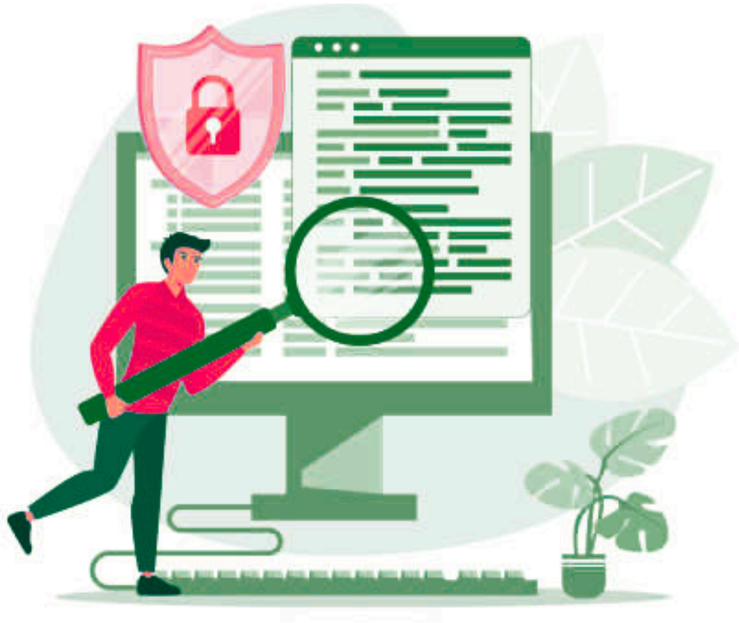
Identifikácia relevantných digitálnych stôp pri forenznom vyšetrovaní

PF UPJŠ, Ústav informatiky
17.4.2024

Bc. František Kurimský
doc. RNDr. JUDr. Pavol Sokol, PhD.

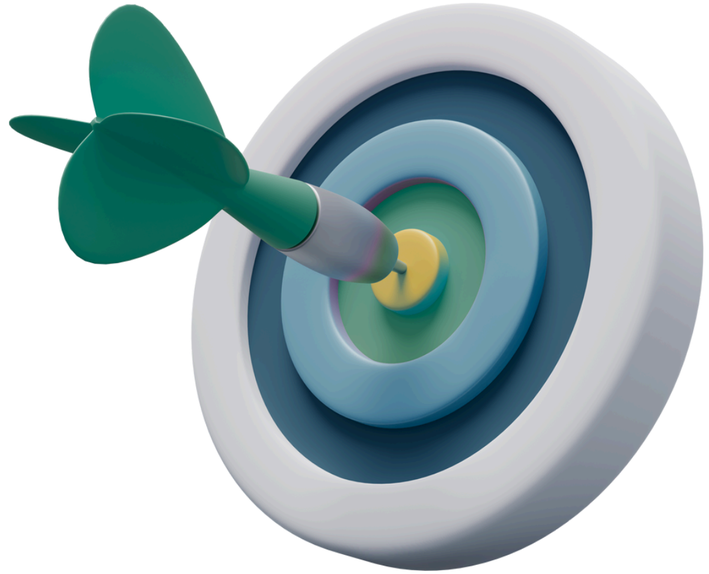
Motivácia

- Čo najrýchlejšie sa dopracovať k relevantným digitálnym stopám (dátam)
- Veľa nerelevantných záznamov z monitorovacích zariadení
- Lepšia orientácia v dátach pre forenzných analytikov
- Ušetriť čas forenzného analytika pri hľadaní relevantných dát



Cieľ

- Identifikácia vhodnej reprezentácie forenzných artefaktov v dátových rámcoch (dataframeoch) a transformácia dát
- Automatizovať identifikáciu relevantných digitálnych stôp



Príprava dát I.

