These Artifacts aren't Fiction

TECHNOLOGY FIRST®

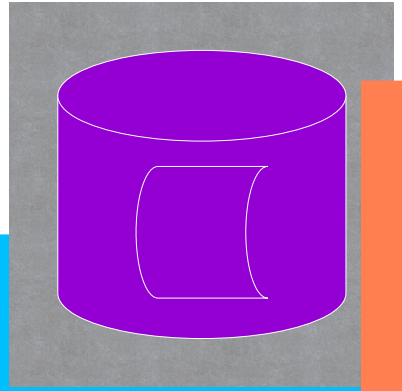
Ohio Information Security Conference

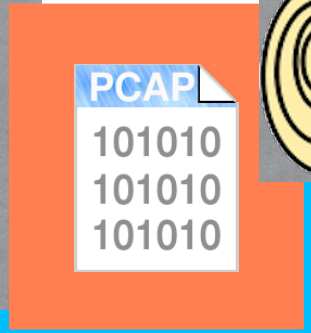
March 1, 2023 | Sinclair Conference Center

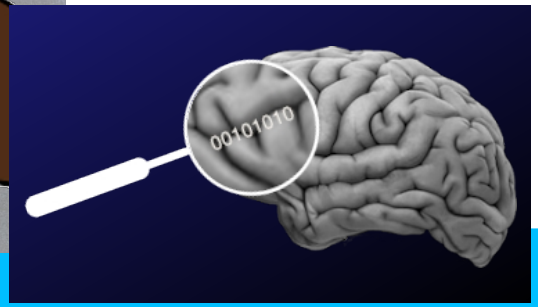
Matt Scheurer

Tuan Phan

Dayton, Ohio







#DFIR

PDF http://slides.dfirmatt.com

Introducing: Matt Scheurer

Matt works for a big well-known organization...

As an Assistant Vice President (AVP) of Computer Security and Incident Response (IR). However, he has many years of hands-on technical experience, including Digital Forensics & Incident Response (DFIR).

He is also a Podcast Host for

ThreatReel

https://threatreel.com

Follow / contact Matt:

https://www.linkedin.com/in/mattscheurer

https://twitter.com/c3rkah

Where Matt volunteers...

Matt is an Official

Advocate

https://www.hackingisnotacrime.org

He is also a

Women's Security Alliance (WomSA) Technical Mentor

https://www.womsa.org

Introducing: Tuan Phan

- Independent Security Researcher
- First-time speaker!
- Professional Experience
  - Digital Forensics, Investigation, Data Security, eDiscovery, and Insider Threat Strategy

Disclaimer!

Yes, the presenters both have day jobs. However…

Opinions expressed are based solely on their own independent security research and do not express or reflect the views or opinions of their employers.

We are not Lawyers!

This presentation is for educational purposes only! Please consult with qualified legal counsel before using these techniques in an actual investigation.

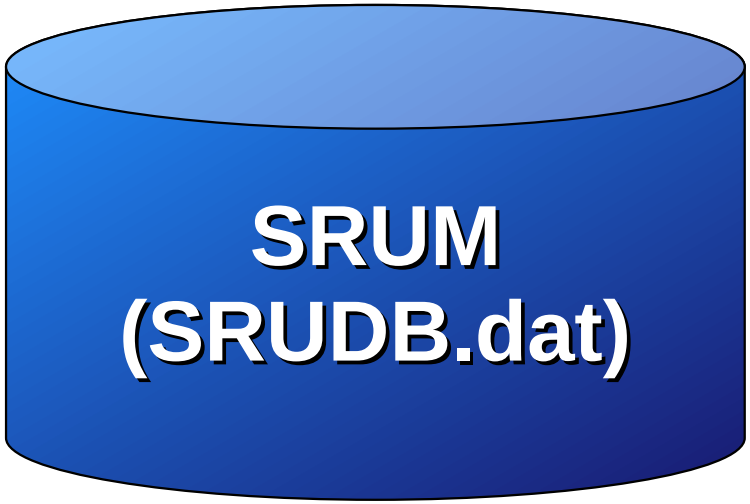
Out-of-Scope Topics

- 3rd party “Forensically Sound” tools for
  - Memory Capture (a.k.a. a “Memory Dumps”)
  - Disk Imaging
- How-To’s
  - Chain of Custody
  - Court Cases and Trials
    - Data handling and acceptable practices
  - Isolation, remote access, and when to disconnect or shutdown
- Data storage, data archival, data write blockers, etc.

Data Preservation Methodology

- Collect a “Forensic Image” first and foremost!
  - Work from a “Forensic Clone”
    - A working copy of your original “Forensic Image”
  - After completing & hashing a “Forensic Image”
    - Creating a “Forensic Clone”, while the “Forensic Image” is copying, provides a good opportunity to conduct live host eDiscovery acquisition
- Minimize activities that could modify system data and access times as much as possible

The Windows SRUM Database



The System Resource Utilization Monitor (**SRUM**) is built into Windows 8 and above. System "*App History*" data is recorded and stored in an Extensible Storage Engine (ESE) database named "**SRUDB.dat**".

