ANALÝZA FORENZNÝCH ARTEFAKTOV WEBOVÝCH PREHLIADAČOV V OPERAČNÝCH SYSTÉMOCH WINDOWS

DIPLOMOVÝ SEMINÁR Z INFORMATIKY
02. 05. 2024

Pracovisko: Ústav informatiky
Autor: Bc. Zuzana Hennelová
Vedúci: doc. RNDr. JUDr. Pavol Sokol, PhD.

Motivácia

- Rôzne nástroje pre každý prehliadač
- Nástroje, ktoré sa nepozerajú do RAM
- Málo dokumentácie artefaktov
- Málo informácií o inkognito módoch a TOR
- Nástroje iba zobrazujú dáta

Zdroj: icons8

Ciele práce

01 Vyhodnotenie prístupov k analýze forenzných artefaktov.

02 Návrh spôsobu extrakcie, korelácie a reprezentácie artefaktov pri analýze vypnutých a zapnutých zariadení.

03 Tvorba nástroja pre analýzu artefaktov so zameraním na identifikáciu relevantných stôp a vzťahov medzi nimi.

Artefakty

SQLite databázy – história, sťahovanie, cookies, záložky,...

Prefetch súbory, amcache – spustenia programov

Súborový systém (MFT) – stiahnuté súbory

Rozšírenia

Zdroj: https://www.opensourceforu.com/wp-content/uploads/2020/12/SQLite-data-featured-image.jpg

Odkiaľ čerpať dáta?

ARSENAL RECON

Image Filename	OS	Source / Project
BloomCON2022Forensics Challenge.E01	Windows 10 Pro	Bloomsburg University / BloomCON Forensics Challenge 2022
sda Image.E01	Windows 10 Pro	Cellebrite / CTF 2021
Narcos-1.001	Windows 10 Pro	Digital Corpora / Narcos Scenario 2019
Narcos-2.001	Windows 10 Pro	Digital Corpora / Narcos Scenario 2019
Narcos-3.001	Windows 10 Pro	Digital Corpora / Narcos Scenario 2019
Horcrux.E01	Windows 10 Pro & Kali Linux	DefCon / CTF 2019
LoneWolf.E01	Windows 10 Education	Digital Corpora / Lone Wolf Scenario 2018
bart.E01	Windows 11 Pro	Nuno Mourinho, Mario Candeias, and Rogerio Bravo / ForensicVM Showcase 2023 - Bart the hacker
MaxPowersCDrive.E01	Windows 10 Enterprise	Magnet / CTF 2018
MUS-CTF-19-DESKTOP-001.E01	Windows 10 Enterprise	Magnet / CTF 2019
Laptop1Final.E01	Windows 11 Home Insider Preview	Magnet / CTF 2022
PC-MUS-001.E01	Windows 11 Home	Magnet / CTF 2023
HD1.E01	Windows 10 Pro	Digital Corpora / Owl Scenario 2019
base-rd01-cdrive.E01	Windows 10 Enterprise	SANS

Aké prehliadače budeme skúmať?

Extrakcia artefaktov - KAPE

- záznamy udalostí,
- webové prehliadače,
- Windows časová os,
- **súborový systém**,
- evidece of execution,
- **SQLite databázy**
- + nástroje od Erica Zimmermana

