D12 – Metóda automatizovaného zberu digitálnych stôp

Projekt Automatizácia digitálnej forenznej analýzy a reakcie na incident (ADFIR) financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09-I05-03-V02-00079.

OBSAH

1 Popis projektu

Projekt **Automatizácia digitálnej forenznej analýzy a odpovede na incident** (ďalej len „**ADFIR**“) je financovaný **Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky** pod číslom projektu č. 09-I05-03-V02-00079. Tento projekt sa zaoberá jednou z kľúčových výziev v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti – ako spracovať obrovské množstvo digitálnych dôkazov, ktoré vznikajú počas incidentov kybernetickej bezpečnosti alebo forenzných vyšetrovaní. V súčasnosti je tento proces veľmi náročný z hľadiska ľudských zdrojov a času. Automatizácia pomocou metód strojového učenia môže preto výrazne **zlepšiť kvalitu digitálnej forenznej analýzy** a skrátiť čas potrebný na jej vykonanie. Celkovo to umožňuje bezpečnostným tímom efektívnejšie reagovať na kybernetické hrozby. Hlavné prínosy tohto projektu sú:

- **Rýchlejšie riešenie incidentov v oblasti kybernetickej bezpečnosti.** Projekt ADFIR zavádza automatizované prístupy k zberu, spracovaniu a analýze digitálnych stôp. Vďaka tomu môžu bezpečnostné tímy rýchlejšie identifikovať príčiny incidentov a prijať účinné opatrenia na ich riešenie.
- **Zníženie pracovnej záťaže forenzných analytikov**. Rutinné a časovo náročné úlohy spojené so spracovaním digitálnych stôp budú nahradené automatizovanými metódami. To umožní analytikom sústrediť sa na zložitejšie prípady a strategické rozhodovanie.
- **Vyššia kvalita a konzistentnosť výstupov.** Použitie jednotných metodík a nástrojov zaručuje, že spracované digitálne stopy budú presnejšie, konzistentnejšie a ľahšie overiteľné. To výrazne znižuje riziko chýb spôsobených ľudskými faktormi.
- **Možné využitie v trestnom konaní**. Výstupy projektu budú vyvinuté v súlade s právnymi požiadavkami a normami, čo umožní, aby digitálne stopy boli akceptované ako relevantné dôkazy pre vyšetrovanie a súdne konania.

2 Úvod

Pracovné balíky (KPB2 – KPB3), ktoré budeme popisovať, odrážajú časť životného cyklu digitálneho spracovania a analýzy dôkazov, začínajúc identifikáciou digitálnych zdrojov dôkazov a zberom digitálnych dôkazov (KPB2), pokračujúc extrakciou digitálnych dôkazov / digitálnych artefaktov dôležitých pre ďalšiu analýzu a reprezentáciu extrahovaných informácií (KPB3). Údaje spracované týmto spôsobom sú vhodné na ďalšiu analýzu používateľmi (digitálnym forenzným analytikom).

V rámci úvodnej fázy riešenia projektu ADFIR sme sa primárne zamerali na konceptualizáciu a detailný návrh metodiky pre tvorbu datasetu a zber forenzných dát. Keďže kvalita vstupných dát je kritická pre následný tréning modelov strojového učenia, hlavným cieľom tohto obdobia bolo zadefinovanie robustných a opakovateľných postupov, ktoré zabezpečia forenznú integritu a konzistenciu budúcich dátových sád. Vytváraná metodika počíta s hybridným prístupom, ktorý bude v realizačnej fáze kombinovať zber dát zo simulovaných útokov v kontrolovanom prostredí s anonymizovanými artefaktmi z reálnej praxe.

Pre proces samotného zberu a spracovania dát navrhujeme a schvaľujeme technologický stack, ktorý kombinuje etablované „industry-standard“ riešenia s internými nástrojmi spoločnosti IstroSec. Metodika zberu bude explicitne definovať využitie nástrojov od Erica Zimmermana (parsery pre forenzné artefakty v OS Windows) pre fázu rýchlej triáže a extrakcie štandardných artefaktov. Kľúčovou pridanou hodnotou navrhovanej metodiky je však integrácia vlastných nástrojov **Gryphon** a **Athena**. Nástroj Gryphon je v metodike určený na zachytávanie telemetrie a behaviorálnych vzorcov na úrovni procesov, zatiaľ čo nástroj Athena bol do procesu zakomponovaný pre potreby špecifickej normalizácie a korelácie dát, čím sme pripravili pôdu pre spracovanie formátov, ktoré bežné nástroje nepokrývajú v dostatočnej hĺbke.

V rámci prípravy metodiky taktiež realizujeme hĺbkovú analýzu a následnú selekciu forenzných artefaktov, ktoré budú tvoriť jadro budúceho datasetu. Tento výber vychádza z mapovania techník útočníkov na framework MITRE ATT&CK. Metodika striktne určuje, že predmetom zberu budú primárne artefakty exekúcie (ShimCache, Amcache, Prefetch), súborového systému (MFT, USN Journal) a perzistencie. Tieto artefakty boli vybrané preto, že podľa našich analýz poskytujú najvyššiu informačnú hodnotu pre plánované algoritmy detekcie anomálií a rekonštrukciu časovej osi incidentov.

Výstupom tejto fázy budú komplexne pripravené a verifikované postupy. Cieľom je presne zadefinovať, **ako** sa budú dáta zbierať, **aké** nástroje sa použijú na zabezpečenie ich integrity a **prečo** sa zameriame na konkrétne typy digitálnych stôp. Týmto vytvoríme nevyhnutný predpoklad pre začatie samotného zberu a generovania dát v ďalšej etape projektu.

3 Úloha KPB2.1

ÚlohaKPB2.1 – Identifikácia forenzných cieľov a ich zdrojov artefaktov, ktoré spĺňajú forenzné ciele na účely potvrdenia alebo vyvrátenia forenznej hypotézy (IstroSec).

V tejto úlohe definujeme ciele forenznej analýzy a určujeme zdroje artefaktov, ktoré sú najužitočnejšie pre dosahovanie cieľov analýzy. Zdroje by mali byť dostatočne robustné a byť nositeľmi takých záznamov, ktoré umožnia potvrdiť alebo vyvrátiť forenznú hypotézu.

3.1 Proces forenznej analýzy

Forenzná analýza ako proces pozostáva z viacerých krokov. Pred tým, ako postúpime k popisu forenzného nástroja, je potrebné si ujasniť, akými krokmi prechádza digitálna stopa počas analytického procesu.

Najznámejším štandardom, ktorý popisuje proces forenznej analýzy, je **NIST SP 800-86 (2006)**.Definuje **4 hlavné fázy**, ktoré uvádzame v
Tab. 1:

Fáza	Slovenský preklad	Kľúčové činnosti, zahrnuté v tejto fáze
Collection	Zber	Identifikácia, označenie, záznam a získavanie dát z relevantných zdrojov pri zachovaní integrity
Examination	Preskúmanie / extrakcia	Forenzné spracovanie získaných dát (dekompresia, vyhľadávanie, extrakcia skrytých dát) s použitím automatizovaných aj manuálnych nástrojov
Analysis	Analýza	Analýza výsledkov preskúmania → odpovede na otázky incidentu (čo, kedy, ako, kto)
Reporting	Správa / reporting	Prezentácia výsledkov (čo bolo nájdené, ako bolo nájdené, význam pre prípad)

Tab. 1 - Fázy procesu forenznej analýzy podľa NIST SP 800-86

NIST explicitne hovorí, že tieto fázy sa môžu prebiehať iteratívne a paralelne. Projekt sa zameriava najmä na druhú a tretiu fázu procesu forenznej analýzy: predspracovanie stôp, extrakcia relevantných dát z artefaktov, spracovanie týchto dát do datasetu použitého v ďalšej fáze projektu. V rámci zberu dát však projekt má presah i do prvej fázy NIST metodiky.

3.2 Hlavné kategórie forenzných artefaktov (Windows) a ich zdroje

Kategória	Typické artefakty a zdroje	Príklad významu

Program Execution	Prefetch, Amcache, Shimcache, UserAssist, Jump Lists, LNK súbory, SRUM, Event Logs (4688/4689)	Ktoré .exe boli spustené, kedy, koľkokrát
Persistence	Run/RunOnce keys, Services, Scheduled Tasks, WMI Event Subscriptions, AppInit_DLLs, Startup folder	Ako sa útočník/malware udržiava na systéme po reštarte
File / Folder Access	Shellbags, LNK + CustomDestinations, OpenSaveMRU, LastVisitedMRU, RecentDocs, Windows 10 Timeline, Thumbcache	Ktoré priečinky a súbory používateľ otváral
USB / External Devices	setupapi.dev.log, registre USBSTOR/USB, Amcache, MountedDevices, Event ID 4663 + 4656 v Security logu	Ktoré USB kľúče boli pripojené a kedy
User Activity	Windows Timeline, SRUDB.dat, TypedPaths, RunMRU, Browser history/cache	Čo používateľ robil, hľadal, písal
Authentication / Logon	Security Event Log (4624, 4625, 4648, 4672), Netlogon.log, LSA secrets	Kto sa prihlasoval, odkiaľ, akým spôsobom, úspešne/neúspešne
Network Activity	DNS cache, BITS logs, PowerShell Operational, Sysmon Event ID 3, Event ID 3 (Microsoft-Windows-NetworkProfile)	Komunikácia so sieťou, C2 servery
Browser Artifacts	Edge/Chrome/Firefox – History, Cookies, Downloads, WebCacheV01.dat, Login Data	Surfovanie, prihlásenia na weby, stiahnuté súbory
System Configuration	Register HKLM\SYSTEM\CurrentControlSet, kľúče BCD, Drivers, Services	Ako je systém nastavený, ktoré ovládače
Anti-Forensics / Timestomping	$MFT $STANDARD_INFORMATION vs $FILE_NAME, Event Log clearing (ID 1102 v Security.evtx), $RecycleBin	Pokusy o zahladenie stôp po prítomnosti útočníka
Memory / Volatile	Obraz pamäte RAM → nástroje Volatility/WinPMEM (hivelist, pslist, netscan, malfind)	Bežiaci malware, injekcie, šifrovacie kľúče
Data Exfiltration	Väčšina vyššie uvedených vie v nejakej miere pomôcť pri identifikácii exfiltrácie dát. Patria sem tiež rôzne logy programov slúžiacich na zdieľanie dát a pod.,	Aké spustiteľné súbory/programy boli v systéme, aké aj bežali, ktoré aplikácie prenášali dáta po sieti, pod akými kontami aktivity prebiehali, či vznikali nejaké väčšie archívne

	ktorým sa v dokumente podrobne nevenujeme.	súbory, čo môže svedčať o stageingu dát pred ich exfiltráciou.
File Presence	Výrazný prienik s vyššie uvedenými kategóriami.	Svedčí o prítomnosti súboru na systéme, či už poskytuje presnú časovú pečiatku, alebo nie.

Tab. 2 - Hlavné kategórie forenzných artefaktov (operačný systém Windows)

Na základe predchádzajúcich riadkov môžeme odvodiť minimálny set dát, ktoré musí byť nástroj schopný zaistiť a spracovať:

1. Všetky *.evtx logy
2. Prefetch priečinok
3. Amcache.hve
4. SRUDB.dat
5. Všetky NTUSER.DAT + UsrClass.dat
6. HKLM kľúče (SYSTEM, SOFTWARE, SAM, SECURITY)
7. %SYSTEMROOT%\appcompat\pca* (Program Compatibility Assistant)
8. Scheduled Tasks + WMI repository
9. $MFT, $LogFile, $UsnJrnl:$J (ak je možné)
10. Pamäťový dump (ak je systém bežiaci)

Tieto zdroje pokryjú s vysokou pravdepodobnosťou väčšinu bežných forenzných otázok (kto, čo, kedy, ako sa to dostalo do systému, čo to robilo, ako pretrváva).

Prirodzene, nástroj vyvíjaný pre komerčné účely by zaisťoval omnoho širšie portfólio dát, ako napríklad údaje o emailových klientoch a obsah poštových schránok, artefakty zanechané nástrojmi pre vzdialený prístup (TeamViewer a množstvo alternatív) či zdieľanie dát v cloude (OneDrive, Google Cloud a podobne). V kontexte nášho projektu je však podstatné definovať set dát umožňujúci vývoj a testovanie analytického modelu. Vytvorený postup by mal byť následne rozšíriteľný o ďalšie zdroje údajov (artefaktov), ich zber, spracovanie a zapojenie do vyhodnocovania.

3.3 Zhrnutie

Uvedené kategórie a artefakty tvoria komplexnú množinu digitálnych stôp na Windows systéme. Pre každý artefakt je potrebné, aby forenzný nástroj:

- **Zbieral** daný súbor alebo kľúč (napr. kopíroval NTUSER.DAT, MFT atď. z live či image).
- **Parsoval** formát (či už ide o textový log, binárny formát, databázu) a extrahoval forenzne významné informácie (časové pečiatky, cesty, mená, hodnoty).
- **Koreloval** ich do kategórií: napr. z Prefetch a Shimcache odvodiť “Execution”, z LNK a Shellbag “File Use”, z Event logov “Login/Remote Access” atď.

Takýto nástroj by umožnil expertom rýchlo získať odpovede na kľúčové otázky vyšetrovania: Čo sa spustilo? Aké súbory užívateľ otvoril? Kedy a kam sa pripájal vzdialene? Aké mal nastavené perzistencie? Čo robil na internete? S kým komunikoval? atď., čím by výrazne zefektívnil digitálnu forenznú analýzu Windows systémov.

V nasledujúcej kapitole budeme pri uvádzaní ciest k artefaktom na disku budeme používať skratky uvedené v Tab. 3.

Skratka	Význam
%SYSTEMROOT%	zodpovedá umiestneniu C:\Windows
%SYSTEMDRIVE%	systémový disk, C:\
%USERPROFILE%	profilový adresár používateľa, C:\Users\<username>
%APPDATA%	priečinok %USERPROFILE%\AppData\Roaming používateľa
HKLM	HKEY_LOCAL_MACHINE registry hive, na offline (vypnutom) systéme jeho obsah reflektujú podporné súbory SAM, SYSTEM, SECURITY v priečinku %SYSTEMROOT%\System32\config
HKCU	HKEY_CURRENT_USER, registrový hive pre aktuálne prihláseného používateľa; offline sa jeho obsah získava z podporného súboru NTUSER.DAT z profilu používateľa, a takisto z podporného súboru USRCLASS.DAT (keďže tento obsahuje dáta z kľúča HKEY_CURRENT_USER\Software\CLASSES)
HKU	HKEY_USERS, registry hivy pre všetkých používateľov na systéme, v offline stave ich obsah reflektujú podporné súbory NTUSER.DAT v profiloch používateľov;
Live a offline	Live zaistenie znamená zaistenie z bežiaceho, zapnutého zariadenia. Offline, alebo post mortem, je pojem, ktorým budeme označovať zaistenie stôp či artefaktov z vypnutého zariadenia či image disku.

