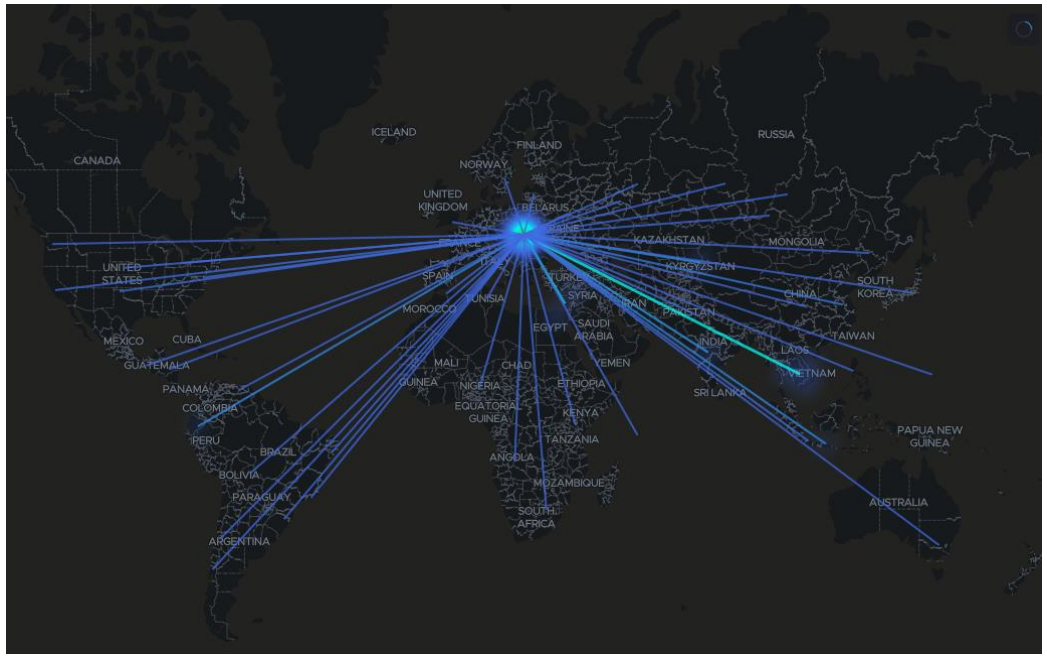
Informačná a kybernetická bezpečnosť - bakalárske práce

CSIRT UPJS

Cyber Security Lab

CSIRT-UPJS

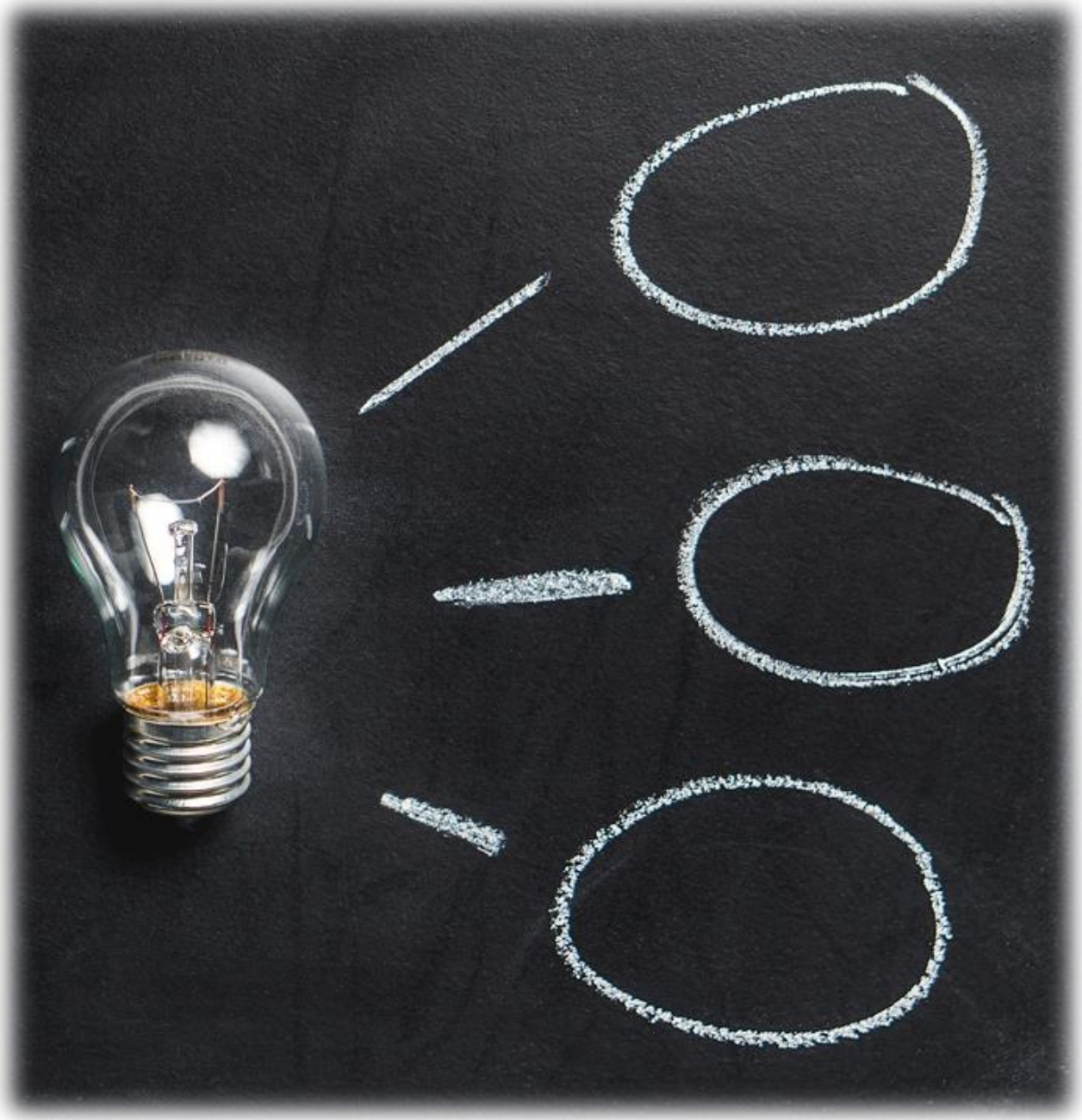
- 1. akademický CSIRT v Slovenskej republike
- Proaktívne a reaktívne činnosti
  - Ochrana voči bezpečnostným hrozbám
  - Riešenie bezpečnostných incidentov
  - ...



