´À..þ>7I§ºi)$Ê«.º..ú.ómá¯ü.âby+....÷Oú.¤''w.4à¹Í.Ç._.
```

Obrázok 16: Obsah zašifrovaného súboru

Detekcia šifrovania súborov je **triviálna** a samotné dáta je možné obnoviť iba v prípade zle odstráneného pôvodného súboru. Ak teda uvažujeme, že útočník dokáže odstrániť dáta nezašifrovaného súboru, šifrovanie má **vysokú** úroveň vplyvu na dáta a žiadny vplyv na ostatné artefakty podľa 5.1.1 a **stredný vplyv** podľa matice 5.1.2.

Čo sa týka šifrovania celej partície alebo disku, je opäť veľmi jednoduché techniku detegovať, keďže dáta sú nečitateľné. Ovplyvnené však nie sú iba dáta konkrétnych

súborov, ale všetko uložené na danej partícii, vrátane MFT, denníka, logov (ak sa jedná o partíciu, kde je uložený operačný systém), obsahu koša, prefetchov, odkazov atď.

Podľa úrovní vplyvu má šifrovanie **vysoký vplyv** na všetky artefakty nachádzajúce sa na šifrovanej partícii/disku. Podľa matice vplyvu je to iba **stredný vplyv,** vzhľadom na jednoduchosť detekcie. Ohodnotenie pomocou úrovne vplyvu je v tomto prípade výstižnejšie, keďže forenzná analýza zašifrovaného disku býva neúspešná.

5.6 Vplyv vytvárania falošných stôp

Vyskúšali sme, ako vplýva vytvorenie nových súborov, ktoré vznikli v čase útoku, na detekciu anomálií. Do datasetu sme pridali modifikované záznamy, ktoré sú vytvorené pre iný súbor s rovnakou príponou (.txt, .exe). Zmenili sme názov, inode a časové pečiatky. V tabuľke 9 uvádzame výsledné hodnoty pre súčet všetkých behov funkcie ECOD. Výrazný pokles nastal pri agregácii podľa názvu, ale aj pri agregácii podľa inodu došlo k poklesu pri všetkých hodnotiacich technikách.

	Presnosť		**Senzitivita**		**F1 skóre**	
	názov	inode	názov	inode	názov	inode
Originál	0,1859	0,2830	0,0761	0,0220	0,1080	0,0409
Falošný súbor .txt	0,0988	0,2527	0,0385	0,0207	0,0555	0,0382
Falošný súbor .exe	0,0254	0,2681	0,0091	0,0215	**0,0134**	0,0398

Tabuľka 9: Porovnanie hodnotiacich techník (falošné stopy)

V tabuľke 10 sú výsledné hodnoty pre priemer piatich najlepších nastavení. Aj v tomto prípade došlo k poklesu všetkých hodnotiacich techník. Vo výsledku teda dokáže vytvorenie čo i len jednej zavádzajúcej stopy (súboru) výraznejšie zhoršiť výsledky pri automatizovanej detekcii anomálií.

		TP	**FP**	**Presnosť**	**Senzitivita**	**F1 skóre**
názov	**Originál**	14,0	57,2	0,1967	0,8235	0,3175
	Falošný súbor .txt	9,0	59,6	0,1314	0,5294	**0,2105**
	Falošný súbor .exe	9,0	58,6	0,1334	0,5294	0,2130
inode	**Originál**	12,0	10,2	0,5513	0,8000	0,6483
	Falošný súbor .txt	7,2	13,2	0,3634	0,4800	0,4126
	Falošný súbor .exe	8,4	12,8	0,4067	0,5600	0,4672

Tabuľka 10: Priemer piatich najlepších nastavení (falošné stopy)

5.7 Vplyv timestompingu

Vplyv na artefakty

Odskúšali sme zmenu časových pečiatok pomocou príkazového riadku ako aj pomocou nástrojov *nTimestomp* a *Timestomp*, tieto nástroje však dokázali modifikovať iba SI pečiatky. Použitie príkazového riadku PowerShell sa ukázalo ako najefektívnejší spôsob, ktorý navyše nezanecháva stopy po inštalácii.

V PowerShelli je možné zmeniť časové pečiatky jednoduchým nastavením pečiatky súboru $a na dátum $b, napr. $a.CreationTime = $b (viď. obrázok 17). Možné je takto nastaviť pečiatku vzniku súboru (B), poslednej modifikácie (M) a posledného prístupu (A). Tento prístup je možné skombinovať s premiestňovaním súboru (viď. 3.3.2).