- Vstupom je obraz disku operačného systému Windows so súborovým systémom NTFS
- Vytvorenie časovej osi pomocou nástroja Log2timeline
  - `log2timeline.py --parsers=win7_slow --status_view window –storage <file>.E01 --partitions "all"`
- Nástroj psort.py sme prevedli získané dáta do čitateľnej tabuľkovej podoby
  - `psort.py --status-view window --output_time_zone utc -o l2tcsv -w timeline.csv timeline.dump`

Príprava dát II.

- Binarizácia dát
- timestamp = ’M’, ’A’, ’C’, ’B’,
- source type = ’file stat’, ’NTFS file stat’, ’file entry shell item’, ’NTFS USN change’,
- file type = ’filef’, ’directory’,’link’,
- dir type = ’dir appdata’, ’dir win’, ’dir user’, ’dir other’,
- file type2 = ’file executable’, ’file graphic’, ’file documents’,’file ps’, ’file other’,
- file format = ’mft’, ’lnk shell items’, ’olecf olecf automatic destinations/lnk/shell items’, ’winreg bagmru/shell items’, ’usnjrnl’,

Agregácia dát I.

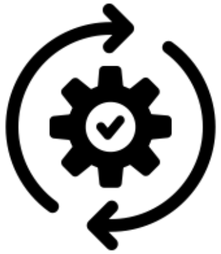
- Agregácia dát naprieč atribútom “inode”
- Agregačné funkcie

sum	**modifikované z-score**
max	**robustné z-score**
mean	**frekvencie v rámci dní I.**
z-score	**frekvencie v rámci dní II.**

Detekcia anomálií

- V prípade útoku je s veľkou pravdepodobnosťou aktivita útočníka anomáliou, teda neštandardnou aktivitou.
- Množina aktivít/udalostí, detegovaných v systéme ako anomália má veľký prienik s množinou aktivít útočníka

Metódy



METÓDA	NÁZOV	TYP
COPOD	Copula Based Outlier Detector	Unsupervised
ECOD	Empirical-Cumulative-distribution-based Outlier Detection	Unsupervised
INNE	Isolation-based Anomaly Detection Using Nearest-Neighbor Ensembles	Unsupervised
IForest	Isolation Forest	Unsupervised
LODA	Lightweight on-line detector of anomalies	Unsupervised
LOF	Local Outlier Factor	Unsupervised
PCA	Principal Component Analysis	Unsupervised