Slovakia	
Beset-Cirt	Listed (since 20 Sep 2021)
Binconf CDC (SK)	Accredited (since 20 Sep 2018)
CSIRT-UPJS	Accredited (since 19 Oct 2020)
CSIRT.MIL.SK	Accredited (since 12 Feb 2018)
CSIRT.SK	Accredited (since 06 May 2011)
ENERGOTEL.SK-CSIRT	Accredited (since 13 Nov 2022)
GOV CERT SK	Listed (since 16 Mar 2022)
IstroCSIRT (SK)	Accredited (since 17 Sep 2022)
SK-CERT	Certified (since 26 Mar 2020)
VNET CSIRT (SK)	Listed (since 11 Apr 2022)
VOID SOC	Accredited (since 01 Nov 2019)
ws-csirt	Listed (since 16 Apr 2021)

Čo robíme?

- Dátová analýza v oblasti bezpečnosti
- Detekcia a predikcia bezpečnostných udalostí
- Analýza bezpečnostných hrozieb
- Honeypoty (pasce na útočníkov)
- Digitálna forenzná analýza
- Riešenie bezpečnostných incidentov
- …



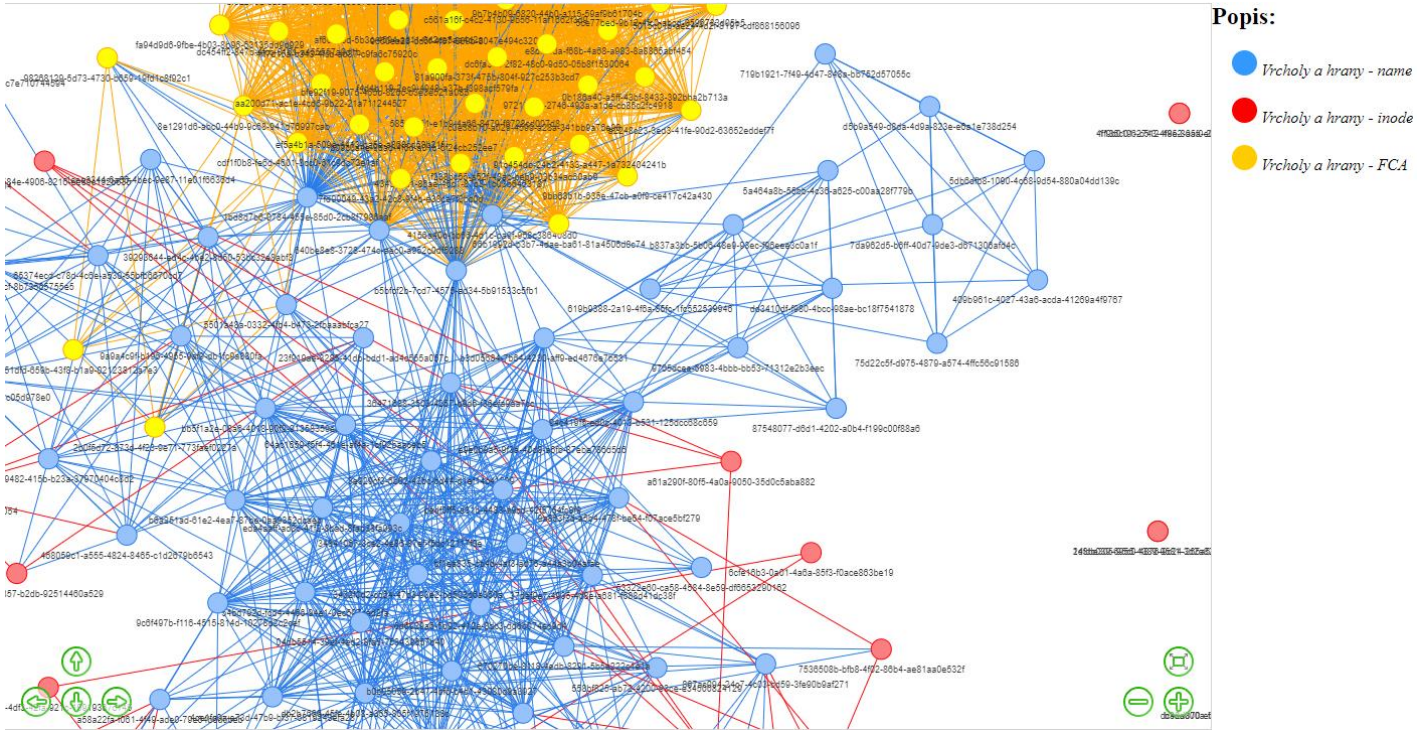
Cyber Security Lab

CSIRT UPJS

Spolupráca


ESET
BINARY CONFIDENCE
di:Sig
CSIRT.SK
cesnet certs
SK NBÚ CERT
CSIRT-MU
shadowserver
HN/P

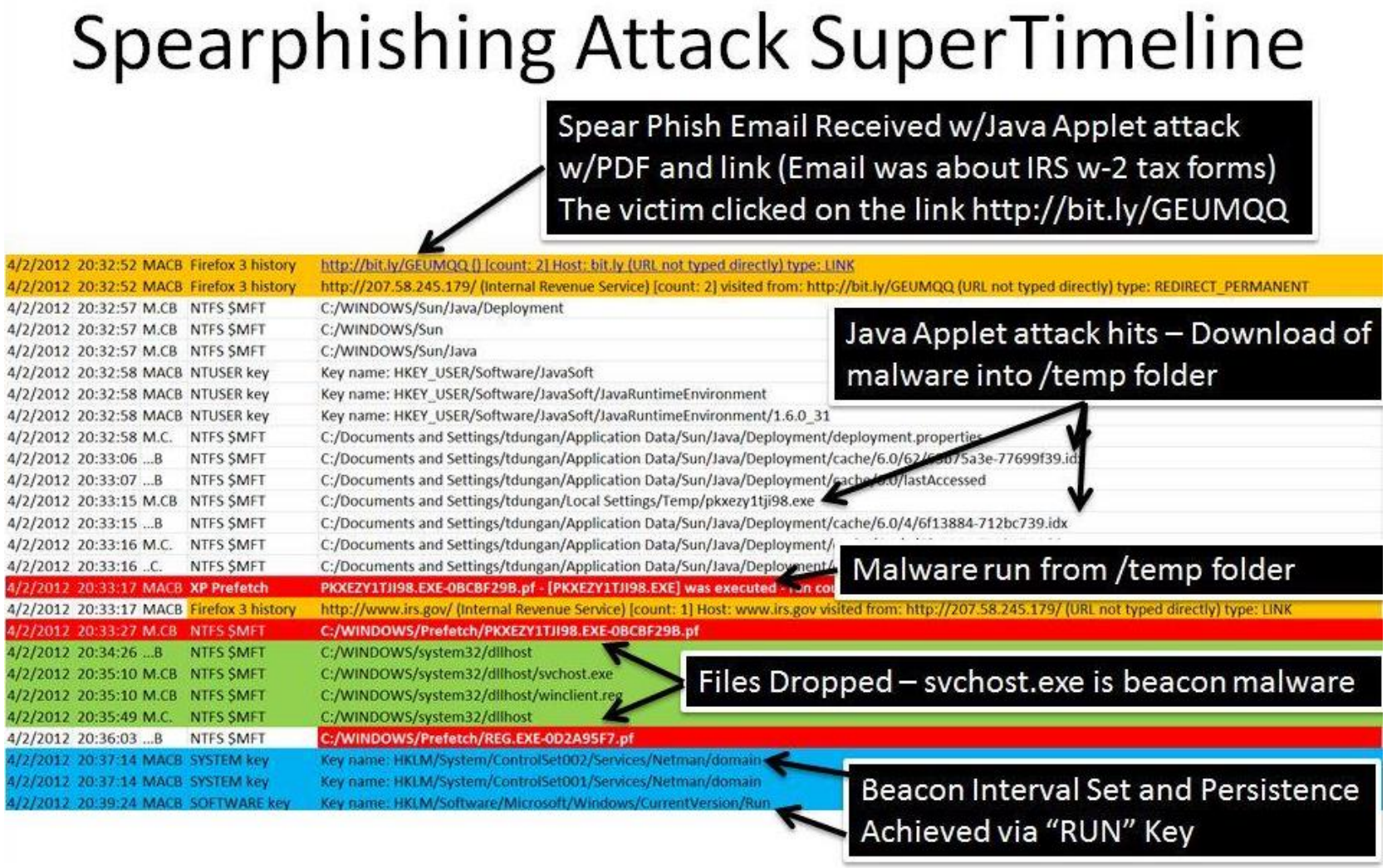
Výskum v oblasti automatizácie digitálnej forenznej analýzy a odpovede na bezpečnostné incidenty.