```
PS: PowerShel> $a.CreationTime = get-date -year 2022 -month 10 -day 10
PS: PowerShell>$a | Get-ItemProperty -Name CreationTime


CreationTime : 10. 10. 2022 19:03:43
```

Obrázok 17: Timestomping času vzniku súboru

V tabuľke 11 a 12 uvádzame vyextrahované časové pečiatky. Postup 1 predstavuje iba zmenu pečiatok a postup 2 zahŕňa premiestňovanie. Je vidieť, že prvý postup nie je vôbec efektívny, ale druhým spôsobom je možné nepriamo nastaviť aj systémové pečiatky (FN, 0x30). Pečiatky A nie sú modifikované, pretože sa so súborom ďalej manipulovalo. Za povšimnutie však stoja pečiatky Last Record Change, ktoré hovoria o poslednej aktualizácii metadát. Bez kontextu by to mohlo vyzerať tak, že bol súbor iba presunutý (vtedy sa aktualizuje iba pečiatka C) a otvorený (mení sa iba pečiatka A). Na základe týchto údajov teda nie je možné jednoznačne potvrdiť timestomping.

postup	Created 0x10	Created 0x30	LastModified 0x10	LastModified 0x30
1	10.10.2022 13:14	6.3.2023 14:01	11.11.2022 14:15	6.3.2023 14:01
2	15.10.2022 12:49		15.10.2022 12:49	

Tabuľka 11: Časové pečiatky z MFT (časť 1)

postup	LastRecordChange 0x10	LastRecordChange 0x30	LastAccess 0x10	LastAccess 0x30
1	6.3.2023 14:16	6.3.2023 14:01	12.12.2022 14:16	6.3.2023 14:01
2	16.3.2023 13:56	16.3.2023 13:55	16.3.2023 13:57	16.3.2023 13:55

Tabuľka 12: Časové pečiatky z MFT (časť 2)

Ak je manipulácia so súborom stále viditeľná v denníku, nie je možné odtiaľ zistiť, o aké zmeny sa jedná, pretože všetky úpravy pečiatok sa zaznamenávajú s rovnakým popisom (zmena jednej pečiatky viď. tabuľka 13) a všetko by to mohli byť zmeny posledného pristúpenia k súboru. Ani na základe denníka teda nie je možné jednoznačne potvrdiť timestomping.

Name	UpdateTimestamp	UpdateReasons
timestomping.docx	6.3.2023 14:16	BasicInfoChange
timestomping.docx	6.3.2023 14:16	BasicInfoChange|Close

Tabuľka 13: Záznam v denníku pri aktualizácii MACB

Ďalším možným ukazovateľom timestompingu sú odkazy. Otestovali sme teóriu, že otvorenie súboru pri timestompingu aktualizuje časové pečiatky príslušných linkových súborov, podľa času nastaveného v súbore, čo sa ukázalo ako nepravdivé. Otvorenie súboru nastavilo časové pečiatky odkazu podľa systémového času. Preto sme odkazy modifikovali ručne, zistili sme však, že nie je možné odkaz po premiestnení z pôvodného priečinka vrátiť späť. Preto je možné na linkové súbory aplikovať iba prvý spôsob timestompingu, ktorý spôsobuje rozpor medzi SI a FN pečiatkami a teda nie je veľmi efektívny. Vždy sa však dajú odkazy úplne odstrániť, hoc aj to by mohlo poukazovať na podozrivé dianie v systéme.

Pomocou timestompingu je teda možné dosiahnuť **vysoký vplyv** na MACB umiestnené v MFT. Do istej miery je možné ovplyvniť aj linkové súbory (či už systémové alebo Office nedávne súbory), na ktoré je teda **stredný vplyv.** Ostatné artefakty neboli ovplyvnené. Rovnaké ohodnotenie vplyvu na jednotlivé artefakty dostávame aj z matice vplyvu, kde techniku timestompingu kategorizujeme ako takmer nedetekovateľnú.

