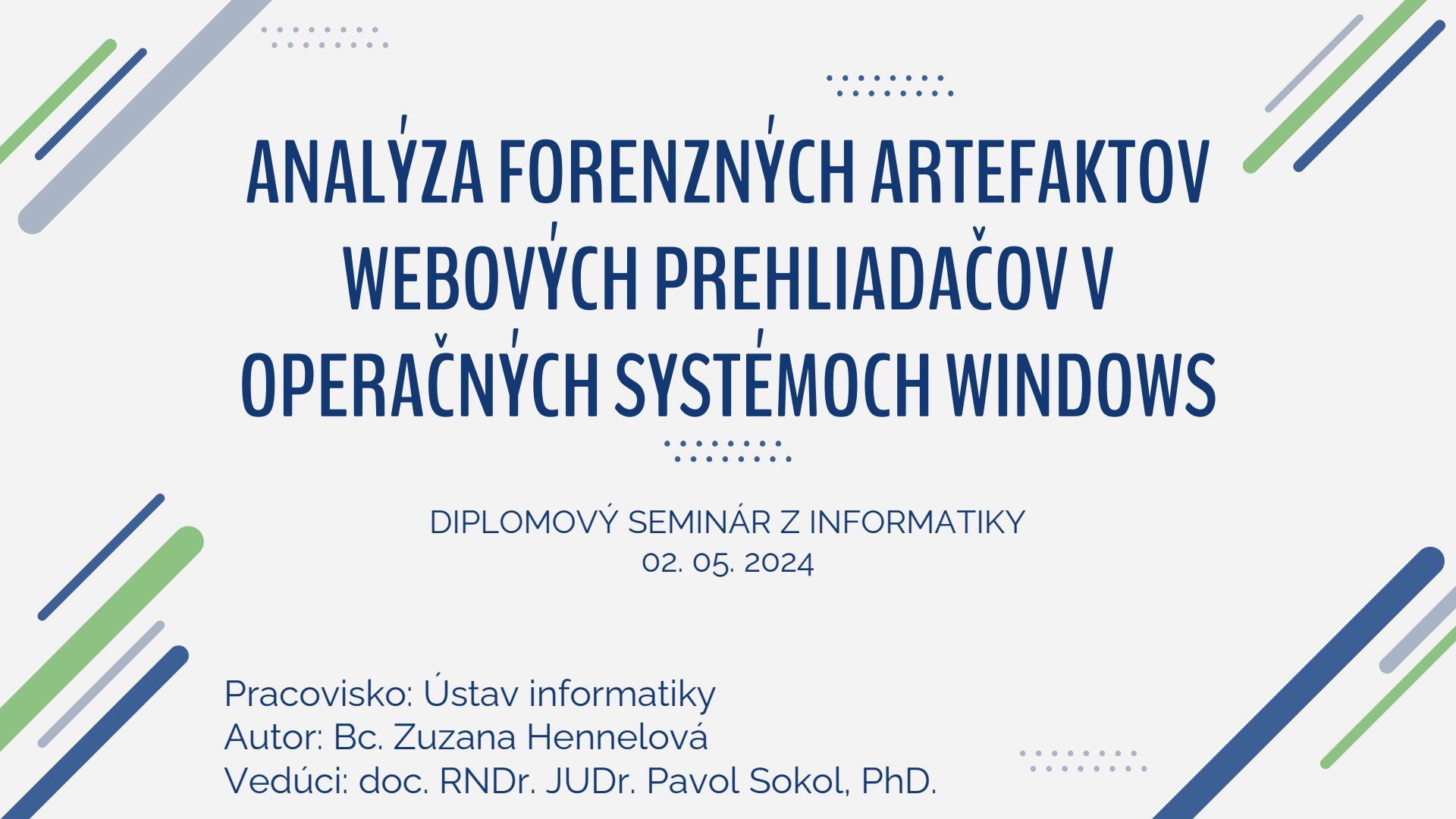




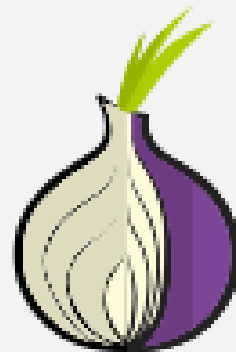
ANALÝZA FORENZNÝCH ARTEFAKTOV WEBOVÝCH PREHLIADAČOV V OPERAČNÝCH SYSTÉMOCH WINDOWS