Analýza digitálnych stôp (I.)

date	time	MACB	sourcetype	type	short
39649	0.06115	MACB	Email PST	Email Read	Message 114: Attachment m57biz.xls Opened
7/20/2008	1:27:40	MACB	XP Prefetch	Last run	EXCEL.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:27:40	.AC.	NTFS $MFT	$SI [.AC.] time	C:/Program Files/Microsoft Office/Office/EXCEL.EXE
7/20/2008	1:27:40	.AC.	UserAssist key	Time of Launch	UEME_RUNPATH:C:/PROGRA~1/MICROS~2/Office/EXCEL.EXE
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:043	MACB	NTFS $MFT	$SI [MACB] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/Desktop.LNK
7/20/2008	1:28:03	MACB	FileExts key	Extension Change	File extension .xls opened by EXCEL.EXE
7/20/2008	1:28:03	MACB	NTFS $MFT	$SI [MACB] time	C:/windows/system32/winsvchost.exe
7/20/2008	1:28:03		SOFTWARE key	Last Written	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7/20/2008	1:27:40		Memory Process	Process Started	winsvchost.exe|1556|1032||0x02476768
7/20/2008	1:27:40		Memory Socket	Socket Opened	4|134.182.111.82:443|Protocol: 6 (TCP)|0x8162de98|||
7/20/2008	1:27:40		XP Prefetch	Last run	WINSVCHOST.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:03	.A..	Shortcut LNK	Access	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:04	MAC.	NTFS $MFT	$SI [MAC.] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist012008072020080
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist012008072020080
7/20/2008	1:28:04	MACB	RecentDocs key	File opened	Recently opened file of extension: .xls - value: m57biz.xls

Analýza digitálnych stôp (II.)



Automatizovaná analýza digitálnych stôp (I.)

Názov: Dátové sady pre automatizovanú analýzu digitálnych stôp

- Vedúci: Pavol Sokol / Tomáš Bajtoš / Rastislav Krivoš-Belluš

(1) Analyzovať dostupné dátové sady vzhľadom na presnosť, reprezentatívnosť a aktuálnosť z hľadiska digitálnych forenznej analýzy.

(2) Navrhnúť spôsob vytvorenia novej dátovej sady alebo rozšírenia existujúcej dátovej sady.

(3) Navrhnúť a implementovať metódy na efektívne vytvorenie dátových sád pomocou metód strojového učenia.

Automatizovaná analýza digitálnych stôp (II.)

Názov: Anonymizácia digitálnych stôp

- Vedúci: Pavol Sokol / Tomáš Bajtoš / Rastislav Krivoš-Belluš

(1) Analyzovať súčasné prístupy k anonymizácii digitálnych stôp, identifikovať ich výhody a nevýhody a posúdiť ich efektívnosť pri zohľadnení požiadaviek právnej úpravy.
(2) Navrhnúť a implementovať metódu, ktorá využíva de-identifikáciu a kódovanie na odstránenie citlivých údajov z digitálnych stôp.

(3) Vykonať experimenty na posúdenie efektívnosti navrhnutej metódy z hľadiska ochrany súkromia, zníženia veľkosti dát a zachovania užitočnosti údajov pre analytické účely.

Automatizovaná analýza digitálnych stôp (III.)

Názov: Detekcia anomálii v digitálnych stopách pomocou analýzy časových radov

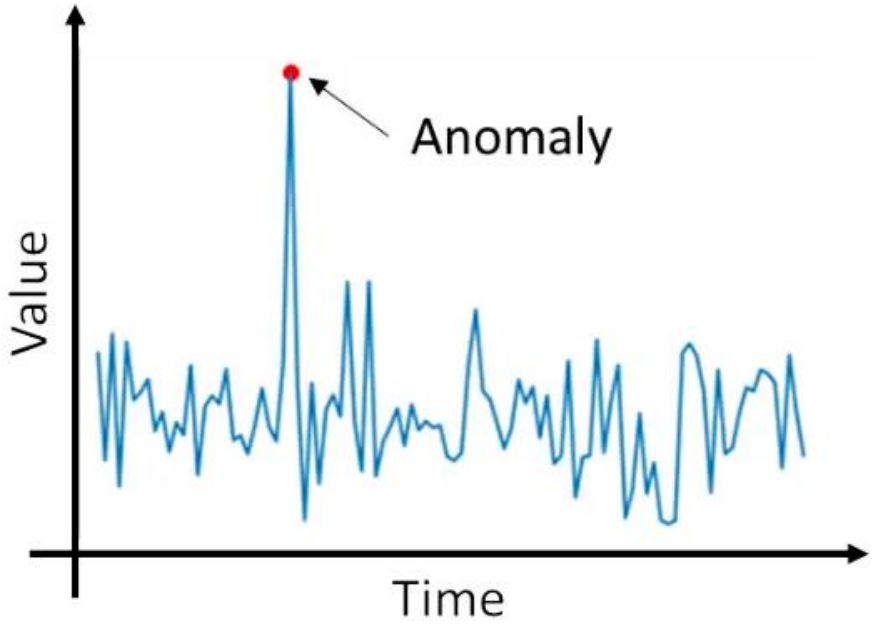
- Vedúci: Pavol Sokol / Tomáš Bajtoš / Rastislav Krivoš-Belluš

(1) Preskúmať existujúce prístupy k detekcii anomálií v digitálnych stopách.