Vplyv na hľadanie anomálií

V CSV súbore sme simulovali timestomping zmenou atribútov *date* a *time* pre súbor NoJerry.txt, konkrétne všetky jeho dáta okrem záznamov z denníka, keďže týmto záznamom nie je možné v systéme upraviť časové pečiatky. Dátum a čas sme nastavili na dobu pred útokom, konkrétne na deň 18.01.2023. Na týchto dátach sme hľadali anomálie na základe názvov súborov aj inodov. Tým, že sme zmenili čas na dobu pred útokom, vyhľadávanie anomálií vlastne tieto upravené záznamy vôbec nebralo do úvahy.

Pri pohľade na hodnotiace techniky (tabuľka 14) je vidieť, že použitie timestompingu znížilo pri hľadaní podľa názvu všetky hodnoty. Pri vyhľadávaní podľa inodov sa však zlepšila senzitivita a teda aj výsledné F1-skóre je mierne vyššie.

	Presnosť		**Senzitivita**		**F1 skóre**	
	názov	inode	názov	inode	názov	inode
Originál	0,1859	0,2830	0,0761	0,0220	0,1080	**0,0409**
Timestomping	0,1549	0,2657	0,0651	0,0229	0,0917	0,0421

Tabuľka 14: Porovnanie hodnotiacich techník (timestomping)

V tabuľke číslo 15 sú porovnania hodnôt pre 5 najlepších nastavení vzhľadom na originálne dáta. Najhoršie obstála detekcia anomálií na základe názvov pre dáta s použitým timestompingom, ktorá má všetky sledované parametre najhoršie. Aj pri detekcii na základe inodov je vidieť pri timestompingu výraznejší pokles presnosti, senzitivity aj F1 skóre.

		TP	**FP**	**Presnosť**	**Senzitivita**	**F1 skóre**
názov	**Originál**	14,0	57,2	0,1967	0,8235	0,3175
	Timestomping	8,0	58,6	0,1204	0,4706	**0,1916**
inode	**Originál**	12,0	10,2	0,5513	0,8000	0,6483
	Timestomping	8,6	13,0	0,4141	0,6143	0,4902

Tabuľka 15: Priemer piatich najlepších nastavení (timestomping)

Timestomping teda môže výrazne ovplyvniť automatizovanú detekciu anomálií.

6 Vyhodnotenie a diskusia

V tejto kapitole uvádzame zhrnutie výsledných vplyvov otestovaných anti-forenzných techník na manuálne aj automatizované forenzné vyšetrovanie. Vplyvy na artefakty pri manuálnej forenznej analýze sú uvedené vo výslednej tabuľke č. 16. Uvedené sú vplyvy podľa oboch navrhnutých prístupov na porovnanie.

Spôsob porovnania	Anti-forenzná technika	Dáta súborov	MACB	Logy
Úroveň vplyvu	**Mazanie súborov**	Vysoký	Žiadny	Žiadny
	ADS	Vysoký	Žiadny	Žiadny
	Šifrovanie súboru	Vysoký	Žiadny	Žiadny
	Šifrovanie disku	Vysoký	Vysoký	Vysoký
	Mazanie logov	Žiadny	Žiadny	Vysoký
	Timestomping	Žiadny	Vysoký	Žiadny
	Falošné stopy	Malý	Žiadny	Žiadny
Matica vplyvu	**Mazanie súborov**	Stredný	-	-
	ADS	Malý	-	-
	Šifrovanie súboru	Stredný	-	-
	Šifrovanie disku	Stredný	Stredný	Stredný
	Mazanie logov	-	-	Stredný
	Timestomping	-	Vysoký	-
	Falošné stopy	Malý	-	-

Tabuľka 16: Zhrnutie vplyvov vybraných techník

Zo všetkých otestovaných techník sa ukázalo šifrovanie disku ako najvýznamnejšie, keďže má vysoký/stredný vplyv na všetky artefakty uložené na disku. Druhá najvýznamnejšia technika je timestomping, keďže má vysoký vplyv podľa oboch ohodnotení. Šifrovanie súboru a mazanie súboru majú podľa tabuľky rovnaký vplyv na dáta súborov a majú tretí najväčší vplyv. Za nimi nasleduje mazanie logov s vysokým/stredným vplyvom a ukrývanie v ADS s vysokým/malým vplyvom. Ako najmenej významné sa ukázalo vytváranie falošných stôp s malým vplyvom.