DIPLOMOVÝ SEMINÁR Z INFORMATIKY
02. 05. 2024

Pracovisko: Ústav informatiky
Autor: Bc. Zuzana Hannelová
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



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 čerpat 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
		Nuno Mourinho, Mario Candeias, and Rogerio Bravo / ForensicVM Showcase 2023 - Bart the hacker
bart.E01	Windows 11 Pro	
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?



statcounter
GlobalStats

[Press Releases](#) [FAQ](#) [About](#) [Feedback](#)

Chrome

65.38%

Edge

12.75%

Safari

8.72%

Firefox

7.26%

Opera

3.05%

360 Safe

0.93%

Desktop Browser Market Share Worldwide - February 2024

Extrakcia artefaktov - KAPE

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

www.kroll.com



Spracovanie dát

Aplikujeme EZ nástroje, ďalší preprocessing 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 Ink 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
SQLLECmd	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

Table:		urls					
		meta					
		urls					
		sqlite_sequence					
		visits					
		visit_source					
		keyword_search_terms					
		downloads					
		downloads_url_chains					
		downloads_slices					
		downloads_reroute_info					
		segments					
		segment_usage					
		typed_url_sync_metadata					
			title	visit_count	typed_count	last_visit_time	hidden
0	1	http	Free, Private & Email Google W...	1	0	13287134911698503	0
1	2	https://	Free, Private & Email Google W...	1	0	13287134911698503	0
2	3	htt	Free, Private & Email Google W...	1	0	13287134911698503	0
3	4	https	Free, Private & Email Google W...	1	0	13287134911698503	0

Mapovanie atribútov

moz_origins	
id	INTEGER
prefix	TEXT NN
host	TEXT NN
frecency	INTEGER NN
recalc_frecency	INTEGER NN
alt_frecency	INTEGER
recalc_alt_frecency	INTEGER NN

moz_bookmarks	
id	INTEGER
type	INTEGER
fk	INTEGER
parent	INTEGER
position	INTEGER
title	VARCHAR
keyword_id	INTEGER

moz_places	
id	INTEGER
url	VARCHAR
title	VARCHAR
rev_host	VARCHAR
visit_count	INTEGER
hidden	INTEGER NN
typed	INTEGER NN
frecency	INTEGER NN
last_visit_date	INTEGER
guid	TEXT
foreign_count	INTEGER NN
url_hash	INTEGER NN
description	TEXT
preview_image_url	TEXT
site_name	TEXT
origin_id	INTEGER

moz_places_extra	
place_id	INTEGER NN
sync_json	TEXT

moz_places_metadata	
id	INTEGER
place_id	INTEGER NN
referrer_place_id	INTEGER
created_at	INTEGER NN
updated_at	INTEGER NN
total_view_time	INTEGER NN
typing_time	INTEGER NN
key_presses	INTEGER NN
scrolling_time	INTEGER NN
scrolling_distance	INTEGER NN
document_type	INTEGER NN
search_query_id	INTEGER