(2) Vybrať vhodné prístupy na identifikáciu nezvyčajného správania v digitálnych stopách pomocou analýzy časových radov.

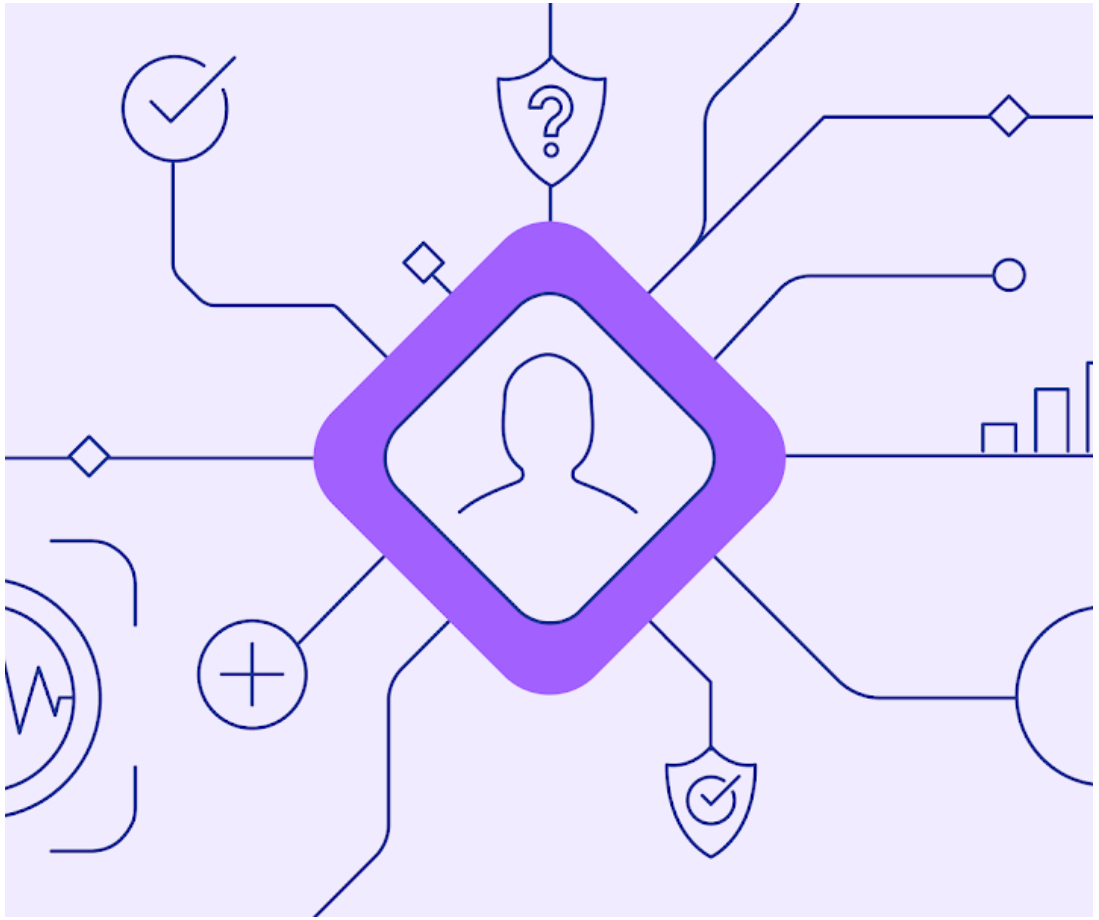
(3) Implementovať a otestovať vybrané prístupy.

(4) Vyhodnotiť efektivitu navrhnutého riešenia.



Zdroj: https://www.linkedin.com/pulse/anomaly-detection-cyber-security-via-machine-learning-deepak-kumar/

Automatizovaná analýza digitálnych stôp (IV.)



Zdroj: https://deepmind.google/discover/blog/best-practices-for-data-enrichment/

Názov: Obohocovanie forenzných artefaktov

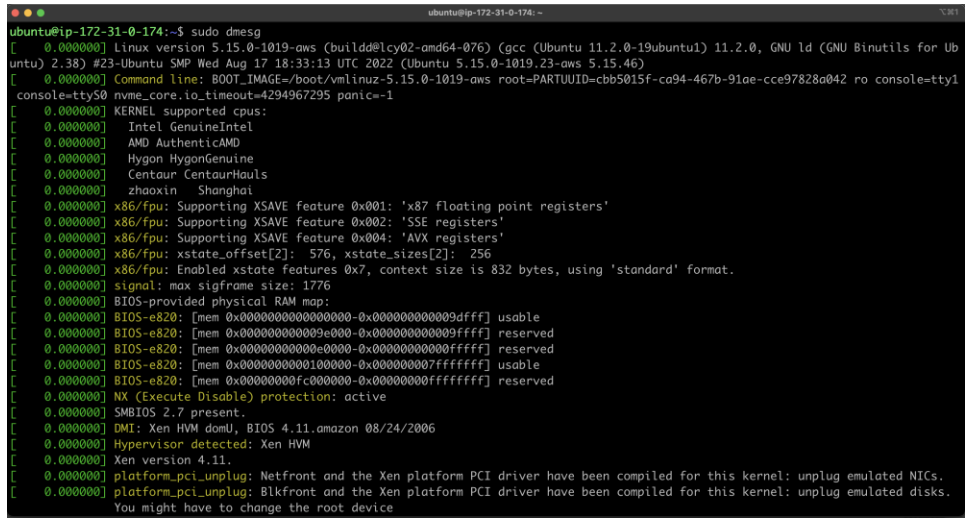
- Vedúci: Pavol Sokol / Tomáš Bajtoš / Rastislav Krivoš-Belluš

- (1) Analyzovať aktuálne prístupy k získavaniu, spracovaniu a interpretácii digitálnych forenzných artefaktov, najmä indikátorov kompromitácie.
- (2) Navrhnúť metódy obohacovania forenzných artefaktov s cieľom zvýšiť informatívnu hodnotu týchto artefaktov.
- (3) Vytvoriť nástroj, ktorý umožní automatizovanú analýzu a doplnenie forenzných artefaktov o relevantné metadáta alebo iné informácie.
- (4) Vyhodnotiť efektívnosť vytvoreného nástroja.