Tab. 3 - Zoznam skratiek

3.4 Artefakty spúšťania programov a ich prítomnosti v systéme

3.4.1 Amcache

3.4.1.1 *Popis*

Databáza Application Compatibility, ktorá zaznamenáva detaily o spúšťaných programoch, najmä kedy boli prvýkrát spustené. Objavuje sa na systémoch od OS verzie Windows 8. (Vo Win7 mal obdobnú funkciu súbor RecentFileCache.bcf.) Amcache obsahuje názvy spustiteľných súborov, verzie, SHA-1 haše a časovú pečiatku, ktorá bola v minulosti interpretovaná ako prvý dátum spustenia. Dátum a čas spustenia nie je 100% spoľahlivý. Artefakt stále dokazuje prítomnosť programu v systéme, no časovú pečiatku nemožno brať

ako definitívny dôkaz spustenia programu. Korelácia s inými artefaktami je na mieste, ak chceme dokázať presný čas spustenia programu.

3.4.1.2 *Umiestnenie*

%SYSTEMROOT%\appcompat\programs\Amcache*

3.4.1.3 *Spôsob zaistenia*

Live aj offline.

3.4.1.4 *Primárna kategória*

Execution

3.4.1.5 *Iné kategórie*

File presence

3.4.2 Background Activity Monitor (BAM/DAM)

3.4.2.1 *Popis*

BAM (a podobný DAM) od Win10 1709 sleduje spúšťané aplikácie na úrovni OS background tasks. Pod kľúčom konkrétneho užívateľa (SID) uvádza cestu spustiteľného súboru a posledný dátum/čas spustenia.

3.4.2.2 *Umiestnenie*

Live: HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\<SID>
Offline: SYSTEM\ControlSet*\Services\bam\State\UserSettings\<SID>

3.4.2.3 *Spôsob zaistenia*

Live aj offline.

3.4.2.4 *Primárna kategória*

Execution

3.4.2.5 *Iné kategórie*

User Activity

3.4.3 MUICache

3.4.3.1 *Popis*

Pri GUI spustení aplikácie cez Windows Explorer si Windows ukladá lokalizovaný názov aplikácie do tzv. MUICache. Prítomnosť záznamu indikuje, že daný program bol spustený daným používateľom (hoci bez časovej pečiatky).

3.4.3.2 *Umiestnenie*

HKCU\Software\Classes\LocalSettings\Software\Microsoft\Windows\Shell\MuiCache (v UsrClass.DAT užívateľa)

3.4.3.3 *Spôsob zaistenia*

Live aj offline.

3.4.3.4 *Primárna kategória*

Execution

3.4.3.5 *Iné kategórie*

File presence, User activity

3.4.4 Prefetch

3.4.4.1 *Popis*

Súbory Windows Prefetch sa vytvárajú na optimalizáciu spustenia aplikácie v systéme Windows. Tieto súbory obsahujú počet spustení pre každú aplikáciu, od jednej do ôsmich časových pečiatok posledných spustení a záznam všetkých súborov otvorených počas nastaveného obdobia po spustení aplikácie.

Prefetch súbory –Windows vytvára *.pf súbory pri spustení executables. Ako spomíname vyššie, PF súbory obsahujú časové pečiatky posledných až 8 spustení programu a zoznam načítaných DLL/súborov. Prefetch slúži ako silný dôkaz spustenia programu (ak nie je vypnutý, napr. na serveroch alebo SSD systémoch môže byť defaultne off).

3.4.4.2 *Umiestnenie*

%SYSTEMROOT%\Prefetch*
(tj %SYSTEMROOT%\Prefetch*.pf)

3.4.4.3 *Spôsob zaistenia*

Live aj offline.

3.4.4.4 *Primárna kategória*

Execution

3.4.4.5 *Iné kategórie*

-

3.4.5 RecentApps

3.4.5.1 *Popis*

Zaznamenáva naposledy spustené aplikácie (najmä UWP a moderné apps). Každý záznam potvrdzuje spustenie programu daným užívateľom.

3.4.5.2 *Umiestnenie*

HKCU\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps (Win10+)

3.4.5.3 *Spôsob zaistenia*

Live aj offline.

3.4.5.4 *Primárna kategória*

Execution

3.4.5.5 *Iné kategórie*

User Activity

3.4.6 Recentfilecache

3.4.6.1 *Popis*

Binárny súbor RecentFileCache.bcf je cache nedávno spúšťaných EXE súborov (najmä v systémoch, kde nie je Prefetch alebo pre inštalačné súbory). Obsahuje zoznam ciest k spúšťaným súborom a základné metaúdaje. Pre forenznú analýzu je užitočný pri určovaní, či a ktoré binárky boli spustené, najmä ak Prefetch nie je dostupný alebo je vypnutý.

Typ/atribúty: Binárny formát BCF. Každý záznam obsahuje cestu k EXE súboru a

pravdepodobne timestamp (čas poslednej modifikácie súboru). Napr. záznam môže vyzerať: C:\Temp\malware.exe – timestamp 2025-06-01.... Významné je, že ak sa súbor objaví v tomto zozname, bol spustený (či už ručne alebo v rámci inštalácie).

3.4.6.2 *Umiestnenie*

%SYSTEMROOT%\AppCompat\Programs\RecentFileCache.bcf (iba na Windows 7)

3.4.6.3 *Spôsob zaistenia*

Skopírovanie z disku. Live aj offline.
Nástroje: *RecentFileCache Parser* (napr. z *Eric Zimmerman* nástrojov alebo *FireEye's RecentFileCacheParser*) dokáže dekódovať .bcf do čitateľného CSV. Tiež *KAPE* (target **EvidenceOfExecution** ho obsahuje).

3.4.6.4 *Primárna kategória*

Execution

3.4.6.5 *Iné kategórie*

File Presence

3.4.7 RunMRU

3.4.7.1 *Popis*

Záznamy príkazov spúšťaných cez dialóg Win+R (Run). Ukladá históriu príkazov/exe, ktoré používateľ spustil ručne cez „Spustiť" – „Run".

3.4.7.2 *Umiestnenie*

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

3.4.7.3 *Spôsob zaistenia*

Live aj offline.

3.4.7.4 *Primárna kategória*

Execution

3.4.7.5 *Iné kategórie*

User Activity

3.4.8 Shimcache

3.4.8.1 *Popis*

Cache kompatibility aplikácií ukladaná v **System** hive. Obsahuje zoznam 1024 nedávno spustených **alebo prístupných** spustiteľných súborov s ich cestou a časovou pečiatkou poslednej modifikácie spustiteľného súboru v čase jeho spustenia (to jest, nie samotný čas spustenia, a od Windows 10 neindikuje ani to, či súbor vôbec spustený bol![1]). **Pozor – zapísaná je do registrov až pri vypnutí OS a nemusí znamenať *skutočné* spustenie (stačí napr. otvoriť priečinok s EXE).**

3.4.8.2 *Umiestnenie*

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache

3.4.8.3 *Spôsob zaistenia*

Live aj offline. Live z pamäte RAM, pretože do registra sa zmeny zaznamenajú až pri reboote zariadenia, dovtedy sú iba v pamäti.

3.4.8.4 *Primárna kategória*

Historicky sa zaraďuje do Execution, v skutočnosti viac zodpovedá File Presence.

3.4.8.5 *Iné kategórie*

-

3.4.9 SRUM: System Resource Usage Monitor

3.4.9.1 *Popis*

Databáza uchovávajúca informácie o využití systémových prostriedkov. Údaje z nej čerpá napríklad nástroj Task Manager.

Databáza SRUM (ESE DB) bola zavedená vo Win8 a sleduje rôzne štatistiky o behu aplikácií – napr. kedy a ako dlho boli procesy spustené, objemy prenesených dát po sieti na proces, spotreba batérie atď. Dá sa z nej zistiť časová os behu aplikácií (v 60-min intervaloch) a sieťová

[1] https://artefacts.help/windows_shimcache.html

aktivita procesov. Môže obsahovať aj záznam o používateľovi, pod ktorého kontom tá-ktorá aplikácia bežala.

- Application Resource Usage

Tabuľka v databáze System Resource Usage, ktorá uchováva štatistiky využívania systémových zdrojov jednotlivými aplikáciami.

- Network Connectivity Usage

Tabuľka v databáze využitia systémových zdrojov, ktorá uchováva štatistiky týkajúce sa sieťových pripojení. Konkrétne obsahuje čas spustenia a trvanie pripojení na každé sieťové rozhranie.

- Network Data Usage

Tabuľka v System Resource Usage databáze, ktorá ukladá štatistiky týkajúce sa využitia sieťových dát na spustenie aplikácií. Zahŕňa cestu k aplikácii, sieťové rozhranie, odoslané bajty a prijaté bajty.

3.4.9.2 *Umiestnenie*

%SYSTEMROOT%\System32\sru\SRUDB.dat

3.4.9.3 *Spôsob zaistenia*

Skopírovanie databázového súboru, ideálne s celým priečinkom. Live aj offline.

3.4.9.4 *Primárna kategória*

Execution

3.4.9.5 *Iné kategórie*

Data Exfiltration, User Activity

3.4.10 UserAssist

3.4.10.1 *Popis*

Kľúč UserAssist sleduje spúšťanie GUI aplikácií používateľom. Názvy sú ROT13-kódované; obsahuje počítadlo spustení a posledný čas spustenia pre každý program spustený cez GUI. Poskytuje stopy o tom, čo používateľ spúšťal a kedy. Môže byť vynulovaný po významnejšej aktualizácii systému.

3.4.10.2 *Umiestnenie*

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count
Na vypnutom systéme a pre neprihlásených používateľov nahrádzame HKEY_CURRENT_USER registrami NTUSER.DAT.

3.4.10.3 *Spôsob zaistenia*

Live aj offline.

3.4.10.4 *Primárna kategória*

Execution

3.4.10.5 *Iné kategórie*

User Activity

3.4.11 Windows Activities – W10 Timeline

3.4.11.1 *Popis*

Windows Timeline (ActivitiesCache.db) je databáza zavedená vo Windows 10 v. 1803 (funkcia Timeline). Ak je timeline povolená, zapisuje aktivity používateľa, potenciálne aj naprieč viacerými zariadeniami: otvorenie dokumentu, webovej stránky, spustenie aplikácie, a to aj s časom začiatku a konca aktivity. Každá aktivita má AppID (napr. Word, Excel, Edge) a často aj názov súboru alebo URL. Je to zlatá baňa pre forenznú analýzu – dá sa z nej vyčítať, že napr. 10. mája 2023 o 14:30 užívateľ otvoril súbor C:\Docs\Tajný.xlsx v Exceli a o 14:55 ho zatvoril. Uchováva záznamy maximálne za posledných 30 dní.
Poznámka: vo Windows 11 už nebude obsahovať signifikantné dáta.

3.4.11.2 *Umiestnenie*

%USERPROFILE%\AppData\Local\ConnectedDevicesPlatform\L.*\ActivitiesCache.db*

3.4.11.3 *Spôsob zaistenia*

Live aj offline.

3.4.11.4 *Primárna kategória*

Execution

3.4.11.5 *Iné kategórie*

User Activity, File Open, Web browsing

3.5 Artefakty perzistencie

3.5.1 DNS Hosts File

3.5.1.1 *Popis*

Záznamy z etc\hosts file. Modifikácia tohto súboru môže útočníkovi pomôcť k zaisteniu perzistencie.

3.5.1.2 *Umiestnenie*

%SYSTEMROOT%\System32\drivers\etc\hosts

3.5.1.3 *Spôsob zaistenia*

Live aj offline.

3.5.1.4 *Primárna kategória*

Persistence

3.5.1.5 *Iné kategórie*

-

3.5.2 Registry Persistence

3.5.2.1 *Popis*

Kolekcia kľúčov databázy Registry, ktoré možno použiť na zaistenie perzistencie škodlivého softvéru.

Run kľúče - HKLM\Software\Microsoft\Windows\CurrentVersion\Run (a RunOnce, …) a podobne HKCU\Software\Microsoft\Windows\CurrentVersion\Run – Kľúče "Run" obsahujú zoznam programov, ktoré sa majú automaticky spustiť pri štarte systému (HKLM pre všetkých užívateľov) alebo pri prihlásení konkrétneho užívateľa (HKCU). Hodnota je cesta k .exe alebo skriptu. Ak forenzný nástroj nájde položku v Run, znamená to, že daný program sa spúšťal perzistentne pri štarte.

AppInit_DLLs – Cesta (v registri): HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs a AppInit_DLLs hodnota – Ak je povolené, DLL uvedené v AppInit_DLLs sa načítajú do každého procesu využívajúceho User32.dll. Toto je starší persistence mechanizmus (dnes menej používaný, v novších Windows default off alebo obmedzený podpisom). Napriek tomu, ak tam nejaká hodnota je, značí to snahu injektovať kód do procesov.

Winlogon Shell / Userinit – Cesta (v registri): HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell a Userinit – Normálne má Shell hodnotu *explorer.exe*. Ak útočník nastaví Shell na iný spustiteľný súbor, spustí sa namiesto Exploreru po prihlásení (**prípadne spolu s Explorerom**, ak tam pridá „Explorer.exe, malware.exe"). Podobne Userinit default %SYSTEMROOT%\system32\userinit.exe, ak je modifikovaný (napr. pridá cestu k malwaru), spustí sa ten pri logone.

3.5.2.2 *Umiestnenie*

HKEY_USERS*\Software\Microsoft\Windows\CurrentVersion\Run*
HKEY_USERS*\Software\Microsoft\Windows\CurrentVersion\RunOnce*
HKEY_USERS*\Software\Microsoft\Windows\CurrentVersion\RunServices*
HKEY_USERS*\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run*
HKEY_USERS*\Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run*
HKEY_USERS*\Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce*
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run*
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce*
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices*
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run*
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run*
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce*
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components**
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\BootExecute

3.5.2.3 *Spôsob zaistenia*

Reg save pre live, offline zachytenie je samozrejme možné tiež.