Parametre pre metódy

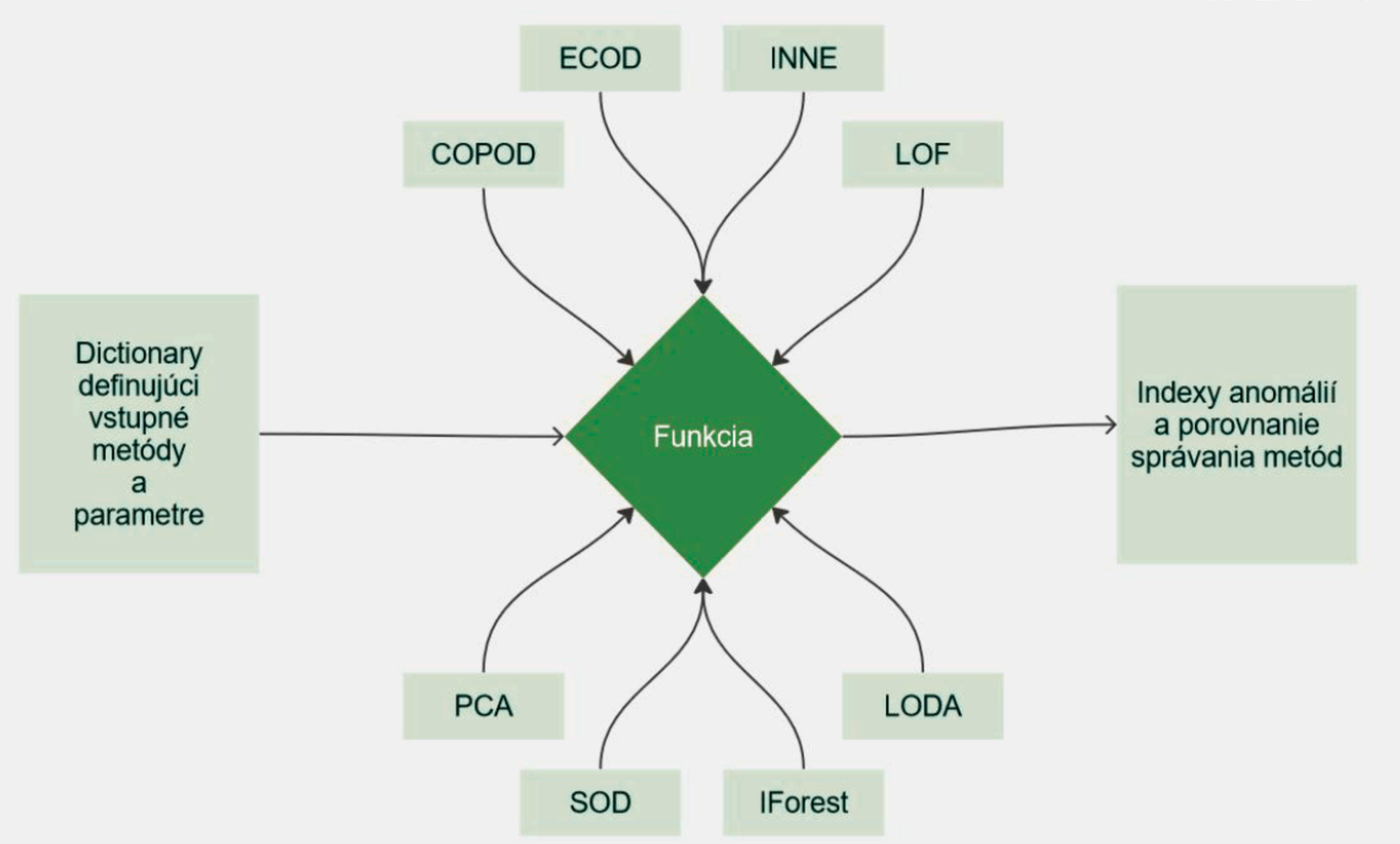
PARAMETER	VSTUP	VYSVETLENIE
n_jobs	int, optional (default=1)	Ak je hodnota -1, počet úloh sa nastaví na počet dostupných jadier procesora.
n_neighbors	int, optional (default=20)	Počet susedov, ktorý sa predvolene použije pre dotazy k-neighbors. Ak je n_neighbors väčšie ako počet poskytnutých vzoriek, použijú sa všetky vzorky.
metrics	string or callable, default ‘minkowski’	-
n_bins	int or string, optional (default=10)	Počet binov pre histogram. Ak je nastavené na "auto", použije sa metóda Birge-Rozenblac na automatické určenie optimálneho počtu binov.
n_estimators	int, default=200	Počet základných odhadcov v súbore.
contamination	float in (0., 0.5), optional (default=0.1)	Podiel anomálií v dátovej sade.

Metriky

City-block	$D_C(x,y) = \sum_{i=1}^{n} \lvert x_i - y_i \rvert$
Euklidovská	$D_E(x,y) = \sum_{i=1}^{n} \sqrt{(x_i - y_i)^2}$
Chebyshevova	$D_{Ch}(x,y) = \max_{i=1}^{n}(\lvert x_i - y_i \rvert)$
Canberrova	$D_{Can}(x,y) = \sum_{i=1}^{n} \frac{\lvert x_i - y_i \rvert}{\lvert x_i \rvert + \lvert y_i \rvert}$