Automatizovaná analýza digitálnych stôp (V.)

Názov: Analýza záznamov (logov) pomocou jazykových modelov

- Vedúci: Pavol Sokol / Tomáš Bajtoš / Rastislav Krivoš-Belluš



Zdroj: https://community.aws/content/2f915mRF2t3iDB2LVQPR6Qmhg02/understanding-log-files-on-your-linux-system

(1) Analyzovať existujúce prístupy k spracovaniu a analýze systémových záznamov, identifikovať ich výhody, nevýhody a obmedzenia, najmä v kontexte veľkého objemu a rôznorodosti údajov.

(2) Preskúmať využitie jazykových modelov v analýze logov.

(3) Navrhnúť a implementovať model, ktorý využíva jazykové modely na automatické spracovanie a analýzu systémových záznamov.

(4) Vyhodnotiť výkonnosť navrhovaného modelu.

Automatizácia reakcie na bezpečnostný incident pre operačný systém MacOS (I.)

Názov: Automatizácia reakcie na bezpečnostný incident pre operačný systém MacOS

Vedúci: Tomáš Bajtoš

- (1) Analýza forenzných artefaktov v operačnom systéme MacOS.
- (2) Analyzovať a porovnať aktuálne prístupy k forenznej analýze operačného systému MacOS.
- (3) Navrhnúť, implementovať a overiť prístup k živej forenznej analýze operačného systému MacOS.

Zdroj: https://en.wikipedia.org/wiki/MacOS

Automatizácia reakcie na bezpečnostný incident pre operačný systém MacOS (II.)

LCDI Patrick Leahy Center for Digital Investigation (LCDI)

Table 13: Yosemite Artifact Location Spreadsheet

Artifact	Location	Description
User Directories		
Downloads Directory	\Users\<user>\Downloads\	User Specific Download Directory
Documents Directory	\Users\<user>\Documents\	User specific Documents Directory
Music Directory	\Users\<user>\Music\	User specific Music Directory
Desktop Directory	\Users\<user>\Desktop\	User Specific Desktop Directory
Library Directory	\Users\<user>\Library\	Hidden directory in Yosemite
Movies Directory	\Users\<user>\Movies\	User Specific Movies directory. Contains video files.
Pictures Directory	\Users\<user>\Pictures\	User Specific Picture Directory
Public Directory	\Users\<user>\Public\	Users public directory
Applications	\Users\<user>\Applications\	User Specific Application Directory containing applications
Applications	\Applications\	Not user-specific
Safari		
Safari Bookmarks	\Users\<user>\Library\Safari\Bookmarks.plist	Plist listing default and user-added Safari bookmarks
Safari Downloads	\Users\<user>\Library\Safari\Downloads.plist	Plist listing files downloaded using Safari Browser
Safari Installed Extensions	\Users\<user>\Library\Preferences\com.apple.Safari.Extensions.plist	Plist describing installed Safari Extensions
Safari Extensions	\Users\<user>\Library\Safari\Extensions\	Directory of Safari Extensions. Safari Extensions utilize .safariextz file extension. Also has a plist listing the extensions
Safari History	\Users\<user>\Library\Safari\History.db	Plist listing Safari web browsing history
Safari History Index	\Users\<user>\Library\Safari\HistoryIndex.sk	An index of Safari History allowing a user to perform keyword searches of visited webpages
Safari Last Session	\Users\<user>\Library\Safari\LastSession.plist	A plist describing the state of Safari when it was last closed
Safari Local Storage Directory	\Users\<user>\Library\Safari\LocalStorage\	A directory for webpage-specific storage. Each webpage stores data in a SQLite database with the file extension of .localstorage.
Safari Local Storage	\Users\<user>\Library\Safari\LocalStorage\StorageT	A database listing the webpage specific

Mac OS X Forensic Artifact Locations Page 10 of 36

LCDI Patrick Leahy Center for Digital Investigation (LCDI)

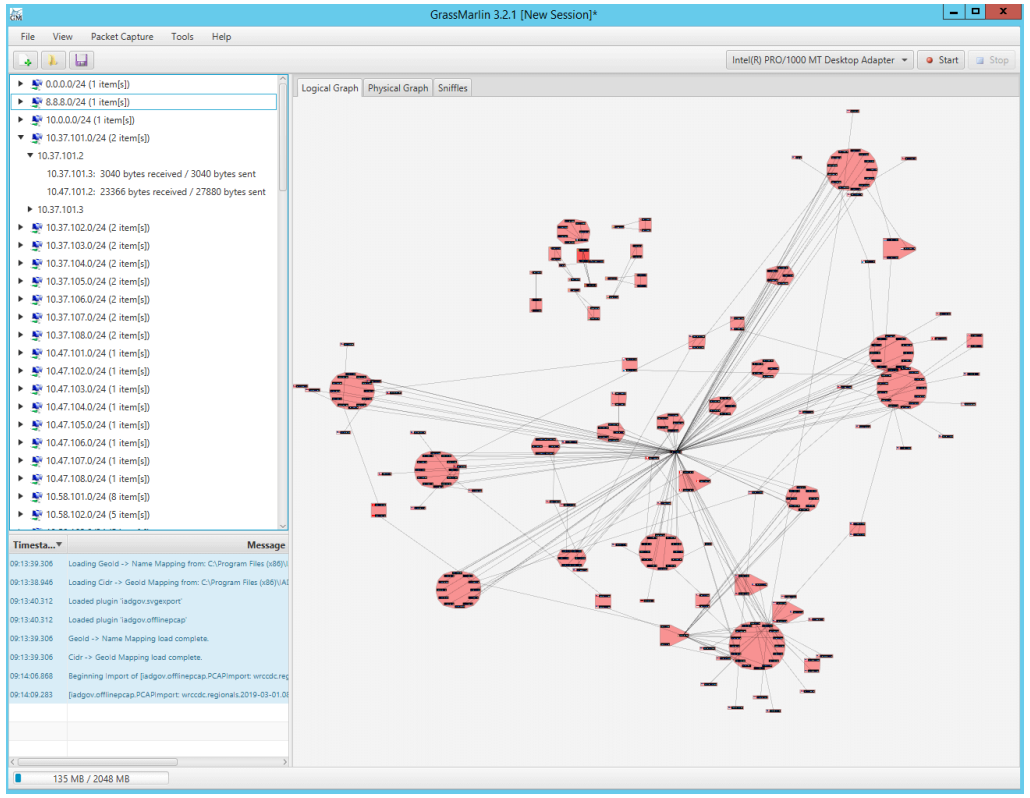
Database	racker.db	databases
Safari Top Sites	\Users\<user>\Library\Safari\TopSites.plist	A Plist listing the webpages belonging to a Safari's Top Sites
Safari Webpage Icons Database	\Users\<user>\Library\Safari\WebpageIcons.db	A database containing saved web page icons for webpages visited
Safari Webpage Databases	\Users\<user>\Library\Safari\Databases\	A directory for webpage-specific database storage
Safari Webpage Databases Database	\Users\<user>\Library\Safari\Databases\Databases.db	A database that keeps track of stored webpage-specific databases
Safari Cache Directory	\Users\<user>\Library\Caches\com.apple.Safari\	A directory containing Safari-specific cache items
Safari Cache	\Users\<user>\Library\Caches\com.apple.Safari\Cache.db	A cache of data from visited webpages
Safari Extensions Cache	\Users\<user>\Library\Caches\com.apple.Safari\Extensions\	A directory containing cached items for Safari Extensions
Safari Webpage Previews	\Users\<user>\Library\Caches\com.apple.Safari\fsCachedData\	A directory containing images of viewed webpages in .png and .jpg formats. The file name is a hash of the webpage URL.
Safari Cookies	\Users\<user>\Library\Cookies\HSTS.plist	A Plist containing cookies from visited webpages
Safari Preferences	\Users\<user>\Library\Preferences\com.apple.Safari.plist	Contains recent safari search strings and downloads folder location in addition to preferences
Safari Saved Application State Directory	\Users\<user>\Library\Saved Application State\com.apple.Safari.savedState\	Application save state for Safari. Directory contains other application save states
Safari Bookmark Cache	\Users\<user>\Library\Caches\Metadata\Safari\Bookmarks\	Each bookmark entry in Bookmarks.plist is stored as an individual file in this directory for more efficient use with Spotlight and to allow the user to select the bookmark entry from Spotlight and have Safari launch the corresponding webpage
Safari History Cache	\Users\<user>\Library\Caches\Metadata\Safari\History\	Each website entry in History.plist is stored as an individual file in this directory for more efficient use with Spotlight and to allow the user to select the webpage entry from Spotlight and have Safari launch the corresponding webpage
Mail		
Mail Cache	\Users\<user>\Library\Caches\com.apple.Mail\Cache.db	Cached images from email messages