www.kroll.com

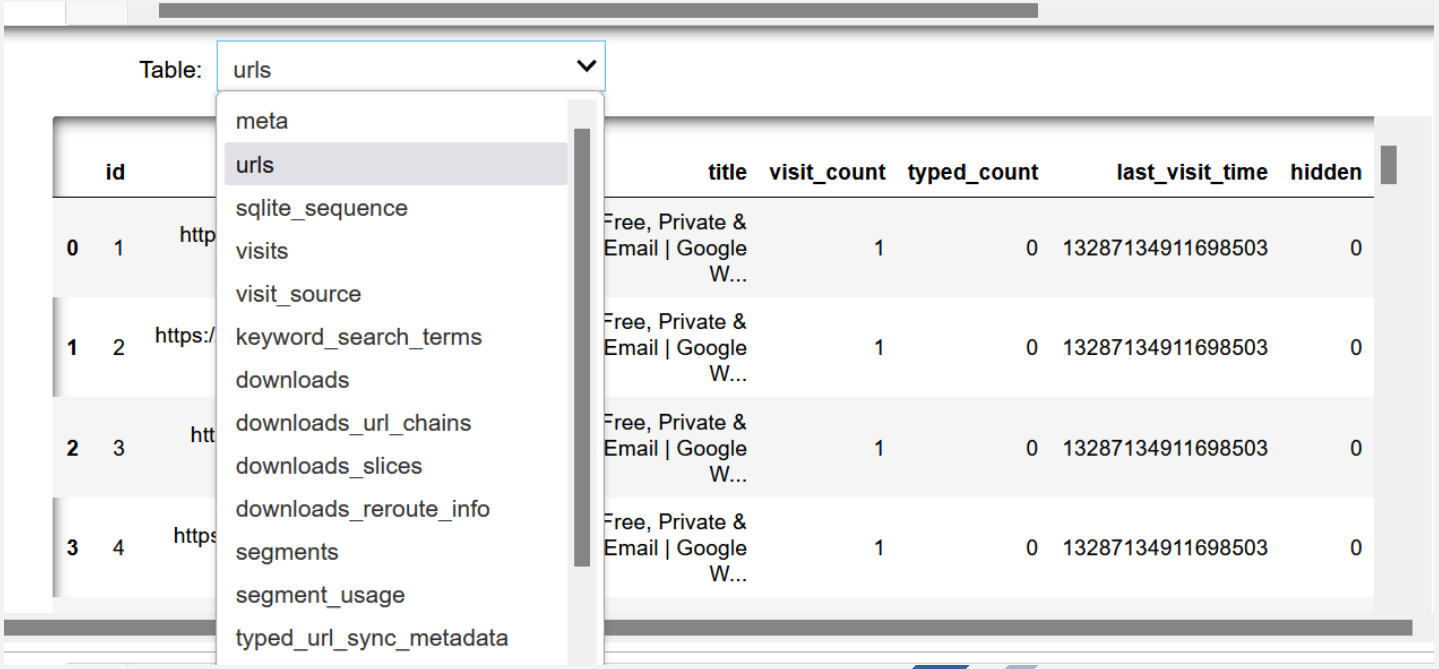
KROLL

Spracovanie dát

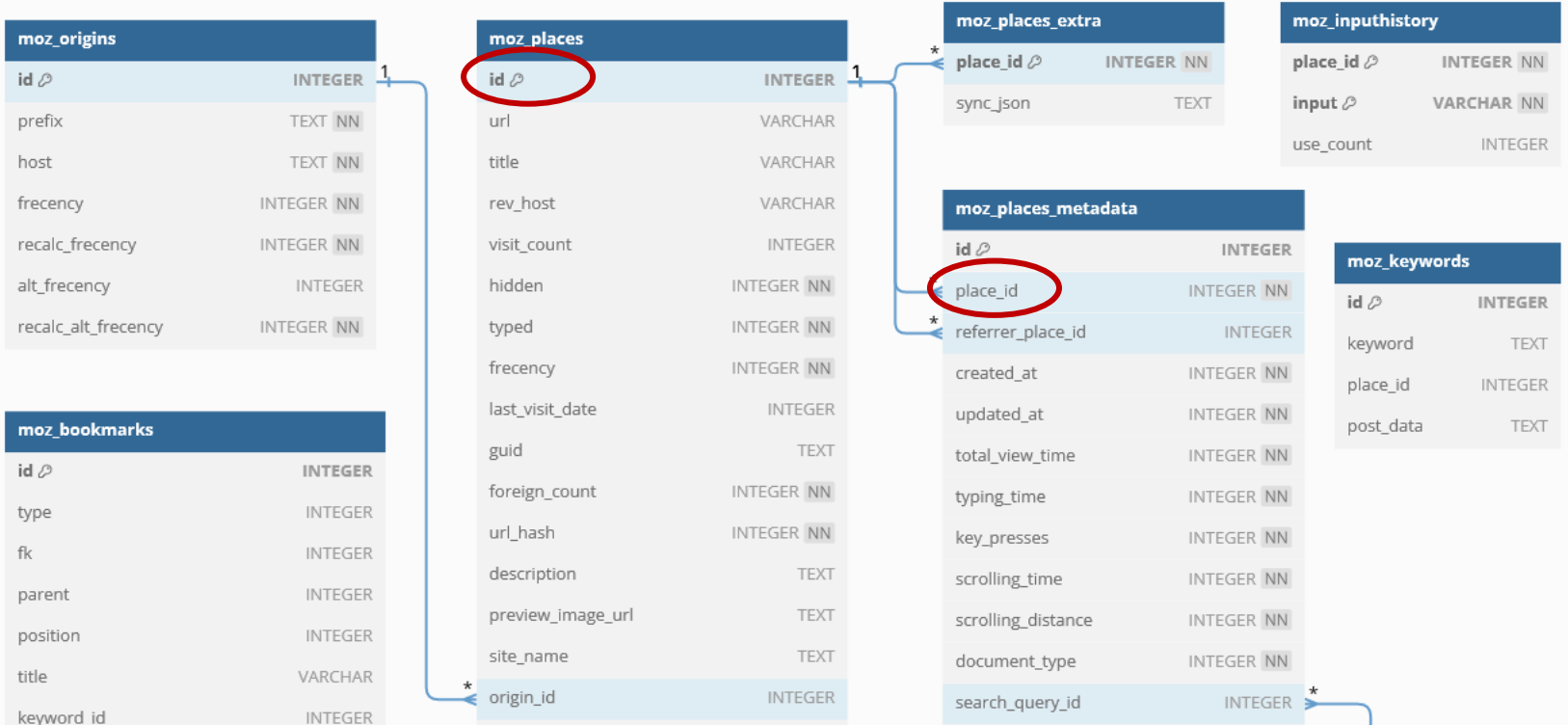
Aplikujeme EZ nástroje, ďalší preprocesing pomocou Python

Name	Version (.net 4 | 6)	Purpose
AmcacheParser	1.5.1.0 | 1.5.1.0	Amcache.hve parser with lots of extra features. Handles locked files
EvtxECmd	1.5.0.0 | 1.5.0.0	Event log (evtx) parser with standardized CSV, XML, and json output! Custom maps, locked file support, and more!
JLECmd	1.5.0.0 | 1.5.0.0	Jump List parser
LECmd	1.5.0.0 | 1.5.0.0	Parse lnk files
MFTECmd	1.2.2.0 | 1.2.2.0	$MFT, $Boot, $J, $SDS, $I30, and $LogFile (coming soon) parser. Handles locked files
PECmd	1.5.0.0 | 1.5.0.0	Prefetch parser
RBCmd	1.5.0.0 | 1.5.0.0	Recycle Bin artifact (INFO2/$I) parser
RecentFileCacheParser	1.5.0.0 | 1.5.0.0	RecentFileCache parser
SQLECmd	1.0.0.0 | 1.0.0.0	Find and process SQLite files according to your needs with maps!
SrumECmd	0.5.1.0 | 0.5.1.0	Process SRUDB.dat and (optionally) SOFTWARE hive for network, process, and energy info!
SumECmd	0.5.2.0 | 0.5.2.0	Process Microsoft User Access Logs found under 'C:\Windows\System32\LogFiles\SUM'
WxTCmd	1.0.0.0 | 1.0.0.0	Windows 10 Timeline database parser