Treba poznamenať, že tieto výsledky sú iba orientačné a môžu sa meniť v závislosti od konkrétnych okolností. Niektoré parametre na určenie vplyvu môžu byť dôležitejšie ako iné, preto je možné zvážiť navrhnutie iných spôsobov porovnanie

vplyvu, ktoré by odrážali dôležitosť konkrétnych aktív danej organizácie. Pri určení vplyvu môže mať význam aj to, či je potrebné klásť dôraz na integritu, dôvernosť alebo dostupnosť daného artefaktu, čo opäť vyplýva zo zamerania organizácie.

V tabuľke 17 uvádzame zhrnutie výsledných F1 skóre pre priemerné hodnoty piatich najlepších nastavení parametrov pre ECOD (vzhľadom na neupravený dataset). Všetky hodnoty sú výsledkom pri agregácii podľa inodu, keďže tento spôsob agregácie dáva vo všeobecnosti vyššie F1 skóre ako pri agregácii podľa názvu súboru.

	TP	FP	**F1 skóre**
Falošný súbor txt	7,2	13,2	**0,4126**
Falošný súbor exe	8,4	12,8	0,4672
Timestomping	8,6	13,0	0,4902
Originál	12,0	10,2	0,6483
Mazanie EVTX logov	12,0	10,2	0,6483
Zmazaný súbor a odkaz	12,0	10,2	0,6483
Zmazaný súbor	11,6	10,2	**0,6521**

Tabuľka 17: Porovnanie F1 skóre vybraných techník

Najväčší vplyv na automatizované vyhľadávanie anomálií má vytváranie falošných stôp, konkrétne textových a spustiteľných súborov. Tieto súbory vznikli v čase útoku a pôsobia ako potenciálne škodlivé súbory. Môžu narušiť hranicu medzi tým, čo je identifikované ako anomália a čo nie je.

Výraznejší vplyv zaznamenala technika zmeny časových pečiatok – timestomping. Naopak mazanie logov či súborov nespôsobilo výrazné zmeny a pri automatizovanej detekcii anomálií sú to zanedbateľné anti-forenzné techniky.

Vytváraniu zavádzajúcich súborov nie je možné v systéme zabrániť ani jednoduchým spôsobom detegovať. Preto je žiadúce ďalej preskúmať správanie takýchto falošných súborov (či boli otvorené, spustené, či spúšťajú ďalšie procesy) a navrhnúť spôsob na ich detekciu a odfiltrovanie počas predspracovania dát.

Je potrebné prihliadať aj na obmedzenia pri testovaní vplyvov na automatizáciu. Takýmto obmedzením je použitie datasetu, ktorý pozostáva iba z údajov získaných zo súborového systému, nad ktorými nie je možné otestovať všetky techniky. Tiež je možné na testovanie použiť iné metódy na detekciu anomálií, ktoré môžu poskytnúť iné výsledky.

7 Záver

Anti-forenzné techniky používajú útočníci na zahladenie či znehodnotenie stôp po útoku, na vyhýbanie sa detekcii alebo na spomalenie procesu forenznej analýzy. Tieto techniky ovplyvňujú forenzné vyšetrovanie rôznymi spôsobmi a v rozličnej miere. Aby sa bolo možné voči týmto technikám brániť, je potrebné poznať ako fungujú a ako zistiť, či boli použité. Je však nereálne poznať a detegovať každú techniku, a preto je potrebné vedieť si určiť priority. Zámerom tejto práce je jednotne popísať vplyvy anti-forenzných techník na digitálne forenzné vyšetrovanie.

V prvej kapitole sme stručne predstavili, čo zahŕňa forenzné vyšetrovanie pozostávajúce z viacerých odlišných fáz. Ďalej sme sa zamerali iba na fázu digitálnej forenznej analýzy, ktorá analyzuje zaistené stopy, keďže práve v tejto fáze je najčastejšie možné prísť do styku s anti-forenznými technikami.

V druhej kapitole sme popísali forenzné artefakty, ktoré sa pri forenznej analýze sledujú najviac. Nakoľko k cieľom patrí aj otestovanie anti-forenzných techník a vyhodnotenie údajov pred a po ich použití, hľadali sme pri testovaní jednotlivých techník zmeny predovšetkým v týchto artefaktoch. Zistili sme ako sa použitie konkrétnych anti-forenzných techník odrazí v jednotlivých artefaktoch. Princípy fungovania vybraných anti-forenzných techník sme popísali v tretej kapitole.