Mac OS X Forensic Artifact Locations Page 11 of 36

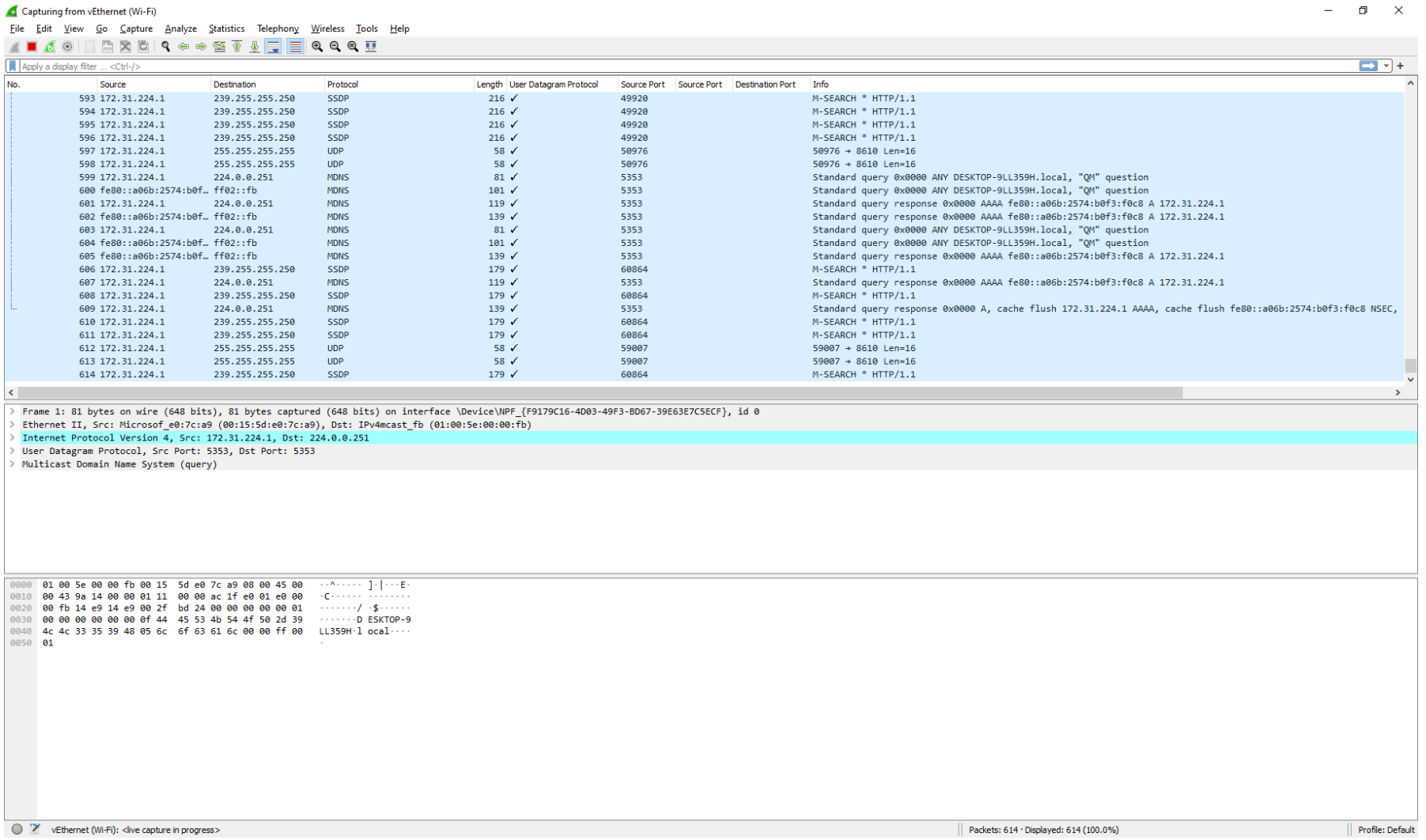
Spracovanie rozsiahlej sieťovej komunikácie (I.)