Jaccardova	$D_{Jacc}(x,y) = \frac{\lvert x \cap y \rvert}{\lvert x \cup y \rvert}$
Cosínusová	$\mathrm{D}_{cos} = 1 - \frac{\sum_{i=1}^{n} \frac{x_i y_i}{\lvert x_i \rvert + \lvert y_i \rvert}}{\sqrt{\sum_{i=1}^{n} x_i^2}\ \sqrt{\sum_{i=1}^{n} y_i^2}}$
Minkovského	$D_{M,p} = (\sum_{i=1}^{n} \lvert x_i - y_i \rvert^p)^{\frac{1}{p}}$
Braycurtisova	$\sum_{i=1}^{n} \lvert x_i - y_i \rvert \ / \sum_{i=1}^{n} \lvert x_i + y_i \rvert$

Návrh riešenia

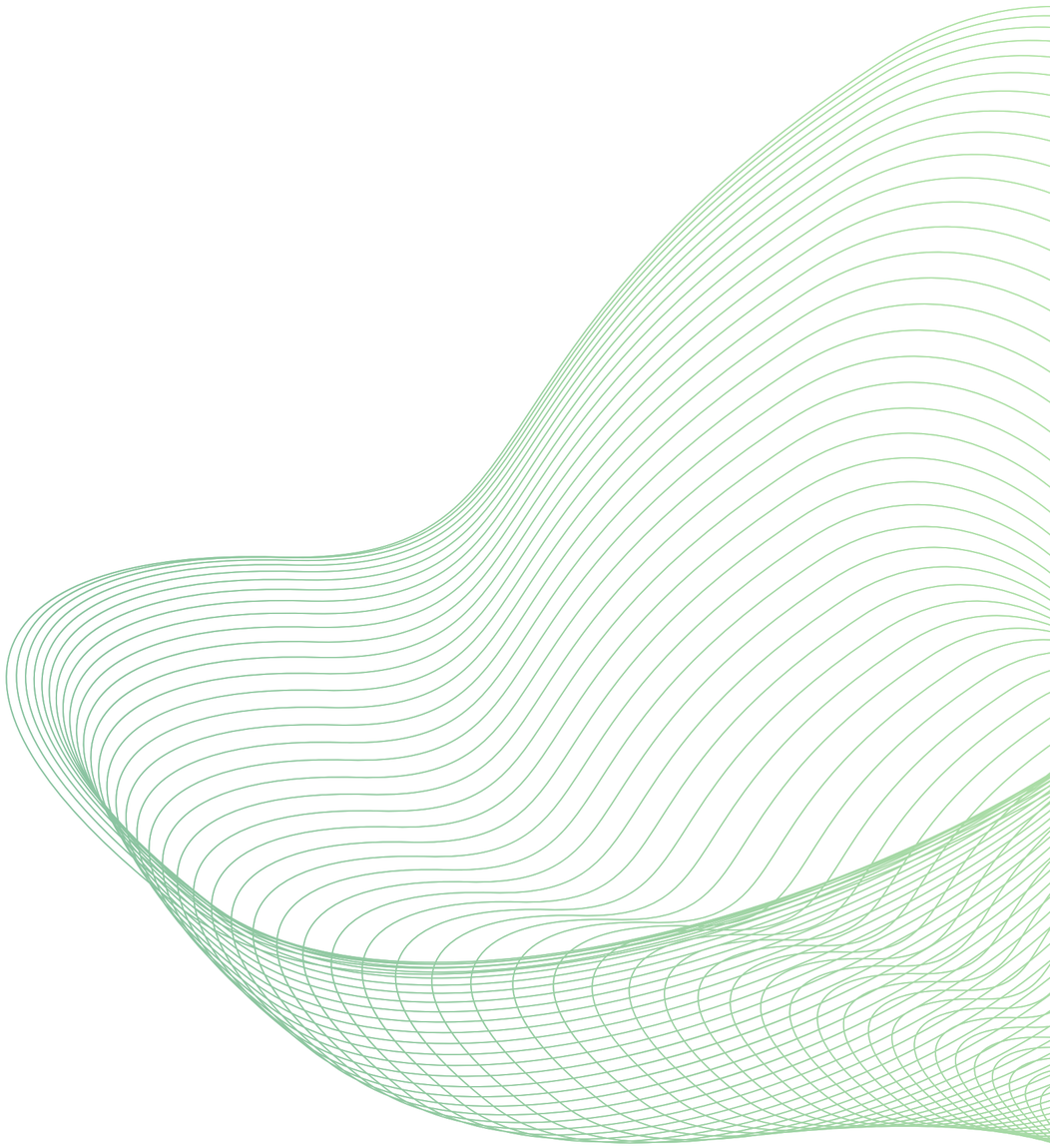


comb	final_score
20274-NTFS:\FileShare\Secret\PortalGunPlans.txt	17
86967-NTFS:\FileShare\Secret\NoJerry.txt	17
87102-NTFS:\$Recycle.Bin\S-1-5-21-2232410529-1445159330-2725690660-500\$IU2L112.txt	17
87111-NTFS:\FileShare\Secret\Beth_Secret.txt	17
1-NTFS:\$MFTMirr	16
34-NTFS:\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000002	16
84656-NTFS:\$Extend\$UsnJrnl:$J	16
87132-NTFS:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCookies\Y8KFNFMU.txt	16
0-NTFS:\$MFT	15
19402-NTFS:\ProgramData\Start Menu	15
19515-NTFS:\ProgramData\Desktop	15
19516-NTFS:\ProgramData\Documents	15
19518-NTFS:\Documents and Settings	15
19519-NTFS:\ProgramData\Templates	15
19557-NTFS:\ProgramData\Application Data	15
29-NTFS:\$Extend\$RmMetadata\$TxfLog	15
30-NTFS:\$Extend\$RmMetadata\$Txf	15
73635-NTFS:\$Recycle.Bin\S-1-5-21-2232410529-1445159330-2725690660-500\$RU2L112.txt	15