3.5.2.4 *Primárna kategória*

Persistence

3.5.2.5 *Iné kategórie*

Execution, User Activity

3.5.3 Scheduled Tasks

3.5.3.1 *Popis*

Naplánované úlohy sa používajú na spúšťanie programov alebo skriptov systému Windows v určených intervaloch. Plánované úlohy predstavujú mechanizmus perzistencie – umožňujú spustiť skript/program pri štarte, prihlásení, alebo v plánovaných intervaloch. Malware často vytvára vlastnú Scheduled Task na pretrvanie po reštarte. Analýza obsahu Tasks\ odhalí meno úlohy, časové spúšťače a najmä **cestu k spúšťanému programu alebo príkazu**. Tento artefakt je kľúčový pri hľadaní persistentných *backdoorov* a automatizovaných aktivít. Napr. úloha s názvom "Windows Update Service" spúšťajúca *C:\Temp\evil.exe* pri logone poukazuje na perzistenciu útočníka.

- **Cesta:** XML súbory v %SYSTEMROOT%\System32\Tasks\ – Každá úloha plánovača (Task Scheduler) je reprezentovaná XML súborom. Dôležité sú tie, ktoré spúšťajú nejaké .exe na určitý trigger (pri štarte, pri logone, alebo periodicky). Okrem toho, nastavenia úloh sú aj v registri pod HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\. Forenzná analýza odhalí názov úlohy, spúšťaný príkaz/program, podmienky spustenia a naposledy spustené časy. Útočníci často vytvárajú skryté úlohy pre perzistenciu.
- **Scheduled Tasks Events** – V logu **Microsoft-Windows-TaskScheduler/Operational** sú eventy **ID 200 a 201**, ktoré indikujú spustenie a ukončenie úlohy plánovača. Ak malware alebo admin vytvoril Scheduled Task na spúšťanie .exe, nasledovné udalosti v logu Security.evtx odhalia kedy a čo sa spustilo.
    - **4698:** A scheduled task was created.
    - **4699:** A scheduled task was deleted.
    - **4700:** A scheduled task was enabled.
    - **4701:** A scheduled task was disabled.
    - **4702:** A scheduled task was updated (modified)

- **Nástroje:** *KAPE* target **ScheduledTasks** (zbiera .job aj .xml). Parsovanie .job súborov je možné nástrojom *jf.exe* (Job File parser) alebo *TZworks silentrunner*. XML úlohy sa dajú čítať priamo (obsahujú v XML tagoch definíciu triggerov a akcí). Taktiež Sysinternals **Autoruns** zobrazí väčšinu naplánovaných úloh.

Typ/atribúty naplánovaných úloh:

- *.job* (binar.): obsahuje názov úlohy, plán (dátum/čas spustenia) a príkaz + parametre.
- *.xml*: obsahuje sekciu <Actions> (s príkazom napr. <Exec><Command>C:\path\program.exe</Command>), sekciu <Triggers> (kedy sa spúšťa – napr. AtLogon) a <Principals> (pod akým užívateľom). **Kľúčové atribúty:** *TaskName*, *TriggerType* (Startup/Logon/Daily/etc.), *ActionPath* (cesta k exe alebo skriptu), *Arguments*. Z týchto údajov viete identifikovať škodlivú úlohu a čo presne spúšťa.

3.5.3.2 *Umiestnenie*

- %SYSTEMROOT%\Tasks*.job - legacy .job formát
- %SYSTEMROOT%\System32\Tasks* - XML súbory s detailnými nastaveniami
- HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Schedule\TaskCache
- Event Logs: Microsoft-Windows-TaskScheduler/Operational (ID 106, 200–201)

3.5.3.3 *Spôsob zaistenia*

Live aj offline.
Pripájame príklady, ako sa dá na tento účel využiť PowerShell.

```
Get-ScheduledTask
gci -path C:\windows\system32\tasks -recurse | Select-String Command | FL Filename, Line
gci -path C:\windows\system32\tasks -recurse | Select-String "<Command>",Argument | FT
Filename,Command,Line
gci -path C:\windows\system32\tasks -recurse | Select-String Command | ? {$_.Line -match
"MALICIOUSNAME"} | FL Filename, Line
(gci -path C:\windows\system32\tasks -recurse | Select-String "<Command>" | select -exp
Line).replace("<Command>","").trim("</Command>").replace("`"","").trim();
gci 'REGISTRY::HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree' -rec -force | ?{$_.Property -notcontains 'SD'}
gci 'REGISTRY::HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree' -rec -force | Get-ItemProperty |
?{$_.SD.length -lt 100}
```

3.5.3.4 *Primárna kategória*

Perzistence

3.5.3.5 *Iné kategórie*

Execution, File Presence

3.5.4 Services

3.5.4.1 *Popis*

Služby sú aplikácie systému Windows, ktoré je možné spustiť bez interakcie používateľa – niečo ako daemony v UNIX/Linux OS. Služby možno použiť ako metódu perzistencie malvéru.

- **Cesta (v registri):** HKLM\SYSTEM\CurrentControlSet\Services\<ServiceName> – Všetky systémové služby sú v tomto kľúči. Ak útočník pridá malvérovú službu, objaví sa tu. Dôležité polia: **ImagePath** (cesta k spúšťanému .exe alebo .dll), **Start** typ (či štartuje automaticky). Eventuálne event log **System** (7045) indikuje inštaláciu novej služby. Pre každú službu tu môže byť evidované, kedy bežala (Log events 7035/7036 ako spomenuté vyššie).

3.5.4.2 *Umiestnenie*

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*

3.5.4.3 *Spôsob zaistenia*

Live aj offline.

3.5.4.4 *Primárna kategória*

Persistence

3.5.4.5 *Iné kategórie*

Execution

3.5.5 Shim Databases

3.5.5.1 *Popis*

Databázy používané infraštruktúrou kompatibility aplikácií na použitie "shims" na spustiteľné súbory pre spätnú kompatibilitu. Tieto databázy možno použiť na vloženie škodlivého kódu do legitímnych procesov a udržanie perzistencie na koncovom bode.

3.5.5.2 *Umiestnenie*

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB*

3.5.5.3 *Spôsob zaistenia*

Live aj offline.

3.5.5.4 *Primárna kategória*

Persistence

3.5.5.5 *Iné kategórie*

Execution

3.5.6 Windows Drivers files

3.5.6.1 *Popis*

Vhodné pre krížovú referenciu s registrovým kľúčom Services. **Drivers (Ovládače)** sú tiež služby (typ=1 v registri). Škodlivé rootkity môžu pridávať ovládače. Artefakt pre ovládače v registroch je preto rovnaký ako v prípade Windows služieb – kľúče Services. Ak sa v adresári %SYSTEMROOT%\System32\drivers\ nachádzajú podozrivé .sys súbory a majú registráciu v Services, ide o perzistenciu na úrovni kernelu.

3.5.6.2 *Umiestnenie*

%SYSTEMROOT%\System32\drivers*.sys

3.5.6.3 *Spôsob zaistenia*

Live aj offline.

3.5.6.4 *Primárna kategória*

Persistence

3.5.6.5 *Iné kategórie*

-

3.5.7 WMI Repository

3.5.7.1 *Popis*

Zoznam WMI EventConsumers a akýchkoľvek EventFilterov, ktoré sú k nim pripútané prostredníctvom FilterToConsumerBinding. WMI EventConsumers môžu byť použité ako metóda bezsúborovej (fileless) perzistencie malvéru. Takisto zaisťujeme WMI objekty (.mof súbory) a WMI event log.

- **WMI Event Subscription** – Windows Management Instrumentation môže byť zneužité na perzistenciu cez tzv. Event Subscriptions. Artefakty sa ukladajú v WMI repozitári

(MOF databáza). Pomocou nástrojov (napr. PowerShell Get-WmiObject -Namespace root\subscription) sa dajú nájsť **Consumer** a **Filter** nastavenia, ktoré spúšťajú príkazy pri určitých udalostiach (napr. pri logone). V registri to priamo nie je textovo vidno, ale WMI-Activity Operational log (Microsoft-Windows-WMI-Activity/Operational) môže obsahovať eventy, ak sa WMI triggery vykonali.

- **WMI Persistence (MOF súbory)**
  Cesta: %SYSTEMROOT%\System32\wbem\mof*.mof (prípadne subfolder *...\wbem\mof\en-US* pre lokalizované)

  Perzistencia cez WMI využíva tzv. **Permanent Event Subscriptions** – nastavenia vo WMI, ktoré môžu spúšťať kód pri udalostiach (napr. pri štarte systému). Tieto nastavenia sa dajú zapísať aj cez .MOF (Managed Object Format) súbory – ak sú uložené v wbem\mof\ priečinku, WMI ich automaticky načíta a zaregistruje. Útočníci takto vytvárajú perzistentné *WMI Event Consumer* a *Filter*, ktoré napr. spustia príkaz vždy pri bootovaní. Pre forenznú analýzu je detekcia neznámych .mof súborov alebo nečakaných WMI Event Consumerov kritická.

  Samotné MOF súbory sú textové (môžu byť zmazané po načítaní).

  KAPE (target **MOF** ak existuje) vie skopírovať *.mof. Ďalej priamo *PowerShell (Get-WMIObject __EventFilter)* alebo **Autoruns** (položka WMI). Existujú aj špecializované skripty, napr. *WMIPersist vbs* skript na výpis WMI permanent eventov.

  Typ/atribúty: .mof skript – text definujúci WMI triedy. Typicky obsahuje inštancie __EventFilter, CommandLineEventConsumer a __FilterToConsumerBinding. Kľúčový je atribút **CommandLineTemplate** v *EventConsumer*, ktorý prezrádza, aký príkaz/program sa spustí. Taktiež *Name* a *Query* vo *EventFilter* (napr. filter typu SELECT * FROM __InstanceModificationEvent ... spúšťaný pri štarte). Pri analýze WMI perzistencie hľadáme príkazy, cesty k spúšťaným súborom alebo skriptom, a neštandardné názvy consumerov.

3.5.7.2 *Umiestnenie*

%SYSTEMROOT%\System32\wbem\Repository\OBJECTS.DATA
%SYSTEMROOT%\System32\wbem\Repository\FS\OBJECTS.DATA
%SYSTEMROOT%\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4Operational.evtx
%SYSTEMROOT%\System32\wbem\mof*.mof (alebo podpriečinok *...\wbem\mof\en-US* alebo iný, kvôli lokalizácií)

3.5.7.3 *Spôsob zaistenia*

Live alebo offline

3.5.7.4 *Primárna kategória*

Persistence

3.5.7.5 *Iné kategórie*

Execution

3.6 Artefakty používateľskej aktivity

3.6.1 Browser History

3.6.1.1 *Popis*

Browser history z Chrome, Edge, Firefox, a Internet Explorer. Vzhľadom na variabilitu upravíme formát tejto sekcie.

Artefakty spojené s prehliadaním webu – história návštev stránok, stiahnuté súbory, cookies, atď. Každý prehliadač má vlastné úložiská, často vo forme databáz.

3.6.1.2 *Internet Explorer / Edge Legacy (IE10-11, Legacy Edge)*

- História, cookies a cache sú uložené v spoločnej ESE databáze **WebCacheV01.dat**: **Cesta:** %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat. Táto databáza (Extensible Storage Engine) obsahuje tabuľky **Container_#** pre navštívené URL, History, Cookies, Cache a pod.. Každý záznam histórie obsahuje URL, názov stránky, čas návštevy (v tzv. FILETIME/GUID formáte v lokálnom čase). Cookies tabuľka obsahuje cookies s atribútmi. **Downloads** sú tiež evidované v histórii.
    - Forenzne: WebCacheV01.dat odhalí **všetky weby, ktoré užívateľ navštívil v IE alebo starom Edge**, s časom a dokonca, ak je MS účet nastavený ako roaming, môže obsahovať históriu aj z iných zariadení. Cookies môžu prezradiť prihlasovacie relácie (napr. cookie k banke).
- **Session Recovery**: %USERPROFILE%\AppData\Local\Microsoft\Internet Explorer\Recovery\ a pre Edge Legacy v priečinku ...MicrosoftEdge\User\Default\Recovery\Active\ – obsahuje snaphoty otvorených tabs (URL) pre prípad obnovy po páde.
- **IE TypedURLs**: HKCU\Software\Microsoft\Internet Explorer\TypedURLs – zoznam URL adries, ktoré užívateľ ručne zadal do adresného riadka IE (top 25).

3.6.1.3 *Microsoft Edge (Chromium, v79+)*

- Nový Edge (ako aj Google Chrome) používa chromium core, takže rovnakú štruktúru dát. **Cesta profilov:** %USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\Default\ (alebo iný profil). Tu je:
    - History – SQLite databáza s tabuľkou urls (obsahuje URL, title, počet návštev, čas poslednej návštevy v Unix epoch mikrosekundách).
    - Cookies – SQLite DB (alebo od určitej verzie .sqlite alebo .ldb súbory), s host, name, value, last access.
    - Cache – súbory cache na disku v Cache\ priečinku.
    - Downloads – záznamy o stiahnutých súboroch (v History DB alebo separate History-journal).
    - Session Storage & Local Storage – v podpriečinku Default\Local Storage\leveldb\ alebo Default\Network atď (we **WebStorage** viď nižšie).
    - **WebStorage (Local Storage & IndexedDB)**: Moderné prehliadače (Chrome, Edge) využívajú WebStorage – lokálne uložené dáta web aplikácií. Tieto sú vo forme súborov (LevelDB databáz) v profile pod ...\Default\Local Storage\ a IndexedDB\. Napr. chatovacie webapky (Slack web) môžu ukladať históriu v LocalStorage. SANS výskum zdôrazňuje, že **WebStorage uchováva obrovské množstvo dát** (až GB) o aktivite na webových službách, často viac než klasická cache.
    - *Forenzne:* Z Edge/Chrome histórie sa dá zrekonštruovať, aké stránky užívateľ navštívil a kedy (napr. konkrétnu URL na cloud úložisku, internet banking, sociálnu sieť). Cookies pomôžu identifikovať prihlásenia k webovým službám (napr. ak tam je session cookie k Gmailu). LocalStorage môže obsahovať čety (napr. správy zo Slacku či Teams, ak bežali vo web prostredí).