Názov: Predspracovanie rozsiahlej sieťovej komunikácie pre jej ďalšiu bezpečnostnú analýzu

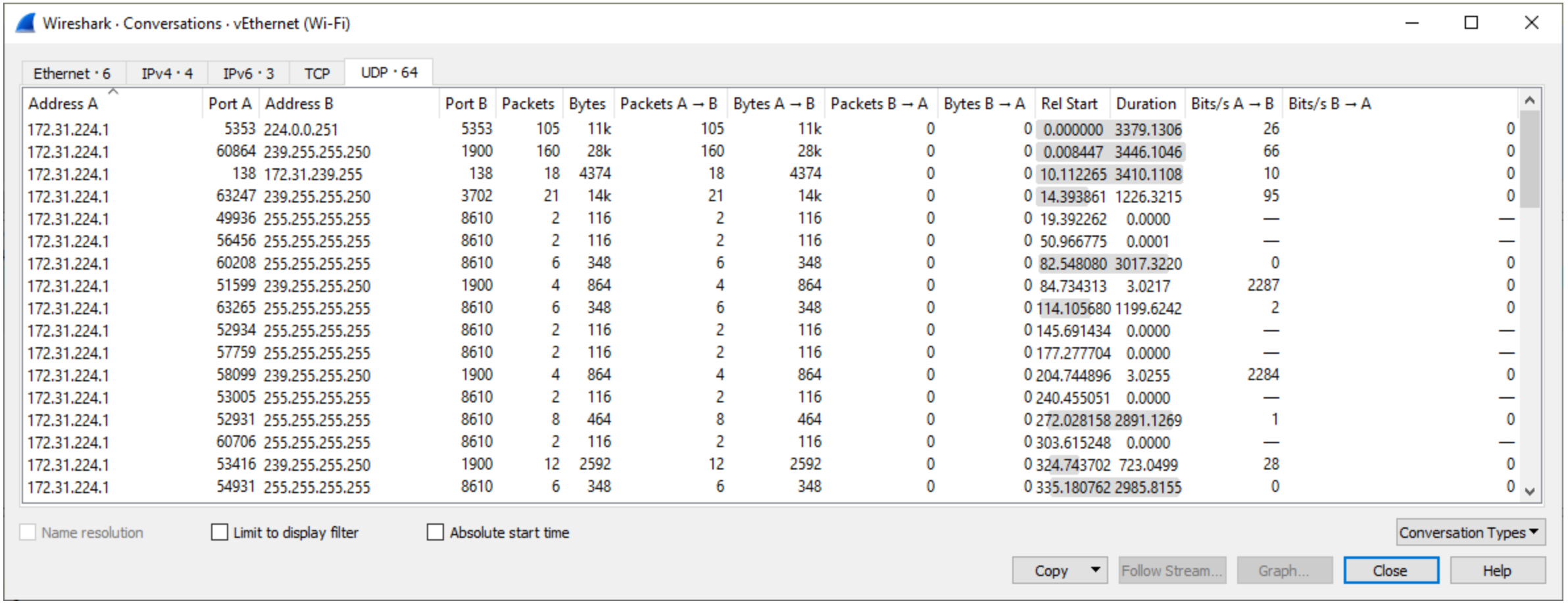
- Vedúci: Tomáš Bajtoš
- Konzultant: Richard Staňa
- (1) Porovnanie nástrojov a metód na spracovanie sieťovej komunikácie
- (2) Detekcia podozrivého správania v rozsiahlej sieťovej komunikácii
- (3) Návrh a implementácia metódy na extrakciu častí sieťovej komunikácie týkajúcich sa detegovaných hrozieb



Spracovanie rozsiahlej sieťovej komunikácie (II.)



Spracovanie rozsiahlej sieťovej komunikácie (III.)



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.31.224.1	5353	224.0.0.251	5353	105	11k	105	11k	0	0	0.000000	3379.1306	26	0
172.31.224.1	60864	239.255.255.250	1900	160	28k	160	28k	0	0	0.008447	3446.1046	66	0
172.31.224.1	138	172.31.239.255	138	18	4374	18	4374	0	0	10.112265	3410.1108	10	0
172.31.224.1	63247	239.255.255.250	3702	21	14k	21	14k	0	0	14.393861	1226.3215	95	0
172.31.224.1	49936	255.255.255.255	8610	2	116	2	116	0	0	19.392262	0.0000	—	—
172.31.224.1	56456	255.255.255.255	8610	2	116	2	116	0	0	50.966775	0.0001	—	—
172.31.224.1	60208	255.255.255.255	8610	6	348	6	348	0	0	82.548080	3017.3220	0	0
172.31.224.1	51599	239.255.255.250	1900	4	864	4	864	0	0	84.734313	3.0217	2287	0
172.31.224.1	63265	255.255.255.255	8610	6	348	6	348	0	0	114.105680	1199.6242	2	0
172.31.224.1	52934	255.255.255.255	8610	2	116	2	116	0	0	145.691434	0.0000	—	—
172.31.224.1	57759	255.255.255.255	8610	2	116	2	116	0	0	177.277704	0.0000	—	—
172.31.224.1	58099	239.255.255.250	1900	4	864	4	864	0	0	204.744896	3.0255	2284	0
172.31.224.1	53005	255.255.255.255	8610	2	116	2	116	0	0	240.455051	0.0000	—	—
172.31.224.1	52931	255.255.255.255	8610	8	464	8	464	0	0	272.028158	2891.1269	1	0
172.31.224.1	60706	255.255.255.255	8610	2	116	2	116	0	0	303.615248	0.0000	—	—
172.31.224.1	53416	239.255.255.250	1900	12	2592	12	2592	0	0	324.743702	723.0499	28	0
172.31.224.1	54931	255.255.255.255	8610	6	348	6	348	0	0	335.180762	2985.8155	0	0

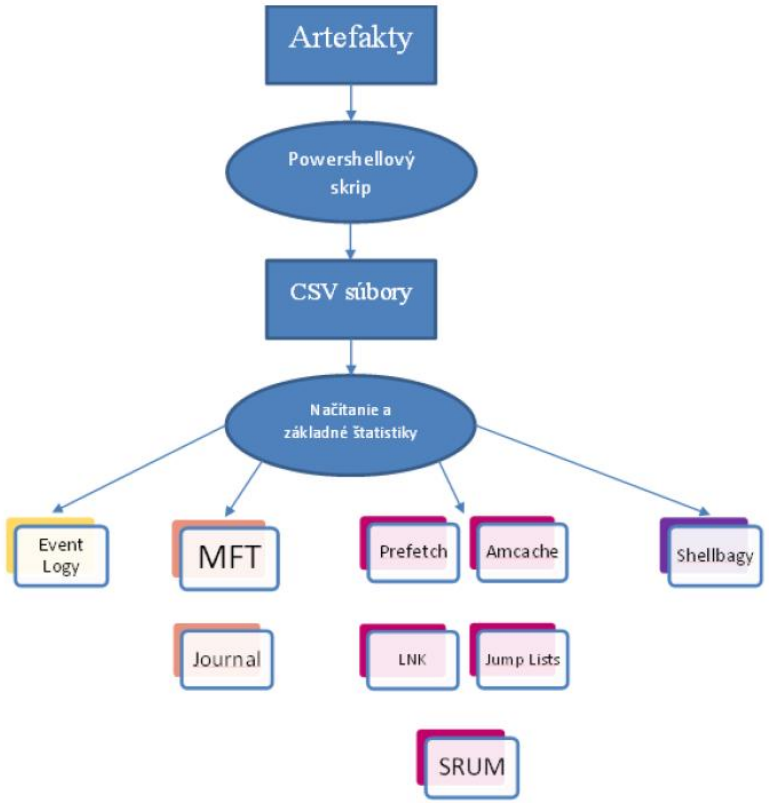
Doménový filter ako obranný mechanizmus proti podvodným správam (I.)