Práca s SQLite pomocou Python



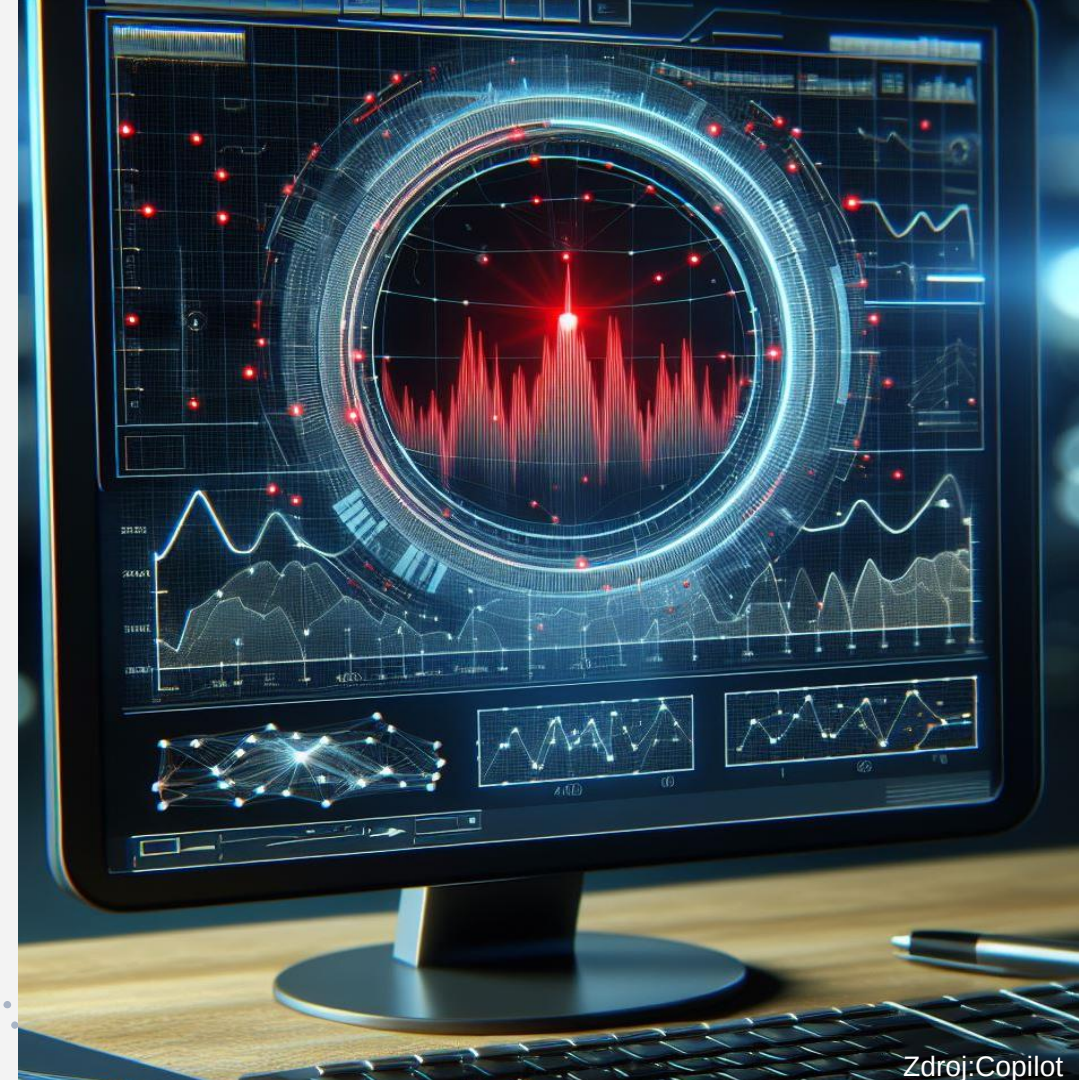
Mapovanie atribútov



Hľadanie anomálií

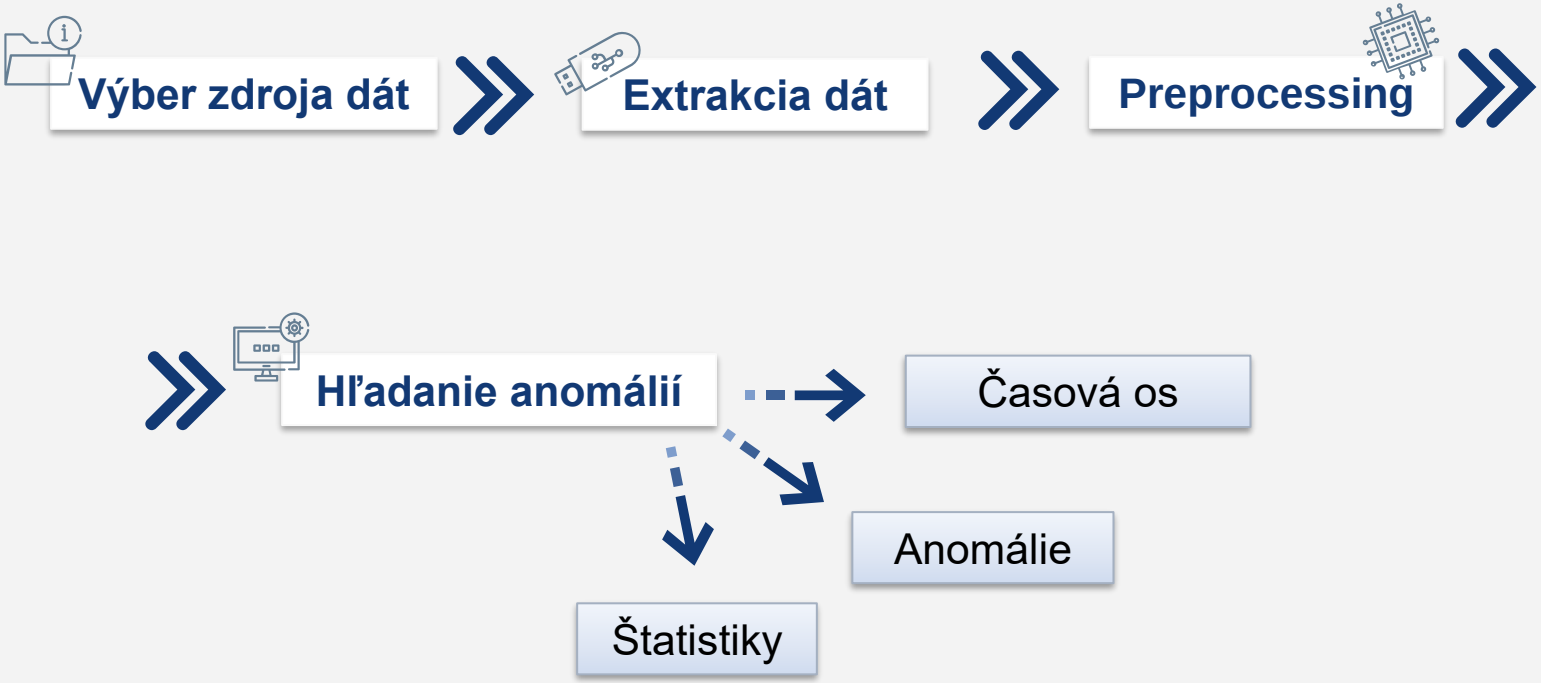
- Málo frekventované operácie
- Záznamy, ktoré sa vyskytujú mimo bežného rámca
- Chýbajúce záznamy

- Metódy bez učiteľa
- PyOD: INNE, ECOD, COPOD, PCA, SOD, ROD, LODA



Zdroj:Copilot

Fungovanie programu



Najbližšie kroky

- Hľadanie vzťahov medzi rôznymi artefaktmi
- Práca s ďalšími datasetmi
- Aplikácia metód hľadania anomálií
- Vyhodnotenie
- ...

Ďakujem za pozornosť.

https://s.ics.upjs.sk/~zuzana_hennelova/thesis.html