Pozreli sme sa na vplyv anti-forenzných techník pri automatizácii, ktorá môže byť súčasťou forenzného vyšetrovania. Použili sme dataset so známymi anomáliami, ktorý je popísaný v štvrtej kapitole. Nad ním sme hľadali anomálie pred a po použití anti-forenznej techniky a porovnali sme F1 skóre získaných výsledkov.

Vplyvy jednotlivých techník na artefakty, ako aj na automatizáciu sú uvedené v piatej kapitole. Nie každá technika však bola vhodná na otestovanie, vzhľadom na použitý dataset či charakter techniky.

Získané výsledky sme zhodnotili v šiestej kapitole a určili sme najvplyvnejšie anti-forenzné techniky. Ukázalo sa, že najväčší vplyv na artefakty má šifrovanie disku a najväčší vplyv pri detekcii anomálií má vytváranie falošných súborov, ktoré sa tvária škodlivo, ale nie sú škodlivé. Ďalej sme diskutovali o možnostiach iného určovania vplyvu a obmedzeniach práce. Navyše bolo problematické navrhnúť spôsob, ktorý by dokázal poňať všetky faktory pôsobiace na určenie výsledného vplyvu.

V budúcnosti by bolo možné túto prácu ďalej rozšíriť, či už otestovaním ďalších anti-forenzných techník a ich kombinácií, navrhnutím iných spôsobov určenia vplyvu, použitím ďalších algoritmov na identifikáciu anomálií alebo zisťovaním vplyvu na iné automatizované procesy. Zaujímavé by bolo aj vytvorenie tréningového obrazu disku, kde by boli použité viaceré anti-forenzné techniky, a slúžil by na vzdelávanie forenzných analytikov ako aj na ďalší výskum.

8 Zoznam použitej literatúry

Adamu, B. Z., Karabatak, M., & Ertam, F. (2020, jún 1). A Conceptual Framework for Database Anti-forensics Impact Mitigation. *8th International Symposium on Digital Forensics and Security, ISDFS 2020*. https://doi.org/10.1109/ISDFS49300.2020.9116375

Alazab, M., Venkatraman, S., & Watters, P. (2009). *EFFECTIVE DIGITAL FORENSIC ANALYSIS OF THE NTFS DISK IMAGE*. https://www.ubicc.org/files/pdf/3_371.pdf

Asawaree; Goldman, J. ;, Nabholz, B. ;, & Eyre, W. (2009). Forensic Science and Technology Commons, and the Information Security Commons Recommended Citation Recommended Citation Kulkarni. *Journal of Digital Forensics, Security and Law, 4*(2). https://doi.org/10.15394/jdfsl.2009.1055

Barker, E. (2020). Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. *NIST Special Publication*, *800*(175B). https://doi.org/10.6028/NIST.SP.800-175Br1

Carrier, B. (2005). File system forensic analysis. *Addison-Wesley Professional*.

EC-Council. (2021). *Digital Forensics Essentials*. EC-Council.

Forensic Focus. (2019). *Windows Registry Analysis 101*. https://www.forensicfocus.com/articles/windows-registry-analysis-101/

Forensics Wiki. (n.d.). *Artifacts*. https://forensics.wiki/artifacts/.

Gül, M., & Kugu, E. (2017, október 30). A survey on anti-forensics techniques. *IDAP 2017 - International Artificial Intelligence and Data Processing Symposium*. https://doi.org/10.1109/IDAP.2017.8090341

H. Majed, H. N. Noura, & A. Chehab. (2020). *Overview of Digital Forensics and Anti-Forensics*. 8th International Symposium on Digital Forensics and Security : 1-2 June 2020 .

Hassaballah, M. (2020). Digital media steganography: Principles, algorithms, and advances. V *Digital Media Steganography: Principles, Algorithms, and Advances*. Elsevier. https://doi.org/10.1016/C2018-0-04865-3

Hassan, N. A. (2019). Digital Forensics Basics A Practical Guide Using Windows OS. V *Digital Forensics Basics*. Apress.