3.6.1.4 *Google Chrome*

- **Cesta profilu:** %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\ – štruktúra je analogická ako Edge (History, Cookies SQLite atď). **History** súbor je SQLite DB s prehľadom URL.
- **Downloads:** v History DB tabuľka downloads alebo v samostatnom súbore DownloadMetadata.
- **Login Data:** SQLite DB s uloženými heslami (šifrované DPAPI).
- *Treba uviesť,* že Chrome taktiež používa WebStorage rovnako, ako MS Edge.

3.6.1.5 *Mozilla Firefox*

- **Profilová cesta:** %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<profil>\ – Hlavná DB je places.sqlite (SQLite) – obsahuje **history** (tabuľky moz_places a moz_historyvisits) a

bookmarks. places.sqlite uchováva URL navštívených stránok aj so timestampom (unix epoch v mikrosek.) a počtom návštev.

- **Downloads:** Firefox taktiež zapisuje stiahnuté súbory do places.sqlite (moz_annos table) a do súboru downloads.sqlite (vo starších verziach).
- **Cookies:** cookies.sqlite – SQLite DB s cookies (name, value, host, lastAccessed).
- **Session restore:** sessionstore.jsonlz4 – komprimovaný JSON s informáciou o otvorených paneloch (adresy URL), ak mal užívateľ niečo otvorené pred zatvorením prehliadača.

3.6.1.6 *Iné*

- **Safari pre Windows** (už nepodporované, ale staršie inštalácie): používalo SQLite databázy History.db atď v %APPDATA%\Apple Computer\Safari\. Pravdepodobne netreba, okrajový prípad.
- **WebCache / Index.dat (IE <10)** – Pre úplnosť, ak by Windows 7 mal IE8/9: starý IE používal skryté súbory index.dat v profile (History, Cookies, Cache). Tie sa dajú parsermi extrahovať. Na Windows 7 však IE11 už používa WebCacheV01.dat.
- **Aplikácie postavené na Chrome (Electron)** – **Dôležité:** Moderné desktopové aplikácie ako Skype for Desktop, Slack, WhatsApp Desktop, Signal, Discord, Teams atď sú často postavené na Electron (Chromium) a **ukladajú dáta podobne ako prehliadač**. Tzn. v ich AppData priečinkoch nájdeme **Local Storage** (LevelDB) a prípadne históriu ak ide o integrovaný prehliadač.
    - Napr. **Slack** (desktop) používa Chrome WebStorage na cache správ (to isté platí pre Teams). Preto vo forensic analýze web storage netreba hľadať len prehliadačové domény, ale aj dáta týchto app (napr. https://app.slack.com local storage môže byť aj v prehliadači, alebo v Electron priečinku Slacku).

Pre potreby automatizačného nástroja ešte spomeňme, že vzhľadom na vyššie popísané skutočnosti by mal vedieť parsovať hlavné formáty – SQLite DB (Chrome, Firefox), ESE DB (WebCacheV01.dat), LevelDB (LocalStorage), JSONLZ4 (Firefox session), a extrahovať históriu URL, cookies, downloads atď.

3.6.1.7 *Primárna kategória*

User activity

3.6.1.8 *Iné kategórie*

Execution, file presence, data exfiltration

3.6.2 ComDlg32/CidSizeMRU

3.6.2.1 *Popis*

Registrový kľúč, ktorý obsahuje zoznam nedávno spustených aplikácií. Aplikácia využíva funkciu Common Dialog Box, teda umožňuje používateľovi pomocou dialógového okna Windows Prieskumníka otvoriť či uložiť súbor. Príkladom sú napríklad kancelárske aplikácie umožňujúce cez Súbor... tlačidlo pristupovať k rôznym takýmto funkciám.

3.6.2.2 *Umiestnenie*

HKEY_USERS*\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU

3.6.2.3 *Spôsob zaistenia*

Live aj offline.

3.6.2.4 *Primárna kategória*

User Activity

3.6.2.5 *Iné kategórie*

Execution

3.6.3 ComDlg32/LastVisitedPidlMRU

3.6.3.1 *Popis*

Registrový kľúč obsahujúci zoznam aplikácií a ciest k priečinkom, ktoré sú asociované s nedávno otvorenými súbormi v používateľovom OpenSavePidlMRU kľúči.

3.6.3.2 *Umiestnenie*

HKEY_USERS*\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU
HKEY_USERS*\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRULegacy

3.6.3.3 *Spôsob zaistenia*

Live aj offline.

3.6.3.4 *Primárna kategória*

User Activity

3.6.3.5 *Iné kategórie*

Execution

3.6.4 ComDlg32/OpenSavePidlMRU

3.6.4.1 *Popis*

Kľúč databázy Registry obsahujúci zoznam naposledy otvorených a uložených súborov pre dané používateľské konto.
Open/Save MRU (ComDlg32) – **Cesta (v registri):**
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU – Ukladá cesty súborov a priečinkov, ktoré používateľ vyberal v štandardných dialógových oknách „Otvoriť/Uložiť ako“. Taktiež LastVisitedPidlMRU uchováva posledné navštívené priečinky v dialógoch. Tieto kľúče indikujú, s akými súbormi užívateľ pracoval cez aplikácie (napr. naposledy otvorený súbor v prehrávači, naposledy uložený dokument v Office, atď.).

3.6.4.2 *Umiestnenie*

HKEY_USERS*\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU

3.6.4.3 *Spôsob zaistenia*

Live aj offline

3.6.4.4 *Primárna kategória*

User Activity - File Open

3.6.4.5 *Iné kategórie*

-

3.6.5 EventTranscript.db

3.6.5.1 *Popis*

Tento artefakt sa na systéme nevytvára by default! Ale ak na systéme je, môže obsahovať obrovské množstvo dát o aktivite na zariadení.

Od Win 10, 01/2021

- EventTranscript.db je SQLite databáza umiestnená v lokalite: C:\ProgramData\Microsoft\Diagnosis\EventTranscript\EventTranscript.db

Obsahuje 7 tabuliek v rámci databázy SQLite:

- categories
- event_categories
- event_tags
- events_persisted
- producers
- provider_groups
- tag_descriptions

Zaznamenáva šesť (6) rôznych typov udalostí s nasledujúcimi označeniami:

- História prehliadania: Záznamy histórie prehliadania webu pri používaní funkcií aplikácie alebo cloudovej služby, uložené v službe alebo aplikácii
- Pripojenie a konfigurácia zariadenia: údaje, ktoré popisujú pripojenia a konfiguráciu zariadení pripojených k službe a sieti vrátane identifikátorov zariadení (napr. IP adries), konfigurácie, nastavenia a výkonu
- Písanie rukou a reč: Záznam vstupných údajov poskytnutých koncovým používateľom prostredníctvom metódy interakcie alebo akcie, ako je písanie rukou, písanie na klávesnici, reč alebo gestá
- Výkonnosť produktov a služieb: Zhromaždené údaje o meraní, výkone a prevádzke schopností produktu alebo služby. Tieto údaje predstavujú informácie o schopnosti a jej použití so zameraním na poskytovanie schopností produktu alebo služby.
- Používanie produktov a služieb: Údaje poskytnuté alebo zachytené o interakcii koncového používateľa so službou alebo produktmi poskytovateľom cloudových služieb. Zaznamenané údaje zahŕňajú záznamy o preferenciách a nastaveniach koncového používateľa pre možnosti, použité možnosti a príkazy poskytnuté schopnostiam.
- Nastavenie a inventár softvéru: Údaje, ktoré popisujú inštaláciu, nastavenie a aktualizáciu softvéru.

3.6.5.2 *Umiestnenie*

- C:\ProgramData\Microsoft\Diagnosis\EventTranscript\EventTranscript.db

3.6.5.3 *Spôsob zaistenia*

Live aj offline

3.6.5.4 *Primárna kategória*

User Activity

3.6.5.5 *Iné kategórie*

-

3.6.6 JumpLists

Od Windows 7 sa v OS Windows používajú Jump Listy: ide o súbory *.automaticDestinations-ms *.customDestinations-ms ktoré pre každú aplikáciu uchovávajú zoznam naposledy otváraných súborov v danej aplikácii a/alebo zoznam posledných akcií, ktoré sa s aplikáciou vykonali (napríklad otvorenie RDP session pomocou Remote Desktop klienta, alebo otvorenie okna webového prehliadača v privátnom režime).

Napr. JumpList pre MS Word bude obsahovať zoznam naposledy otvorených .docx. Tieto záznamy indikujú **videnie alebo otvorenie** konkrétnych súborov užívateľom a s akou aplikáciou.
Pre forenznú analýzu poskytujú dôkaz otvorenia konkrétnych súborov používateľom (napr. posledných N dokumentov MS Word, PDF v Adobe Readeri a pod.) aj v prípade, že samotné súbory už neexistujú.

Typ/atribúty: Binárny formát (.ms súbory). Každá položka obsahuje cestu k nedávno otvorenému súboru a dátum/čas (napr. LastModified v jump liste).

Atribúty: AppID (identifikuje aplikáciu, napr. identifikačný string v názve súboru jump listu), FilePath otvoreného súboru, LastAccessTime. Tieto informácie umožňujú povedať ktorý súbor bol otvorený v ktorom programe a kedy naposledy.

Nástroje: KAPE target LNKFilesAndJumpLists (zbiera .automaticDestinations-ms aj .customDestinations-ms). Na parsovanie sa používa JumpList Explorer (JLECmd) od Eric Zimmermana alebo nástroje ako ShellBags & JumpLists Parser. Tie extrahujú zoznam súborov, čas posledného otvorenia a identifikátor aplikácie.

3.6.6.1 *Spôsob zaistenia*

Live aj offline, na parsovanie je možné použiť nástroje Erica Zimmermana JumpListExplorer a JLECmd.

3.6.6.2 *Umiestnenie*

AutomaticDestinations:
%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\<APP_ID>.automaticDestinations-ms

CustomDestinations:
%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\<APP_ID>.customDestinations-ms

3.6.6.3 *Primárna kategória*

User Activity

3.6.6.4 *Iné kategórie*

Execution

3.6.7 RecentDocs

3.6.7.1 *Popis*

Obsahuje zoznam naposledy otváraných súborov rôznych typov (člení sa podľa prípony). U každého súboru ukladá názov a posledný otvorený čas. Napríklad podkľúč .docx obsahuje naposledy otvorené Word dokumenty.

3.6.7.2 *Umiestnenie*

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

3.6.7.3 *Spôsob zaistenia*

Live aj offline

3.6.7.4 *Primárna kategória*

User Activity

3.6.7.5 *Iné kategórie*

File Presence/Interaction

3.6.8 ShellBags

3.6.8.1 *Popis*

Kľúče registra, ktoré zaznamenávajú preferencie rozloženia používateľa pre každý priečinok, s ktorým používateľ interaguje.

- **Cesta (v registri, XP–7):** HKCU\Software\Microsoft\Windows\Shell\BagMRU (+ \Bags) v NTUSER.DAT; **Win Vista+ (USRCLASS.DAT):** HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU (+ \Bags). Shellbagy zaznamenávajú nastavenia priečinkov v Prieskumníkovi (napríklad či si používateľ prezeral súbory v priečinku ako zoznam, alebo ako ikony či náhľady), ale nepriamo prezrádzajú **históriu prezeraných priečinkov** (či už na lokálnych diskoch, sieťových zdieľaniach alebo USB). Pre forenzné účely sú cenné, lebo prezradia, aký priečinok (cesta) užívateľ otvoril a dokonca aj zmazané alebo odpojené priečinky.

- *ShellBags* udržiavajú nastavenia priečinkov v Prieskumníkovi a tým pádom **logy priečinkov, ktoré užívateľ otvoril**. Obsahujú hierarchiu prehliadaných adresárov (MRU – Most Recently Used) aj s menami priečinkov a niekedy poslednými prístupmi. Pre forenznú analýzu tak vieme zistiť, aké adresáre používateľ prehliadal (vrátane napr. cez externé disky alebo sieťové zdieľania), a či mená týchto priečinkov naznačujú napr. ukladanie nelegálnych dát. ShellBags dopĺňajú časovú os, najmä keď klasické „LastAccess“ časové pečiatky na súboroch sú vypnuté.

- **Nástroje:** *ShellBags Explorer* (Eric Zimmerman) alebo *RegRipper plugin shellbags.pl* dokážu extrahovať obsah ShellBag kľúčov a premeniť ho na zoznam priečinkov s posledným zobrazením a ich nastaveniami. *KAPE* modul **ShellBags** (ak existuje) by vyžadoval získanie predmetných NTUSER/UsrClass registrov (napr. cez **RegistryHives** target).

- **Typ/atribúty:** Údaje v binárnej podobe vo vnútri registra.
    - Dôležité polia: **Path (názov/cesta priečinka)** – môže byť absolútna alebo relatívna, **LastWrite čas kľúča** – indikuje čas poslednej zmeny (často zodpovedá poslednému otvoreniu priečinka), a nastavenia pohľadu (ikonky, veľkosť okna). Shellbags niekedy obsahujú aj GUID zariadení (pre externé jednotky) a tým vedia identifikovať napr. písmeno disku, ku ktorému priečinok patril.

3.6.8.2 *Umiestnenie*

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Shell\Bags
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Shell\BagMRU
HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags
HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

3.6.8.3 *Spôsob zaistenia*

Live aj offline

3.6.8.4 *Primárna kategória*

User Activity: File (Folder) presence, Folder interaction

3.6.8.5 *Iné kategórie*

-

3.6.9 SUM (UAL)

3.6.9.1 *Popis*

User Access Logging (UAL) je funkcia zavedená a predvolene povolená v systéme Windows Server 2012, ktorá konsoliduje údaje o aktivite klienta. Okrem iných informácií je prístup používateľov ku konkrétnym rolám Windows Servera (napríklad Active Directory Domain Services na radiči domény) zaznamenaný v UAL. Konkrétna aktivita, ktorá spúšťa záznam, ktorý sa má zaznamenať pre danú rolu, nie je zdokumentovaná.

Na radičoch domény tak UAL poskytuje informácie o otváraní relácií na počítačoch pripojených k doméne (ak bol daný radič domény kontaktovaný kvôli autentifikácii alebo načítaniu skupinovej politiky).