84978-NTFS:\Users\Administrator\AppData\Local\Application Data	15
84980-NTFS:\Users\Administrator\AppData\Local\History	15
84981-NTFS:\Users\Administrator\AppData\Local\Temporary Internet Files	15
84982-NTFS:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files	15
85025-NTFS:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Internet Explorer.lnk	15
NTFS:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Windows PowerS	15
86-NTFS:\Boot\memtest.exe	15
\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\9b9cdc69c1c24e2b.automaticDes	15
7085-NTFS:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1024_768_POS4.J	15
87089-NTFS:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\Low\Content.IE5	15
FS:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\28c8b86deab549a1.customDestin	15
106-NTFS:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_2306_1230_POS4.J	15
87112-NTFS:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\Beth_Secret.lnk	15
\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1bc392b8e104a00e.automaticDes	15
10-NTFS:\$UpCase	14
11-NTFS:\$Extend	14
WinSxS\amd64_microsoft.windows.powershell.common_31bf3856ad364e35_6.3.9600.16384_none_219db062ef302354\Winc	14
19535-NTFS:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools\Windows PowerShell (x86).lnk	14
s\WinSxS\amd64_microsoft.windows.powershell.common_31bf3856ad364e35_6.3.9600.16384_none_219db062ef302354\W	14