Hassan, N. A., & Hijazi, R. (2017). Data Hiding Under Windows® OS File Structure. V *Data Hiding Techniques in Windows OS* (s. 97–132). Elsevier. https://doi.org/10.1016/b978-0-12-804449-0.00004-x

Hosgor, E. C. (2020). Detection and Mitigation of Anti-Forensics. *International Journal of Computer Science and Information Security*. https://doi.org/10.5281/zenodo.4425257

Choi, J., Park, J., & Lee, S. (2021). Forensic exploration on windows File History. *Forensic Science International: Digital Investigation*, *36*. https://doi.org/10.1016/j.fsidi.2021.301134

Jain, A., & Chhabra, G. S. (2014). Anti-forensics techniques: An analytical review. *2014 7th International Conference on Contemporary Computing, IC3 2014*, 412–418. https://doi.org/10.1109/IC3.2014.6897209

Jansen, W. (2017). *Detection and recovery of NSA's covered up tracks*. Fox-IT International blog. Cit 10. apríl 2023, z https://blog.fox-it.com/2017/12/08/detection-and-recovery-of-nsas-covered-up-tracks/

Jansen, W., & Ayers, R. (2004). Guidelines on PDA Forensics. *National Institute of Standards and Technology Special Publication*, *800*(72). https://doi.org/10.6028/NIST.SP.800-72

Kanstrén, T. (2020). *A Look at Precision, Recall, and F1-Score*. Towards Data Science. https://towardsdatascience.com/a-look-at-precision-recall-and-f1-score-36b5fd0dd3ec

Kaur, R., & Kaur, A. (2012). Digital Forensics. *International Journal of Computer Applications*, *50*(5).

Liu, V., & Brown, F. (2006). Bleeding-Edge Anti-Forensics. *Infosec World Conference & Expo, MIS Training Institute.*

Markova, E., Sokol, P., & Kovacova, K. (2022). Detection of relevant digital evidence in the forensic timelines. *2022 14th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2022*. https://doi.org/10.1109/ECAI54874.2022.9847438

MITRE ATT&CK®. (n.d.). *Impair Defenses: Disable Windows Event Logging, Sub-technique T1562.002 - Enterprise*. Cit 13. apríl 2023, z https://attack.mitre.org/techniques/T1562/002/

Mohamed, A., & Khalid, C. (2021). Detection of suspicious timestamps in NTFS using volume shadow copies. *International Journal of Computer Network and Information Security*, *13*(4). https://doi.org/10.5815/ijcnis.2021.04.06

Montasari, R. (2016). Review and Assessment of the Existing Digital Forensic Investigation Process Models. *International Journal of Computer Applications*, *147*(7). https://doi.org/10.5120/ijca2016911194

Pajek, P., & Pimenidis, E. (2009). Computer anti-forensics methods and their impact on computer forensic investigation. *Communications in Computer and Information Science*, *45*, 145–155. https://doi.org/10.1007/978-3-642-04062-7_16/COVER

Palmbach, D., & Breitinger, F. (2020). Artifacts for Detecting Timestamp Manipulation in NTFS on Windows and Their Reliability. *Forensic Science International: Digital Investigation*, *32*. https://doi.org/10.1016/J.FSIDI.2020.300920

Perlman, A. (2022, január 30). *Anti-Forensics Techniques*. Cynet. Cit. 15. Marec z https://www.cynet.com/attack-techniques-hands-on/anti-forensics-techniques/

Singh, A., Venter, H. S., & Ikuesan, A. R. (2018). Windows registry harnesser for incident response and digital forensic analysis. *Australian Journal of Forensic Sciences*, *52*(3), 337–353. https://doi.org/10.1080/00450618.2018.1551421

svch0st. (2020). *Event Log Tampering Part 2: Manipulating Individual Event Logs*. Medium. https://svch0st.medium.com/event-log-tampering-part-2-manipulating-individual-event-logs-3de37f7e3a85

The Senator Patrick Leahy Center for Digital Investigation. (2015). *Windows 10 Forensics*. http://www.lcdi.champlain.edu

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research*, *17*(2). https://doi.org/10.1080/15614263.2015.1128163

Xu, M., Sun, J., Zheng, N., Qiao, T., Wu, Y., Shi, K., Ge, H., & Yang, T. (2018). A novel file carving algorithm for EVTX logs. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *216*. https://doi.org/10.1007/978-3-319-73697-6_7

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). *Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations*. http://arxiv.org/abs/2103.17028

9 Prílohy

Príloha A: Bakalárska práca v elektronickej podobe, zdrojové kódy k hľadaniu anomálií, k úprave datasetu a k porovnávaniu nájdených anomálií spolu so samotným datasetom v CSV súbore.