Informácie sa lokálne ukladajú do maximálne piatich (5) Extensible Storage Engine (ESE) databázových súborov (.mdb):

1. Súbor Current.mdb, ktorý obsahuje údaje za posledných 24 hodín.
2. Maximálne 3 súbory <GUID>.mdb, ktoré obsahujú údaje za celý rok (prvý až posledný deň) od 2 rokov. Údaje v databáze Current.mdb sa každý deň skopírujú do príslušnej databázy (<GUID>.mdb) pre aktuálny rok.
3. Systemidentity.mdb, ktorý obsahuje metadáta na lokálnom serveri vrátane mapovania identifikátorov GUID a názvov rolí.

Historické údaje spred 2 rokov je teda možné získať v databázových súboroch UAL.

Tabuľka CLIENTS databázových súborov Current.mdb a <GUID>.mdb obsahuje viacero zaujímavých informácií:

- GUID a popis roly Windows Servera, ku ktorej sa pristupovalo. Okrem iného sa možno stretnúť s nasledujúcimi rolami:
    - Doménové služby Active Directory (identifikátor GUID: ad495fc3-0eaa-413d-ba7d-8b13fa7ec598).
    - Súborový server (GUID: 10a9226f-50ee-49d8-a393-9a501d47ce04).
    - Certifikačná služba Active Directory (identifikátor GUID: c50fcc83-bc8d-4df5-8a3d-89d7f80f074b).
- Klientska doména a používateľské meno.

- Celkový počet prístupov.
- Časové pečiatky prvého, posledného a denného prístupu.
- Adresa IPv4 alebo IPv6 klienta. V radičoch domény je možné načítať názov hosta priradený k adrese IP v danom čase, pretože počítačové kontá počítačov pripojených k doméne sa overujú aj v službách AD DS.

Každá položka v tabuľke CLIENTS sa skladá z jedinečnej množiny roly Windows Servera, domény/používateľského mena klienta a zdrojovej IP adresy.

Tabuľka DNS databázových súborov obsahuje informácie o DNS resolutions: názov hostiteľa, priradenú IP adresu a časovú pečiatku posledného DNS prekladu.

3.6.9.2 *Umiestnenie*

Súbory v adresári <SYSTEMROOT>\System32\Logfiles\SUM\:

- Current.mdb (dáta za posledných 24 h).
- Najviac 3 "<GUID>.mdb" files (aktuálny rok a história max 2 rokov).
- Systemidentity.mdb (mapovanie GUIDov rolí a ich mien).

3.6.9.3 *Spôsob zaistenia*

Live aj offline. Pri live zachytávaní pozor na prípadné nekonzistencie databázy, odporúčame zachytiť celý priečinok, v ktorom DB je.

3.6.9.4 *Primárna kategória*

User Activity

3.6.9.5 *Iné kategórie*

-

3.6.10Windows Index Search (Windows.edb)

3.6.10.1 *Popis*

Databáza Windows Search poskytuje index funkcií Windows Search na zvýšenie rýchlosti vyhľadávania indexovaním obsahu. Index Windows Search sa používa na vyhľadávanie prostredníctvom panela úloh systému Windows, Prieskumníka Windows a niektorých aplikácií Universal Windows Platform (UPW) (napríklad Outlook, OneDrive atď.).

V predvolenom nastavení sa indexuje iba podmnožina priečinkov a súborov (aby sa znížila veľkosť databázy Windows Search a využitie procesora). Skenované priečinky a počet indexovaných položiek nájdete v ponuke "Nastavenia vyhľadávania systému Windows".

Od Windows Vista / Windows Server 2008 to Windows 10 / Windows Server 2019, Windows Search používal databázu Extensible Storage Engine (ESE) (Windows.edb). Počnúc Windows 11 / Windows Server 2022 sa Windows Search prepol na dve databázy SQLite (Windows.db a Windows-gather.db).

Predvolene sa kontrolujú a indexujú iba položky z nasledujúcich zdrojov:

- Súbory a priečinky z priečinkov %USERPROFILE% (okrem adresárov AppData) a C:\ProgramData\Microsoft\Windows\Start Menu\Programs* (ktoré zahŕňajú startup LNK súbory).
    - Dostupné údaje: názov súboru, cesta, veľkosť, atribúty, časové pečiatky MAC. V prípade malého súboru môže byť indexovaná aj časť obsahu súboru.
- Údaje o pošte Outlook (s časovou pečiatkou príjmu, možným obsahom pošty).
- Názov poznámok OneNotu.
- História Internet Explorera (URL, časová pečiatka poslednej návštevy).

3.6.10.2 *Umiestnenie*

Od Windows 11:
%SYSTEMDRIVE%\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.db
%SYSTEMDRIVE%\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows-gather.db

Windows 7 až Windows 10:
%SYSTEMDRIVE%\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Windows XP:
%SYSTEMDRIVE%\Documents and Settings\All user\Application Data\Microsoft\Search\Data\Application\Windows\Windows.edb

3.6.10.3 *Spôsob zaistenia*

Live aj offline.

3.6.10.4 *Primárna kategória*

User Activity

3.6.10.5 *Iné kategórie*

File Presence

3.6.11 INetCache/CryptnetUrlCache

3.6.11.1 *Popis*

Browser sem ukladá nakešované dáta z prehliadania. Parí medzi artefakty webových prehliadačov. V počítačovej forenznej analýze sú **INETCache** a **CryptnetUrlCache** kľúčovými artefaktmi v kontexte prehliadania a internetovej aktivity. Tieto artefakty môžu poskytnúť dôležité informácie týkajúce sa používania webu a internetu používateľom vrátane návštev webových stránok, údajov vo vyrovnávacej pamäti a dokonca aj šifrovaných komunikačných aktivít. Nižšie je uvedený rozpis dôležitosti každého artefaktu, jeho obsahu a spôsobu, akým môže analytik interpretovať údaje.

3.6.11.2 ***INETCache (Internet Cache)***

INETCache ukladá vo vyrovnávacej pamäti kópie webových stránok, obrázkov, skriptov a iných zdrojov, ktoré prehliadač stiahne z internetu. Táto vyrovnávacia pamäť je vytvorená na urýchlenie prehliadania webu ukladaním kópií často navštevovaných webových stránok. Keď používateľ navštívi webovú stránku, namiesto opätovného stiahnutia všetkých prvkov ich prehliadač môže načítať z lokálnej vyrovnávacej pamäte, čím sa skráti čas načítania.

3.6.11.2.1 Umiestnenie

%USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache
V rôznych verziách systému Windows sa cesta môže mierne líšiť.
Umiestnenia špecifické pre prehliadač: Prehliadače Internet Explorer a Microsoft Edge používajú **INETCache** a iné prehliadače, ako napríklad Chrome a Firefox, môžu ukladať údaje vo vyrovnávacej pamäti do svojich vlastných adresárov vyrovnávacej pamäte.

3.6.11.2.2 Obsah

HTML Pages: Verzie navštívených webových stránok vo vyrovnávacej pamäti (vrátane obsahu HTML). **Images, Scripts, a Media Files**: Bežné mediálne súbory, ako sú obrázky (JPG, PNG, GIF) alebo iné dátové zdroje, ktoré sa stiahnu počas návštevy.
Web Forms a Cookies: Informácie, ktoré boli súčasťou webového formulára alebo údajov relácie, niekedy sa používali na zapamätanie si stavov prihlásenia alebo preferencií.
URLs: URL adresy uložené vo vyrovnávacej pamäti a ďalšie údaje o prehliadaní (t. j. história alebo metadáta o navštívených stránkach).

3.6.11.2.3 Význam pre forenzných analytikov:

- **Skúmanie aktivity používateľov**: Analytici môžu určiť, ktoré webové stránky používateľ navštívil, aj keď bola história vymazaná z prehliadača. Môžu načítať údaje o navštívených stránkach a konkrétnych prvkoch, ktoré boli načítané.
- **Fingerprinting prehliadača**: Súbory vo vyrovnávacej pamäti môžu analytikom poskytnúť predstavu o vzorcoch používania prehliadača a zariadenia používateľa.
- **Časové pečiatky**: Analytici môžu obnoviť časové pečiatky o tom, kedy boli webové stránky navštívené a ktoré konkrétne zdroje boli prístupné.
- **Dôkaz o prístupe**: Aj keď sa používateľ pokúsi vymazať svoju históriu prehliadania, údaje vo vyrovnávacej pamäti môžu byť stále dostupné a môžu poskytovať stopu jeho internetovej aktivity.

3.6.11.3 *CryptnetUrlCache*

CryptnetUrlCache je vyrovnávacia pamäť špecificky súvisiaca s **kryptografickými operáciami** v systéme Microsoft Windows a ukladá informácie priradené k adresám URL, ktoré sa používajú na prístup k údajom súvisiacim s certifikátom z internetu. Tento artefakt sa primárne používa vo vzťahu k zabezpečeným internetovým aktivitám, ktoré zahŕňajú certifikáty, ako sú SSL/TLS pripojenia, digitálne certifikáty alebo zabezpečené webové stránky.

3.6.11.3.1 Umiestnenie

Zvyčajne sa nachádza na nasledujúcom mieste:
%USERPROFILE%\AppData\Local\Microsoft\CryptnetUrlCache

3.6.11.3.2 Obsah

- **URL adresy certifikačných autorít:** URL adresy certifikačných autorít uložené vo vyrovnávacej pamäti, ktoré sa použili na overenie pravosti certifikátov SSL/TLS.
- **Metaúdaje SSL/TLS**: Údaje vo vyrovnávacej pamäti súvisiace so zabezpečenou komunikáciou alebo získavaním verejných kľúčov a certifikátov cez protokol HTTPS.
- **Zoznamy zrušených certifikátov (CRL):** Informácie o tom, či bol certifikát zrušený alebo či je stále platný.
- **Údaje relácie SSL**: Informácie o aktívnych alebo nedávno použitých reláciách SSL/TLS, prípadne vrátane šifrovanej komunikácie.

3.6.11.3.3 Dôležitosť pre forenzných analytikov

- **Skúmanie zabezpečenej komunikácie**: Analytici môžu analyzovať CryptnetUrlCache, aby zistili, ku ktorým zabezpečeným stránkam (HTTPS) používateľ pristupoval, a sledovať adresy URL zapojené do overovania certifikátu.
- **Kryptografické dôkazy**: Kryptografické adresy URL a certifikáty používané na overovanie zabezpečených webových pripojení môžu poskytnúť dôkaz o pravosti webovej stránky alebo zabezpečenej transakcie.
- **Korelácia údajov**: Ak používateľ navštívil určité zabezpečené stránky (napríklad bankové alebo e-mailové služby), tento artefakt môže pomôcť potvrdiť webovú aktivitu a poskytnúť ďalšie dôkazy o týchto návštevách.
- **Odhalenie citlivých údajov**: Aj keď táto vyrovnávacia pamäť ukladá hlavne kryptografické informácie, môže byť bránou k pochopeniu toho, ktoré zabezpečené pripojenia používateľ inicioval, čím sa potenciálne odhalia citlivé interakcie, ktoré boli inak šifrované.

3.6.11.3.4 Info, ktoré môže analytik získať

- **História prehliadania používateľa**: Artefakt INETCache poskytuje prehľad o webových stránkach, ktoré používateľ navštívil, a CryptnetUrlCache ponúka informácie o zabezpečených stránkach (HTTPS).
- **Časové pečiatky prístupu k webom**: Analytici môžu extrahovať časové pečiatky, ktoré podrobne popisujú, kedy boli prístupy ku konkrétnym zdrojom alebo lokalitám, čo je užitočné na vytvorenie časovej osi aktivity.
- **URL adresy a zdroje**: Extrahovanie adries URL a súvisiacich zdrojov môže analytikovi pomôcť pochopiť, aký obsah používateľ požadoval, aj keď pôvodná webová stránka už nie je prístupná.
- **Zabezpečené návštevy stránok**: CryptnetUrlCache odhaľuje zabezpečené pripojenia, ktoré používateľ vytvoril, napríklad tie, ktoré zahŕňajú online bankovníctvo alebo e-mail, čo môže byť rozhodujúce pri vyšetrovaní, kde ide o šifrovanú prevádzku.
- **Informácie o relácii**: Obe vyrovnávacie pamäte môžu obsahovať informácie o relácii, ktoré analytikom pomáhajú pochopiť vzorce aktivity používateľov a potenciálnu exfiltráciu údajov.

3.6.11.3.5 Kľúčové úvahy

- **Volatilita údajov**: Obe vyrovnávacie pamäte môžu byť volatilné; môžu byť prepísané, keď používateľ pokračuje v prehliadaní, najmä ak sú dosiahnuté limity veľkosti vyrovnávacej pamäte alebo ak sú nastavenia prehliadača nakonfigurované tak, aby vyrovnávaciu pamäť automaticky vymazali.
- **Potenciál čistenia**: Používatelia sa môžu pokúsiť vymazať vyrovnávaciu pamäť alebo použiť prehliadače zamerané na súkromie. Forenzní analytici však môžu byť stále

schopní obnoviť čiastočne odstránené alebo prepísané súbory pomocou špecializovaných nástrojov na obnovenie.
- **Korelácia s inými artefaktmi**: Artefakty INETCache a CryptnetUrlCache je často potrebné korelovať s inými artefaktmi, ako je história prehliadača, denníky udalostí alebo sieťové denníky, aby sa vykreslil úplný obraz o akciách používateľa.

Stručne povedané, **INETCache** a **CryptnetUrlCache** sú cenné pre forenzných analytikov skúmajúcich prehliadanie webu a bezpečnú internetovú aktivitu. Skúmaním týchto artefaktov môžu analytici identifikovať navštívené stránky, sledovať bezpečnú komunikáciu a potenciálne odhaliť kľúčové dôkazy súvisiace s online správaním používateľa, a to aj tvárou v tvár pokusom o vymazanie alebo zakrytie týchto informácií.

Zatiaľ čo **INETCache** v adresároch používateľov (ako %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache) zvyčajne obsahuje obsah vo vyrovnávacej pamäti súvisiaci s aktivitou prehľadávania používateľa, existuje aj **INETCache na systémovej úrovni** , ktorý možno nájsť v adresári **System32**, najmä vo vzťahu k určitým systémovým procesom a komponentom systému Windows.
Táto vyrovnávacia pamäť na úrovni systému je priradená k **Internet Exploreru (IE)** alebo **Microsoft Edgeu**, pretože tieto prehliadače a ich procesy na úrovni systému tiež ukladajú údaje do vyrovnávacej pamäte v umiestneniach spravovaných systémom.