Návrh riešenia

PF UPJŠ, Ústav informatiky
17.4.2024

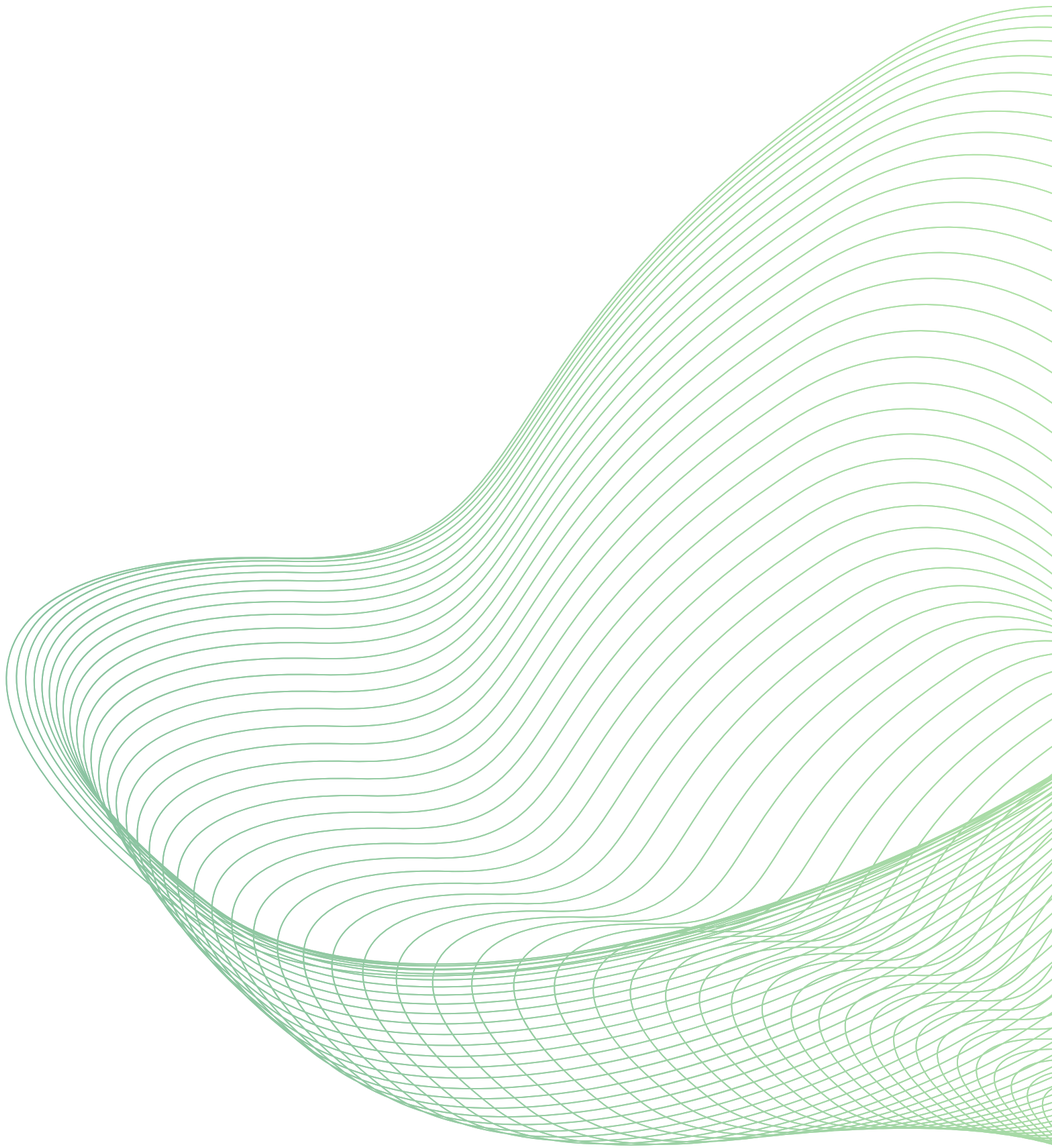
Ďakujem za pozornosť



PF UPJŠ, Ústav informatiky
17.4.2024

Bc. František Kurimský
doc. RNDr. JUDr. Pavol Sokol, PhD.

Otázky



PF UPJŠ, Ústav informatiky
17.4.2024

Bc. František Kurimský
doc. RNDr. JUDr. Pavol Sokol, PhD.