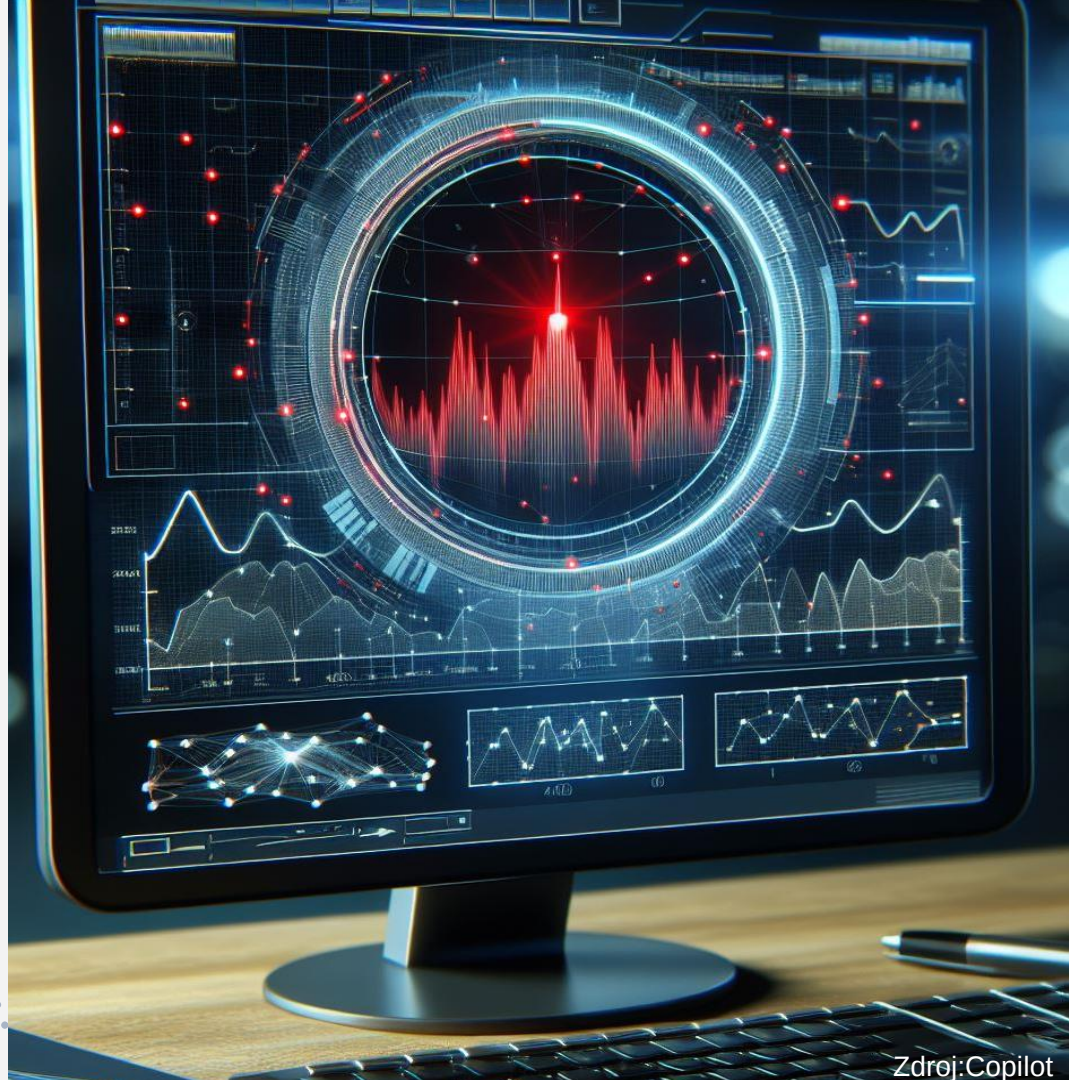
moz_inputhistory	
place_id	INTEGER NN
input	VARCHAR NN
use_count	INTEGER

moz_keywords	
id	INTEGER
keyword	TEXT
place_id	INTEGER
post_data	TEXT



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





Výber zdroja dát



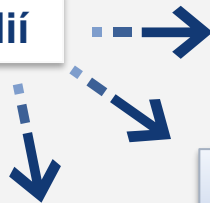
Extrakcia dát



Preprocessing



Hľadanie anomálií



Časová os

Anomálie

Štatistiky

Fungovanie
programu

Najbližšie kroky

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





Ďakujem za pozornosť.

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

CREDITS: This presentation template was created by [Slidesgo](#), and includes icons by [Flaticon](#), and infographics & images by [Freepik](#)