3.6.11.4 *INETCache v System32*

INETCache na **systémovej úrovni** nájdete v:

- %SYSTEMROOT%\System32\inetsrv\INETCache

Toto umiestnenie obsahuje súbory vo vyrovnávacej pamäti, ktoré používajú **Internetové informačné služby (IIS)** a ďalšie súčasti spoločnosti Microsoft, ako je **Internet Explorer** alebo **Microsoft Edge,** pri interakcii s určitými funkciami na strane servera alebo internetovými operáciami na úrovni systému.

3.6.11.4.1 Obsah

- **Ukladanie do vyrovnávacej pamäte na úrovni systému**: Prostriedky vo vyrovnávacej pamäti súvisiace s procesmi systému Windows a systémovými operáciami, ktoré zahŕňajú internetové údaje.
- **Údaje súvisiace so serverom**: Keď systém Windows komunikuje s webovými lokalitami alebo webovými službami prostredníctvom **služby IIS** (Internetové informačné služby), môže do tohto umiestnenia ukladať súbory vo vyrovnávacej pamäti.
- **Obsah z aktualizácií/služieb**: Aktualizácie systému alebo služby založené na webových údajoch môžu tiež ukladať súbory do vyrovnávacej pamäte v tomto priečinku.

- **Dočasné internetové súbory**: Súbory, ako sú stránky HTML, obrázky, skripty a ďalšie zdroje, môžu byť uložené pre rýchlejší prístup pri interakcii systému s určitými webovými službami.

3.6.11.4.2 Význam vo forenznej analýze

- **Celosystémové internetové aktivity**: Analytik môže preskúmať tento **INETCache,** aby preskúmal internetové aktivity na úrovni systému, ako sú interakcie so službou Windows Update, pripojenia k vzdialeným serverom alebo systémová webová prevádzka, ktorá sa nemusí zobraziť v histórii prehľadávania používateľa.
- **Skrytá aktivita alebo aktivita na pozadí**: Niektoré systémové procesy, ktoré interagujú s webovými službami na účely aktualizácií softvéru, certifikátov alebo komunikácie s inými systémami, môžu v tomto umiestnení ponechať údaje vo vyrovnávacej pamäti. Aj keď používateľ nemá priamy prístup k určitým webovým stránkam, táto vyrovnávacia pamäť môže obsahovať dôkazy o nepriamych interakciách.
- **Odhaľovanie komunikácie webových služieb**: Forenzní analytici môžu objaviť údaje vo vyrovnávacej pamäti súvisiace s podnikovými alebo systémovými webovými službami, ktoré môžu zahŕňať komunikáciu so serverom alebo podrobnosti o pripojení.
- **Krížové odkazy s inými systémovými artefaktmi**: Kombinácia údajov nájdených v **System32\INETCache** s inými systémovými protokolmi (ako sú protokoly udalostí alebo sieťová prevádzka) by mohla odhaliť širší rozsah internetovej aktivity systému, ktorý nemusí byť okamžite zrejmý.

3.6.11.4.3 Kľúčové úvahy pre analytikov

- **Operácie na úrovni systému**: Táto vyrovnávacia pamäť s väčšou pravdepodobnosťou obsahuje údaje súvisiace so systémovými operáciami, a nie históriu prehľadávania špecifickú pre používateľa. Ak je vyšetrovanie zamerané na aktivitu používateľov, táto vyrovnávacia pamäť nemusí byť taká relevantná ako vyrovnávacia pamäť špecifická pre používateľa, ale stále môže ponúknuť prehľad o systémových procesoch interagujúcich s internetom.
- **Trvalosť údajov**: **INETCache** v adresári **System32** môže byť trvalejší ako údaje vyrovnávacej pamäte na úrovni používateľa v závislosti od systémových nastavení alebo aktivity. Stále však môže byť vymazaný alebo prepísaný procesmi údržby systému Windows.
- **Rozdiel od vyrovnávacej pamäte používateľa**: Analytik musí rozlišovať medzi údajmi prehliadania na úrovni používateľa (nachádzajú sa v **AppData**) a vyrovnávacou pamäťou na úrovni systému (nachádza sa v **System32**), pretože poskytujú rôzne prehľady o systémových a používateľských aktivitách.

Zatiaľ čo väčšina používateľov pozná **INETCache** umiestnený v adresároch ich používateľských profilov, **INETCache na úrovni systému,** ktorý sa nachádza v adresári **System32,** môže poskytnúť

cenné informácie o interakciách na úrovni systému s webovými službami, procesmi na pozadí a aktualizáciami. Forenzní analytici by nemali prehliadať toto umiestnenie, najmä pri vyšetrovaní systémových aktivít alebo hľadaní dôkazov súvisiacich so službami systému Windows, aktualizáciami alebo vzdialenými interakciami so serverom.

3.6.11.5 *Sumár*

3.6.11.5.1 Umiestnenie

%SYSTEMROOT%\System32\Config\SystemProfile\AppData\Local\Microsoft\Windows\INetCache\IE\
%SYSTEMROOT%\System32\inetsrv\INETCache
%USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache
%USERPROFILE%\AppData\Local\Microsoft\CryptnetUrlCache

3.6.11.5.2 Spôsob zaistenia

Live aj offline

3.6.11.5.3 Primárna kategória

User Activity

3.6.11.5.4 Iné kategórie

-

3.6.12 7-Zip Folder History

3.6.12.1 *Popis*

Kľúč databázy Registry obsahujúci zoznam archívnych súborov, ku ktorým sa pristupovalo pomocou 7-Zip.

3.6.12.2 *Umiestnenie*

Zachytávané cesty v registroch:
HKEY_USERS*\Software\7-Zip\FM\FolderHistory

3.6.12.3 *Spôsob zaistenia*

Live aj offline

3.6.12.4 *Primárna kategória*

Používateľská aktivita

3.6.12.5 *Iné kategórie*

Prítomnosť súboru, spustenie/prítomnosť spustiteľného súboru

3.7 Iné artefakty, spadajúce do žiadnej alebo do viacerých kategórií

3.7.1 Event Logs

3.7.1.1 *Popis*

Úplný zoznam udalostí nájdených v súboroch logov udalostí Windows (.evtx).

3.7.1.2 *Vybrané logy a udalosti, významné pre forenznú analýzu*

- **Windows Security Event Log – Logon/Logoff** – Najdôležitejší zdroj. Pri zapnutom audite prihlasovania obsahuje:
    - Event **4624** – Úspešné prihlásenie užívateľa. Kľúčové polia: **Account Name**, **Logon Type** (2 = interaktívne konzola, 10 = vzdialené/RDP, 3 = sieťové napr. SMB), **Source IP** (pri sieťovom/RDP prihlásení).
    - Event **4625** – Neúspešný pokus o prihlásenie (s uvedením dôvodu – zlé heslo, uzamknutý účet atď).
    - Event **4634** – Odhlásenie (Logon Type uvedený).
    - Event **4647** – Užívateľ inicioval odhlásenie (typicky pri odhlásení cez Start menu).
    - Event **4648** - Používateľ sa úspešne prihlásil do počítača pomocou explicitných prihlasovacích údajov, hoci už bol prihlásený ako iný používateľ.
    - Event **4672** – Prihlásenie s pridelenými privilegovanými právami (administrátor má vždy, značí privilegovaný logon).
    - Event **4778/4779** – Znovupripojenie k odpojenej session / odpojenie session (pre RDP).
      Tieto udalosti vytvárajú chronológiu prihlasovacej aktivity, vrátane lokálnych loginov, UAC elevácií (typ 11), sieťových prístupov (typ 3 pri prístupe k zdielanému priečinku atď).
- Vytvorenie používateľa – **Security.evtx**
    - Event **4720** - „A new account has been created“ – obsahuje meno a SID vytvoreného konta aj používateľa, ktorý konto vytvoril

- **Windows System Event Log – Štart/Stop PC** – Event **6005** (The Event log service was started) a **6006** (bol zastavený) v System logu indikujú boot a shutdown čas. Taktiež

6008 ak predchádzajúci shutdown bol neočakávaný. Tieto pomáhajú v timeline zistiť, kedy boli možné interaktívne prihlásenia.

- **Profil užívateľa – časy** – V registri HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\<SID> je hodnota **ProfileLoadTimeLow/High**, ktorá môže indikovať, kedy bol profil naposledy načítaný (teda kedy sa user naposledy prihlásil). Taktiež v NTUSER.DAT každého profilu LastWrite čas niektorých kľúčov (napr. HKCU\Environment) sa aktualizuje pri logone.
- **Iné autentizácie** – Ak ide o členstvo v doméne: Event **4768/4769** v Security logu (na lokálnej WS ich nevidno, to sú domain controller Kerberos events). Ale napr. ak počítač prijal login cez doménu v offline režime, záznam je normálne 4624 s Domain.
- **Prebúdzanie zo zamknutia (Lock/Unlock)** – Event **4800** (workstation locked) a **4801** (unlocked) v Security logu, spojené s ID užívateľa. Tieto môžu dokresliť aktivitu užívateľa v rámci prihlásenia.
- **Windows RDP – Udalosti pripojenia** – RDP (Remote Desktop Protocol) zanecháva viaceré event logy:
    - **Security log**: Pri úspešnom RDP prihlásení sa zaznamená Event ID **4624** (Logon Type 10 = RemoteInteractive) – obsahuje prihlasovacie meno a IP adresu klienta. Pri neúspešnom pokuse Event **4625** (s Logon Type 10). Odpojenie RDP session môže byť evidované ako **4634/4647** a špeciálne RDP reconnect ako 4778/4779.
    - **Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational**: Event **1149** – indikuje pokus o autentifikáciu cez RDP (meno užívateľa a IP adresa klienta). (1149 sa loguje pri pokuse o prihlásenie – úspešnom aj neúspešnom).
    - **Microsoft-Windows-TerminalServices-LocalSessionManager/Operational**: Event **21** (prihlásenie k relácii), **22** (odhlásenie), **24** (odpojenie session z klienta), **25** (znovupripojenie k session) – tiež obsahujú užívateľa a IP.
    - **Microsoft-Windows-RDPCoreTS/Operational**: Event **131** – úspešné nadviazanie TCP pripojenia na RDP službu (uvádza IP adresu klienta), Event **98** – úspešné dokončenie TLS handshaku RDP spojenia
      Tieto logy spolu poskytujú časovú stopu, kto a odkiaľ sa vzdialene prihlásil cez RDP.
- Vytvorenie procesu – Security.evtx
    - **Process Tracking** – Ak je zapnutý audit procesov, **Security log** zaznamená Event ID **4688** pri vytvorení každého procesu (staršie OS ID 592). Log 4688 obsahuje meno procesu, PID, účet používateľa atď. (vyžaduje zapnúť *Audit Process Creation*).
- Inštalácia servisu –System.evtx, Security.evtx
    - **System log** eviduje event ID **7035** pri štarte alebo zastavení služby (Service Control Manager) – keď služba štartuje, môže to indikovať spustenie príslušného exe ako služby.
    - **System log** takisto eviduje event ID **7045**, "A new service was installed in the system", sa tiež používa na sledovanie inštalácií služieb, ale nemusí vždy prekladať používateľský SID na používateľské meno.

- Event ID **4697**, tentoraz v **Security.evtx**, "A service was installed in the system", zachytáva tvorbu nových služieb a poskytuje podrobnosti o službe a používateľovi, ktorý ju nainštaloval.

3.7.1.3 *Umiestnenie*

%systemroot%\System32\winevt\Logs*

3.7.1.4 *Spôsob zaistenia*

Live aj offline

3.7.1.5 *Primárna kategória*

Všetky

3.7.1.6 *Iné kategórie*

-

3.7.2 Master File Table

3.7.2.1 *Popis*

Master File Table (MFT) je databáza používaná systémom súborov NTFS na ukladanie metaúdajov súborov vrátane časových pečiatok, názvu súboru a veľkosti súboru. Ide o hlavnú tabuľku súborového systému NTFS. Je to špeciálny skrytý súbor, v ktorom každý súbor či priečinok na disku má jeden záznam (štandardne 1024 B). Záznam MFT obsahuje metadáta: názov súboru, fyzickú polohu dát, veľkosť, časové pečiatky v 2 setoch po 4 (vytvorenia, zmeny, posledného prístupu atď.) a informáciu o atribútoch. Forenzne sa z $MFT dá získať úplný zoznam súborov, vrátane zmazaných (ak ešte neboli prepísané, tak sú tiež prítomné, ale označené ako free) a časové pečiatky, ktoré pomáhajú určiť, kedy bol súbor vytvorený alebo modifikovaný.

3.7.2.2 *Umiestnenie*

C:\$MFT, nie len na systémovom disku, ale na ľubovoľnom pripojenom disku so súborovým systémom NTFS.

3.7.2.3 *Spôsob zaistenia*

Live aj offline, hoci na bežiacom systéme nie je prístupná bežnému používateľovi.

3.7.2.4 *Primárna kategória*

File Presence

3.7.2.5 *Iné kategórie*

3.7.3 USN Journal

3.7.3.1 *Popis*

Update Sequence Number Journal je NTFS žurnál, ktorý loguje všetky zmeny súborov na disku (vytvorenie, úprava, zmazanie) spolu s timestampami. Od Windows Vista je USN Journal štandardne zapnutý a funguje ako neustále sa posúvajúci log. Záznamy obsahujú ID súboru (MFT reference), typ zmeny (príznaky – vytvorenie, vymazanie, premenovanie, atď.) a čas v UTC. Pre forenznú analýzu je to kľúčový zdroj pre časovú os udalostí súborového systému – napríklad dokazovanie, že určitý súbor bol zmazaný v konkrétnom čase.

3.7.3.2 *Umiestnenie*

C:\$Extend\$USNJrnl:$J, nie len na systémovom disku, ale na ľubovoľnom pripojenom disku so súborovým systémom NTFS.

3.7.3.3 *Spôsob zaistenia*

Live aj offline

3.7.3.4 *Primárna kategória*

File presence

3.7.3.5 *Iné kategórie*

Operácie so súbormi, spravidla sa zameriavame na ich vymazávanie

3.7.4 Recycle Bin

3.7.4.1 *Popis*

Priečinok používaný ako dočasné úložisko pre odstránené súbory pred trvalým odstránením. Pri zmazaní súboru Windows (ak nie je použitý SHIFT+Delete) presunie súbor do Koša. V priečinku používateľovho SID sa objavia súbory \$I... a \$R...: $I obsahuje metadáta o pôvodnom mene a ceste zmazaného súboru a čase zmazania, $R je samotný obsah súboru. Analýza Koša odhalí, aké súbory používateľ vymazal a kedy (aj ak ich nevyprázdnil úplne).