Názov: Doménový filter ako obranný mechanizmus proti podvodným správam

- Vedúci: Tomáš Bajtoš
- (1) Preskúmať a porovnať doménové filtre a ich účinnosť v identifikácii a blokovaní podvodných správ
- (2) Určiť hlavné vlastnosti a faktory, ktoré prispievajú k úspešnému fungovaniu doménových filtrov v kontexte podvodných správ
- (3) Vyvinúť prototyp doménového filtra, ktorý demonštruje základné princípy jeho fungovania a vyhodnotiť jeho účinnosť

Predchádzajúce záverečné práce (I.)

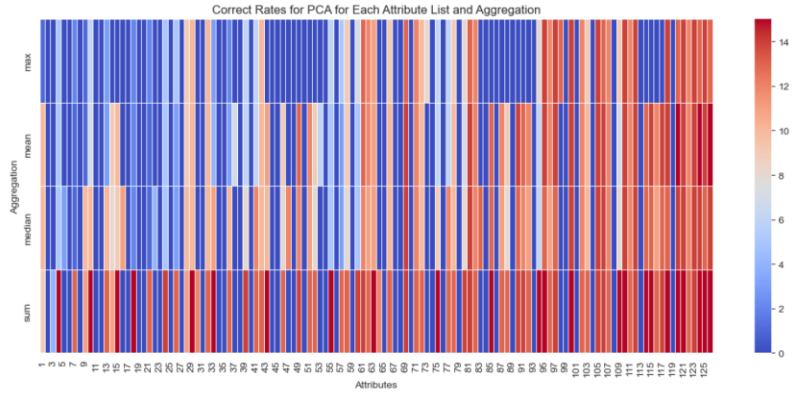
AUTOMATIZOVANÉ SPRACOVANIE FORENZNÝCH ARTEFAKTOV OPERAČNÉHO SYSTÉMU WINDOWS



VPLYV ANTI-FORENZNÝCH TECHNÍK NA DIGITÁLNE FORENZNÉ VYŠETROVANIE

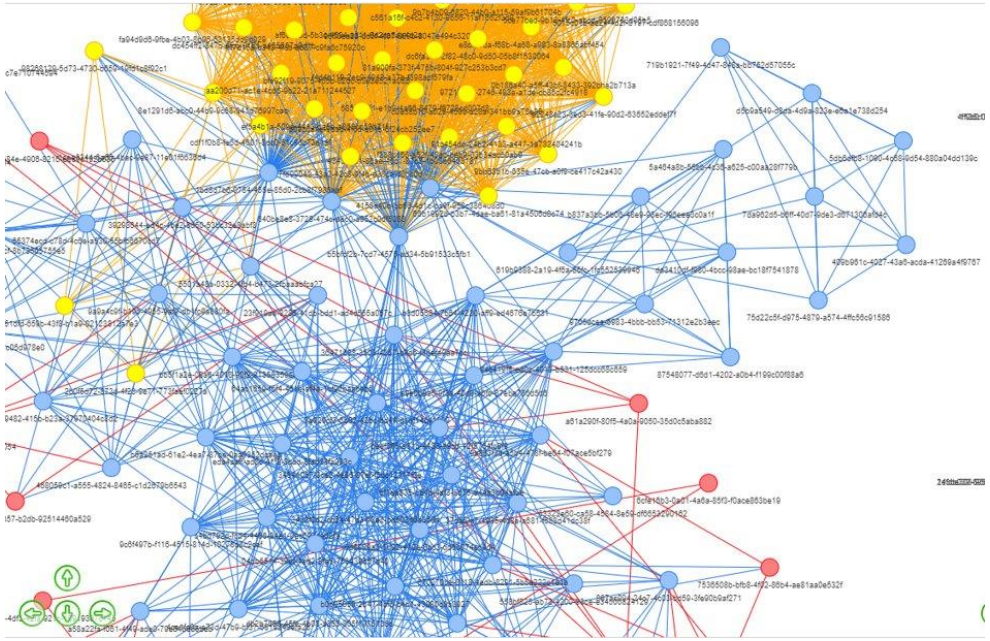
Vplyv anti-forenznej techniky na artefakt		stav artefaktu: je nahraditeľný	dá sa čiastočne zotaviť	nedá sa zotaviť ani nahradiť
detekcia	takmer nemožná			**vysoký vplyv**
	náročná		**stredný vplyv**	
	triviálna	**malý vplyv**		

IDENTIFIKÁCIA PODOZRIVÝCH FORENZNÝCH ARTEFAKTOV

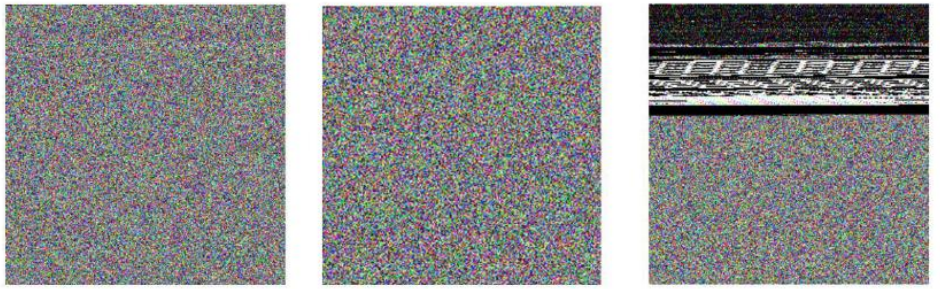


Predchádzajúce záverečné práce (II.)

ČASOVÉ OSI PRI FORENZNEJ ANALÝZE OPERAČNÉHO SYSTÉMU WINDOWS



KLASIFIKÁCIA MALVÉRU POMOCOU NEURÓNOVÝCH SIETÍ



RGB vizuálna reprezentácia troch vzoriek malvéru

Vizuálna reprezentácia štyroch vzoriek malvéru pomocou Simhash algoritmu

Ďakujeme za pozornosť!

https://csl.science.upjs.sk/

https://csirt.upjs.sk/

csirt@upjs.sk

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH • 1959 • 1795 1861

CSIRT UPJS

Cyber Security Lab

PRÍRODOVEDECKÁ FAKULTA UNIVERZITY P.J.ŠAFÁRIKA • 1959 •