3.7.4.2 *Umiestnenie*

C:\$Recycle.Bin***

3.7.4.3 *Spôsob zaistenia*

Live aj offline

3.7.4.4 *Primárna kategória*

User Activity

3.7.4.5 *Iné kategórie*

File Presence, Deletion, Interaction

3.7.5 Pamäť RAM

3.7.5.1 *Popis*

Vo forenznej analýze je operačná pamäť RAM (Random Access Memory) kritickým zdrojom nestabilných dôkazov. Zachytiť ju možno len na bežiacom systéme (hoci na virtuálnych zariadeniach býva zapísaná i do súboru na disku hypervízora, čo zaistenie zjednodušuje), napríklad prostredníctvom výpisov pamäte pomocou nástrojov ako Volatility alebo Rekall, alebo vytvorením obrazu pamäte pomocou WinPMEM, DumpIt či FTK Imagera.

Pamäť RAM odhaľuje systémové stavy v reálnom čase, ktoré sú neviditeľné na perzistentnom úložisku. Z pohľadu vyšetrovania incidentov môže byť kritickým zdrojom informácií o bezsúborovom (tzv. fileless) malware, rootkitoch a iných pokročilých hrozbách.

RAM spravidla obsahuje:

- Bežiace procesy a injektovaný kód
- Otvorené sieťové pripojenia a porty
- Šifrovacie kľúče
- Heslá/prihlasovacie údaje v otvorenom texte
- Dáta zo schránky
- Správy v chate
- Neuložené dokumenty
- Stopy používateľskej aktivity
- Skryté artefakty malvéru

To umožňuje rekonštrukciu akcií útočníka, detekciu prechodných hrozieb a dešifrovanie šifrovaných súborov.

3.7.5.2 *Spôsob zaistenia*

Live

3.7.5.3 *Primárna kategória*

Defacto všetky

4 Úloha KPB2.2

4.1 Zadanie úlohy KPB2.2

Úloha KPB2.2 – Identifikácia vhodnej metódy na zber digitálnych stôp v prevádzkovom a vypnutom stave pre jednotlivé zdroje artefaktov. Súčasne sa výskumný tím v tejto úlohe zameria na zabezpečenie digitálnych dôkazov z viacerých zariadení a zdrojov (IstroSec).

Úloha KPB2.2 – Identifikácia vhodnej metódy zberu digitálnych stôp na bežiacom zariadení a zo zariadenia vo vypnutom stave pre jednotlivé zdroje artefaktov. Súčasne sa výskumný tím v tejto úlohe zameria na zabezpečenie digitálnych dôkazov z viacerých zariadení a zdrojov (IstroSec).

4.2 Metodológia riešenia úlohy KPB2.2

Po definovaní artefaktov, ktorých zberu sa v tejto fáze projektu budeme venovať, sa zameriame na popis spôsobu ich extrakcie z bežiaceho i vypnutého systému.
Pri zaisťovaní dát z bežiaceho systému je nevyhnutné zabezpečiť, aby činnosť v čo najmenšej možnej miere pozmenila predmetný systém. Medzi štandardné činnosti, ktorým sa zaisťovateľ spravidla nevyhne, patria:

- Prihlásenie alebo odomknutie zariadenia zadaním hesla alebo iným spôsobom autentifikácie;
- Pripojenie USB kľúča s pripravenými nástrojmi na zaisťovanie digitálnych stôp;
- Pripojenie zariadenia (USB kľúča či externého disku) na uloženie získaných stôp;
- Spustenie procesu na zaistenie digitálnych stôp – počet a typ sa líši v závislosti od objemu a typu zaisťovaných stôp.

Pri zaisťovaní digitálnych stôp z vypnutého zariadenia je potrebné brať do úvahy nasledovné aspekty a na základe nich prispôsobiť metodiku zaistenia digitálnej stopy:

- Aký typ zariadenia je nosičom stôp?
    - server, pracovná stanica (desktop/tower), notebook, virtuálny server či virtuálna pracovná stanica, flash disk, externý pevný disk, ...
- Aký typ disku zariadenie obsahuje?
    - HDD, SSD, rôzne typy rozhraní (SATA, NVMe, SCSI, USB, ...)

Prvým krokom, ešte pred zaistením dát pred spracovanie nástrojom, bude totiž vytvorenie bitovej kópie zdrojového zariadenia. Hoci to nie je predmetom projektu, pre kompletnosť informácií sme považovali za užitočné tieto skutočnosti spomenúť.

Pred definovaním požiadaviek na nástroj je nutné si ujasniť, aký typ vstupu predpokladáme. Pre potreby tohto dokumentu predpokladajme, že ako vstup forenznej analýzy vypnutého zariadenia je jeho forenzný obraz, napríklad vo formáte .E01 alebo .raw či .dd.

4.3 Postup zaisťovania jednotlivých typov digitálnych stôp

4.3.1 Zaisťovanie registrov: live

V kontexte počítačovej forenznej analýzy je zber registrov z **bežiaceho systému** (live acquisition) citlivý proces. Systémové hives (ako HKLM) sú zamknuté, takže ich nemôžeme jednoducho kopírovať. Najbezpečnejší a najpoužívanejší spôsob je použitie vstavaného príkazu **reg save**, ktorý vytvorí binárnu kópiu hive bez zmeny originálu.

Tento prístup je odporúčaný v forenzných best practices (napr. SANS), pretože minimalizuje footprint a zachováva integritu.

1. Príprava

- Spustite **Command Prompt ako Administrator** (pravý klik na cmd.exe → Run as administrator). Keďže pre bežné používateľské konto je prístup k registrom nemožný, je nutné mať prístup k účtu lokálneho administrátora zariadenia. To so sebou prináša isté riziká, najmä ak je útočník na zariadení stále aktívny.
- Pripravte si cieľový priečinok na externom médiu (napr. USB disk), napr. E:\Forensic\Registry\.
- Po zbere vypočítajte **hash hodnoty** (napr. MD5, SHA1 a SHA-256) exportovaných súborov pre chain of custody.
- Dokumentujte čas, príkazy, i hash hodnoty zaistených registrov (MD5, SHA1, SHA256).

2. Export HKLM (HKEY_LOCAL_MACHINE)
HKLM sa skladá z viacerých sub-hives (SYSTEM, SOFTWARE, SAM, SECURITY atď.). Exportujte ich jednotlivo:

```
reg save HKLM\SYSTEM E:\Forensic\Registry\SYSTEM.hive
reg save HKLM\SOFTWARE E:\Forensic\Registry\SOFTWARE.hive
reg save HKLM\SAM E:\Forensic\Registry\SAM.hive
reg save HKLM\SECURITY E:\Forensic\Registry\SECURITY.hive
```

- Príkaz vytvorí binárny .hive súbor (nie .reg textový export!).
- Pre hive HKLM nie je dostupný priamy spôsob, ako ho exportovať celý: popísané sub-hives pokrývajú väčšinu forenzných artefaktov a zodpovedajú podporným súborom hivu, ktoré sa nachádzajú v lokalite %systemroot%\System32\config.

3. Export používateľských hives (NTUSER.DAT a UsrClass.DAT pre všetkých používateľov)
Tieto sú uložené v profiloch používateľov a môžu byť zamknuté, ak je používateľ prihlásený.

Pre aktuálne prihláseného používateľa (HKCU):

```
reg save HKCU E:\Forensic\Registry\HKCU_current.hive
```

Pre všetkých používateľov (aj neprihlásených):

- Najprv identifikujeme, kde sa nachádzajú profily: dir C:\Users /b
- Pre každého používateľa skopírujte fyzické súbory (ak nie sú zamknuté):

```
copy "C:\Users\<username>\NTUSER.DAT" E:\Forensic\Registry\<username>_NTUSER.DAT
copy "C:\Users\<username>\AppData\Local\Microsoft\Windows\UsrClass.dat" E:\Forensic\Registry\<username>_UsrClass.dat
```

- Ak sú zamknuté (používateľ prihlásený), použite Volume Shadow Copy (VSS) alebo tool ako FTK Imager (viď nižšie).

Automatizácia skriptom (PowerShell ako Admin):

```
PowerShell
$dest = "E:\Forensic\Registry"
New-Item -ItemType Directory -Path $dest -Force

# HKLM sub-hives
reg save HKLM\SYSTEM "$dest\SYSTEM.hive"
reg save HKLM\SOFTWARE "$dest\SOFTWARE.hive"
reg save HKLM\SAM "$dest\SAM.hive"
reg save HKLM\SECURITY "$dest\SECURITY.hive"

# Všetky NTUSER.DAT a UsrClass.dat
Get-ChildItem C:\Users -Directory | ForEach-Object {
  $user = $_.Name
  $ntuser = "C:\Users\$user\NTUSER.DAT"
  $usrclass = "C:\Users\$user\AppData\Local\Microsoft\Windows\UsrClass.dat"

  if (Test-Path $ntuser) { copy $ntuser "$dest\$user`_NTUSER.DAT" }
  if (Test-Path $usrclass) { copy $usrclass "$dest\$user`_UsrClass.dat" }
}
```

4. Alternatívne metódy pre zamknuté súbory – aplikovateľné aj na artefakty popísané v nasledujúcich podkapitolách:

- **Volume Shadow Copy Service (VSS):** Vytvorte shadow copy a kopírujte z nej (nástroj ako vssadmin alebo DiskShadow).
- Forenzné nástroje:
  - **FTK Imager** (zdarma): Spustite → Create Disk Image → Vyberte "Obtain Protected Files" → Vyberte registry hives.
  - **ProDiscover** alebo **EnCase**: Podpora live acquisition.
  - **Belkasoft X** alebo **Magnet AXIOM**: Automatizovaný zber registry z live systému.

- **Pamäťový dump + Volatility:** Ak potrebujete volatilné dáta, zachyťte RAM (FTK Imager) a extrahujte hives pomocou Volatility (plugin hivelist, dumpfiles).

5. Dôležité upozornenia

- **Minimalizujte zmeny:** Live zber vždy mení systém, takže offline analýza je preferovaná, ak je možné.
- **Integrita:** Vždy hashujte (Get-FileHash v PowerShell) a dokumentujte.
- **Právne aspekty:** Získavajte súhlas alebo súdny príkaz.
- Po zbere dáta analyzujte offline.

4.3.2 Zaisťovanie registrov: offline

- Ak ešte nie je vytvorený image disku, začíname vytvorením bitovej kópie!
- Export registrov z image – napr.
    - mount image ako Read-only a z admin cmdline si ich analytik vie aj vykopírovať
    - mount image a priamo spustiť parsovanie
    - Podstatné je nezanedbať čistenie registrov: spojiť samotné podporné súbory hivov s ich transakčnými logmi, tak si zabezpečíme reflektovanie všetkých zmien, aj tých, ktoré ešte do podporných súborov neboli zapísané
- Nástroj tým pádom musí umožňovať vykopírovanie registra zo zdrojovej stopy, zjednotenie transakčných registrov (napríklad pomocou nástroja E. Zimmermana Registry Explorer alebo cmdline nástroja rla.exe).
- Po exporte je nutné súbory zahashovať (SHA1, SHA265, MD5).
- V priebehu procesu by mal nástroj zaznamenávať, aká operácia prebehla v akom čase a s akým výsledkom. Tým pádom bude analytik vedieť, ak sa z ľubovoľného dôvodu niektorý z registrov exportovať alebo zjednotiť s transakčným logom nepodarí (napríklad ak bol transakčný log alebo samotný register zašifrovaný ransomvérom).

4.3.3 Zaisťovanie systémových súborov: live

Nasledujúca stať sa týka zaisťovania súborov, ktoré sú na bežiacom systéme skryté, prípadne uzamknuté:

- $MFT, $USN:$J, $Recycle.Bin
- SRUM.DB, LNK súbory, JumpListy, PCA, ...

Existuje viacero spôsobov i hotových nástrojov, ako sa k podobným artefaktom dostať. Dostupných je množstvo voľne dostupných nástrojov (ako napríklad tie od Erica Zimmermana), ktoré umožňujú extrakciu dát i z bežiaceho zariadenia. Primárna metóda zahŕňa tzv. raw prístup na disk, alebo službu Volume Shadow Copy Service (VSS). Pomocou

oboch sa dajú obísť obmedzenia - zámky súborov. Samozrejme, stale platí, že potrebný je prístup s oprávneniami lokálneho administrátora.

Ak máme záujem extrahovať artefakty pre ďalšie spracovanie, môžeme ich zo systému skopírovať z GUI nástroja FTK Imager (označenie súboru, rightclick à Export files), alebo pomocou nástroja Kape. Podrobnosti o týchto nástrojoch sú nad rámec tohto dokumentu.

Podobne ako v predchádzajúcich prípadoch, vždy vytvoríme hash zaistených súborov.

4.3.4 Zaisťovanie systémových súborov: offline

Pri offline zaisťovaní máme zjednodušenú úlohu v zmysle, že nehrozí pozmenenie stopy tým, že z nej extrahujeme jednotlivé artefakty.

4.3.5 Zaisťovanie Event logov: live

Keďže Event logy nie sú prístupné pre bežného používateľa, potrebujeme oprávnenia na úrovni administrátora zariadenia. Potom je možné logy exportovať z administrátorského príkazového riadka či PowerShellu.

```
Copy-Item C:\Windows\System32\winevt\Logs\* -Destination D:\Work\Logs\
```

4.3.6 Zaisťovanie Event logov: offline

Z pripojeného a namountovaného disku dokážeme súbory s Event logmi jednoducho skopírovať. Alternatíva je ich parsovanie a spracovanie priamo z umiestnenia na image disku, ktorý, ako sme už spomínali, vždy pripájame v read-only móde.

5 Úloha KPB2.3

5.1 Zadanie úlohy KPB2.3

Úloha KPB2.3 – Overenie vhodnosti metódy na zabezpečenie integrity digitálnych dôkazov – v tejto úlohe sa zameriame na zabezpečenie integrity digitálnych dôkazov a možnú detekciu potrebného porušenia digitálnych dôkazov (IstroSec).

V rámci ADFIR nie sú dôkazy statické; ide o dynamický tok dát zbieraných zo živých systémov, často v reálnom čase, ktoré sú následne parsované, normalizované a transformované do štruktúrovaných formátov (CSV, databázy) pre algoritmy strojového učenia. Tento posun si vyžaduje prehodnotenie konceptov integrity. Už nás nezaujíma len fyzická integrita sektorov pevného disku, či odtlačok celého obrazu disku; musíme overovať informačnú integritu abstraktných dátových štruktúr. Napríklad, ak projekt využíva Formálnu konceptuálnu analýzu (FCA) na odvodenie vzťahov medzi artefaktmi, mechanizmus integrity musí zabezpečiť, že vygenerované mriežkové štruktúry presne odrážajú podkladovú binárnu realitu bez zavedenia chýb spôsobených samotným procesom extrakcie.

5.2 Metodológia riešenia úlohy KPB2.3

V tejto kapitole predstavíme princípy a štandardy relevantné pre riešenie úlohy.

5.2.1 Daubertov štandard a vedecká validita

Hoci je projekt ADFIR realizovaný na Slovensku/v EÚ, princípy Daubertovho štandardu (používaného v USA, ale globálne vplyvného v digitálnej forenznej analýze) sú relevantné pre vedeckú validitu. Štandard sa pýta:

- Bola technika testovaná?
- Bola podrobená recenznému konaniu (peer review)?
- Je známa alebo potenciálna chybovosť prijateľná?
- Existujú štandardy kontrolujúce fungovanie techniky?

Pre projekt ADFIR to znamená, že akákoľvek proprietárna alebo „black box“ metóda integrity sa považuje za nevhodnú. Projekt musí využívať otvorené, štandardizované algoritmy (ako SHA-256 alebo BLAKE3), kde sú chybovosti (pravdepodobnosti kolízií) matematicky dokázané a recenzované.

5.2.2 ISO/IEC 27037: Usmernenia na identifikáciu, zber, získavanie a uchovávanie

Tento medzinárodný štandard poskytuje referenčný rámec pre manipuláciu s digitálnymi dôkazmi. Definuje „integritu“ ako vlastnosť zabezpečujúcu presnosť a úplnosť aktív.

- **Relevancia pre ADFIR:** ISO 27037 explicitne uvádza, že živá akvizícia zahŕňa zmenu digitálnych dôkazov. Uvádza, že takéto kroky sú prijateľné, ak sú nevyhnutné, primerané a zdokumentované.
- **Kritériá overenia:** Metóda overená v tejto správe sa považuje za „vhodnú“ iba vtedy, ak generuje potrebné metadáta na splnenie požiadaviek na dokumentáciu podľa ISO 27037. To zahŕňa zaznamenanie použitého nástroja, času vykonania a kontextu používateľa.

5.2.3 Hašovacie funkcie

Základný princíp overovania digitálnych dôkazov spočíva v kryptografii. Dôraz projektu ADFIR na automatizáciu a strojové učenie však mení kritériá pre výber kryptografických primitív. Musíme vyvážiť odolnosť voči kolíziám (bezpečnosť) s priepustnosťou (výkonnosťou) a paralelizovateľnosťou (škálovateľnosť).

Hašovacia funkcia mapuje dáta ľubovoľnej veľkosti na bitový reťazec fixnej veľkosti. Na to, aby bola funkcia vhodná pre účely overovania vo forenznej analýze, musí byť funkcia:

1. **Deterministická:** Rovnaký vstup vždy vedie k rovnakému výstupu.
2. **Odolná voči prvému vzoru (Pre-image Resistant):** Je neuskutočniteľné vygenerovať správu, ktorá poskytne konkrétnu hodnotu hašu.
3. **Odolná voči kolíziám (Collision Resistant):** Je neuskutočniteľné nájsť dve rôzne správy, ktoré majú rovnakú hodnotu hašu.

MD5:

- MD5 produkuje 128-bitový digest. Je kryptograficky prelomená. Kolízne útoky dokážu na modernom hardvéri vygenerovať dva rôzne súbory s rovnakým MD5 hašom.
- Napriek prelomeniu zostáva MD5 najrýchlejším z tradičných algoritmov. V kontexte „identifikácie relevantných digitálnych stôp“ (napr. pre prvotné triedenie alebo deduplikáciu masívnych nekritických datasetov, ako sú milióny bežných systémových súborov), MD5 ponúka výkonnostnú výhodu.
- **Nie je však vhodná** na primárne overenie integrity.

SHA256:

- SHA-256 produkuje 256-bitový odtlačok (digest). Je súčasným priemyselným štandardom (napr. schváleným NIST). Neexistujú žiadne praktické kolízne útoky.

- Použitá pre finálne dôkazy. Na zabezpečenie „prípustnosti výsledkov... v trestnom konaní“ musí byť finálny odtlačok akýchkoľvek zozbieraných dôkazov overený minimálne pomocou SHA-256.

5.3 Overenie narušenia na operačných systémoch Windows

Windows je primárnym cieľom projektu ADFIR. Keď automatizovaný zberný nástroj (vyvinutý spoločnosťou IstroSec) beží na kompromitovanom hostiteľovi so systémom Windows, ovplyvňuje špecifické artefakty.

Systémová pamäť a Prefetch

- **Mechanizmus:** Keď beží proces akvizície, správca pamäte jadra Windows alokuje stránky v RAM. Windows Prefetcher (%SYSTEMROOT%\Prefetch) vytvorí alebo aktualizuje súbor .pf pre tento nástroj, pričom zaznamená, okrem iného, čas jeho spustenia a cestu k spustiteľnému súboru nástroja.

- **Dopad na integritu:** Toto prepíše staršie pamäťové stránky (potenciálne dôkazy) a modifikuje súborový systém (vytvorenie súboru .pf).

- **Overenie vhodnosti:** Vhodná metóda zberu musí explicitne odfiltrovať pamäťové stránky obsahujúce kód nástroja a súbor Prefetch vygenerovaný nástrojom. Táto technika „odčítania vyšetrovateľa“ obnovuje logickú integritu časovej osi.

Artefakty registrov (Shimcache / Amcache)

- **Mechanizmus:** Spustenie nástroja môže aktivovať Application Compatibility Engine (Shimcache), čím sa aktualizuje vetva registra SYSTEM.

- **Dopad na integritu:** Toto mení LastWriteTime kľúčov Registra, čo môže potenciálne zakryť časovú os spustenia malvéru útočníkom, ak k nemu došlo v blízkom čase.

- **Mitigácia:** Automatizovaný nástroj sa musí opýtať na aktuálny systémový čas *pred* akoukoľvek inou akciou a zalogovať ho. Tým sa stanoví „Čas nula“ pre vyšetrovanie. Akýkoľvek artefakt s časovou pečiatkou *po* Čase nula sa považuje za potenciálne vygenerovaný vyšetrovateľom. Dôležité je podotknúť, že sa nemožno spoliehať na čas nastavený na zariadení. Zaznamenať musíme tak spomínaný „čas nula“, ako ho vidíme na zariadení, ale zároveň zaznamenať i čas z iného, nezávislého zdroja (online hodiny, analytikov smartfón/smartwatch a podobne). Ak zistíme odchýlku, budeme s ňou počítať napríklad v prípade nutnosti korelácie výstupov analýzy s výstupmi analýzy iných stôp (endpointy, sieťové zariadenia, EDR a podobne).

Protokoly udalostí (Event Logs)

- **Mechanizmus:** Nakoľko zberný nástroj inštaluje ovládač jadra, Service Control Manager zaloguje Event ID 7045 (Služba nainštalovaná) v systémovom logu.

- **Vhodnosť:** Toto je v skutočnosti *prospešné narušenie*. Vytvára nezmazateľnú auditnú stopu akvizície. Overenie vhodnosti vyžaduje, aby sa nástroj *nepokúšal* vymazať alebo potlačiť tento log, pretože by to predstavovalo ničenie dôkazov (spoliation of evidence).

5.4 Mechanizmy blokovania zápisu

Zabránenie modifikácii dôkazov počas akvizície je základným pravidlom forenznej analýzy. Na tento účel sa používajú softvérové alebo hardvérové blokátory zápisu. Slúžia na zabránenie nechceného zápisu na zaisťované médium tým, že zabezpečia jeho pripojenie len v móde na čítanie.

5.4.1 Hardvérové blokátory zápisu (HWB)

- **Mechanizmus:** Fyzické mostíky, ktoré fyzicky prerušujú signál príkazu „Write“ na rozhraní (SATA/USB).
- **Vhodnosť:**
    - **Post-Mortem:** Nevyhnutné pre analýzu zaistených pevných diskov (diskové zariadenia koncových zariadení).
    - **Automatizácia/Živá forenzná analýza:** Úplne **nevhodné**. Hardvérový blokátor zápisu nemôžete zapojiť do RAM bežiaceho servera alebo vzdialenej cloudovej inštancie.

5.4.2 Softvérové blokovanie zápisu (SWB)

- **Mechanizmus:** Konfigurácie operačného systému, ktoré inštruujú jadro, aby odmietlo požiadavky na zápis na konkrétne zariadenie.
- **Implementácia Windows:** Kľúč Registra HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies\WriteProtect.
- **Overenie vhodnosti:**
    - **Riziko:** Softvérové blokovanie je potenciálne omylné. Rootkit na úrovni jadra alebo chybný ovládač ho môžu obísť.
    - **Verdikt ADFIR:** Pre „Zber digitálnych stôp“ v živých scenároch je softvérové blokovanie zápisu **akceptované ako vhodné**, za predpokladu, že je spojené s:
        1. **Overením hašov:** Hašovanie pred a po analýze (ak je zariadenie statické).
        2. **Auditnými logmi:** Logovanie každého vykonaného príkazu.

6 Úloha KPB2.4

6.1 Zadanie úlohy KPB2.4

Úloha KPB2.4 – Vytvorenie nástroja na experimentálne overovanie zabezpečenia digitálnych dôkazov – vytvorenie nástroja na experimentálne overovanie zabezpečených digitálnych dôkazov (IstroSec).

Táto kapitola definuje metodologický rámec pre automatizovanú akvizíciu digitálnych dôkazov s využitím nástroja „Athena“, ktorý bol vyvinutý partnerom IstroSec pre potreby tohto výskumu.

6.2 Koncept cielenej akvizície

V kontexte rozsiahlych infraštruktúr nie je vždy možné alebo efektívne vytvárať kompletné bitové kópie diskov pre každé podozrivé zariadenie. Athena preto implementuje metodiku "forenznej triáže" a cielenej akvizície, ktorú spoločnosť IstroSec dlhodobo využíva pri reakcii na incidenty (Incident Response - IR). Tento prístup sa zameriava na rýchlu identifikáciu a extrakciu tých artefaktov, ktoré majú najvyššiu výpovednú hodnotu pre potvrdenie alebo vyvrátenie hypotézy o kompromitácii.

Metodika Atheny rozdeľuje proces zberu do dvoch fáz:

1. **Fáza Akvizície (Collection Phase):** Surové dáta sú extrahované z cieľových systémov a uložené do štruktúrovanej SQL databázy. Tento krok zabezpečuje perzistenciu a integritu pôvodných hodnôt pred akoukoľvek analytickou transformáciou.
2. **Fáza Spracovania (Processing Phase):** Nad surovými dátami sú spúšťané špecifické SQL skripty, ktoré vykonávajú čistenie, normalizáciu, de-duplikáciu a formátovanie dát do výstupných CSV súborov.

6.3 SQL Databáza ako centrálne forenzné úložisko

Rozhodnutie využiť relačnú databázu (Microsoft SQL Server) ako centrálne úložisko je podložené viacerými technickými a forenznými, analytickými a výskumnými benefitmi.

Po prvé, relačný model SQL umožňuje zachovať logické väzby medzi entitami, ktoré by pri priamom exporte do CSV zanikli. Napríklad vzťah medzi rodičovským procesom a jeho potomkami, alebo väzba medzi sieťovým spojením a procesom, ktorý ho inicioval, je prirodzene reprezentovateľná pomocou cudzích kľúčov.

Po druhé, SQL databázy poskytujú robustný mechanizmus pre zabezpečenie integrity dát prostredníctvom transakčného spracovania (ACID vlastnosti) a žurnálovania. To je kľúčové pre preukázateľnosť, že dáta neboli počas procesu zberu poškodené alebo modifikované chybou zápisu.

6.4 Zberný agent

Použitie dedikovaného agenta je pre forenzný zber na platforme Windows nevyhnutné predovšetkým kvôli zachovaniu integrity dôkazov a schopnosti získať uzamknuté systémové dáta. Na rozdiel od "agentless" metód (PowerShell/WinRM), ktoré spustením skriptov výrazne menia obsah pamäte RAM, prepisujú logy a zanechávajú masívnu stopu, optimalizovaný agent operuje s minimálnym dopadom na systém. Kľúčovou výhodou agenta je schopnosť pristupovať priamo k fyzickému disku, vďaka čomu dokáže extrahovať aj súbory, ktoré operačný systém drží uzamknuté pre čítanie (napr. $MFT, registre SAM/SYSTEM), bez nutnosti spoliehať sa na limitované Windows API alebo vytvárať tieňové kópie.

Z prevádzkového hľadiska agent zabezpečuje stabilitu a škálovateľnosť, ktorú skriptovacie nástroje nedokážu garantovať. Zatiaľ čo WinRM relácie sú náchylné na výpadky siete a pri hromadnom zbere môžu zahltiť infraštruktúru, agent dokáže dáta zbierať lokálne, asynchrónne ich buffrovať a odoslať až pri stabilnom spojení. Navyše, digitálne podpísaný binárny agent je spravidla legitímnou súčasťou bezpečnostnej politiky. Oproti tomu sú komplexné PowerShell skripty, nutné pre hĺbkový prieskum, modernými EDR/AV systémami často blokované ako podozrivá aktivita. Takéto zablokovanie dokáže znemožniť vyšetrovanie v tom najnevhodnejšom čase krízy, akou kyberbezpečnostné incidenty často bývajú.

Pre potreby agenta sme definovali nasledovné požiadavky (***Tab. 4***):

Parameter	Požiadavka	Odôvodnenie pre ADFIR
Minimálny dopad	Agent musí bežať s minimálnou spotrebou CPU/RAM.	Prevencia narušenia produkčných systémov a prepísania volatile artifacts v pamäti.
Integrita	Využitie kryptografických hašov (SHA-256) pri každom zázname.	Zabezpečenie reťazca dôkazov (Chain of Custody) pre právne účely.
Škálovateľnosť	Schopnosť spracovať 100 000+ záznamov (napr. MFT) v reálnom čase.	Forenzná analýza moderných diskov s miliónmi súborov vyžaduje robustný backend (SQL).

Tab. 4 - Požiadavky na agenta