The “SRUDB.dat” File

The Windows SRUM database file is located at:

C:\Windows\System32\sru\SRUDB.dat

Think of the SRUM database as holding the same level of details typically found in most commercial Endpoint/Network Detection & Response (**XDR)** solutions, but without any monitoring, alerting, “Detection”, or “Response” capabilities.

Useful SRUM Data

The Windows SRUM was never intended to be used for forensic purposes by Microsoft. Consequently, more details are stored than is typically helpful for our investigations. We'll focus our efforts on the following:

- Application Resources Usage
- Network Usage

“SRUDB.dat” Tools

Here are some Free and Open-Source Software options:

- SRUM Dump 2
  - https://github.com/MarkBaggett/srum-dump
- Velociraptor
  - https://www.rapid7.com/products/velociraptor
- NirSoft (AppResourcesUsageView & NetworkUsageView)
  - https://www.nirsoft.net/utils/app_resources_usage_view.html
  - https://www.nirsoft.net/utils/network_usage_view.html

SRUDB.dat Example Output

AppResourcesUsageView

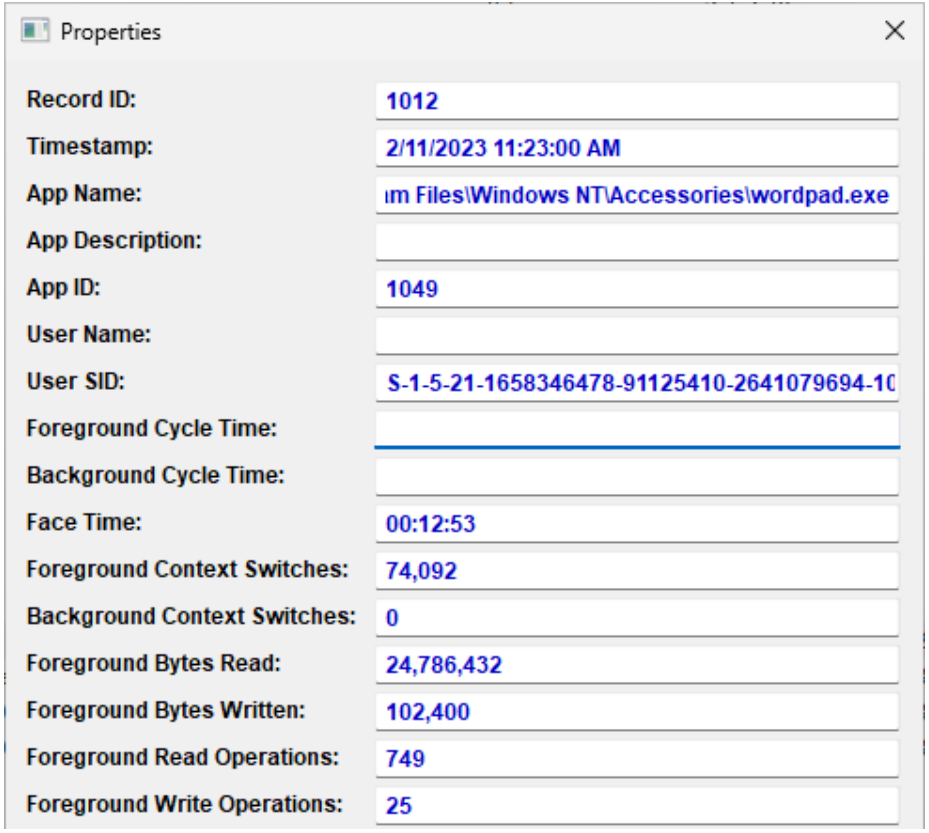
File Edit View Options Help

Record ID	Timestamp	App Name	App Description	App ID	User SID	Foregrou
1001	2/11/2023 11:23:00 AM	\Device\HarddiskVolume4\Windows\System32\WindowsPowerShell\v1.0\powershell.exe		410	S-1-5-21-1658346478-91125410-2641079694-1000	
877	2/8/2023 9:49:00 AM	\Device\HarddiskVolume4\Windows\System32\cmd.exe		722	S-1-5-21-1658346478-91125410-2641079694-1000	
1132	2/11/2023 1:22:00 PM	\Device\HarddiskVolume4\Windows\System32\ApplicationFrameHost.exe		1047	S-1-5-21-1658346478-91125410-2641079694-1000	
1009	2/11/2023 11:23:00 AM	\Device\HarddiskVolume4\Windows\System32\ApplicationFrameHost.exe		1047	S-1-5-21-1658346478-91125410-2641079694-1000	
1256	2/11/2023 2:22:00 PM	\Device\HarddiskVolume4\Windows\System32\ApplicationFrameHost.exe		1047	S-1-5-21-1658346478-91125410-2641079694-1000	
1445	2/11/2023 4:23:00 PM	\Device\HarddiskVolume4\Windows\System32\ApplicationFrameHost.exe		1047	S-1-5-21-1658346478-91125410-2641079694-1000	
1379	2/11/2023 3:24:00 PM	\Device\HarddiskVolume4\Windows\System32\ApplicationFrameHost.exe		1047	S-1-5-21-1658346478-91125410-2641079694-1000	
1566	2/11/2023 4:26:00 PM	\Device\HarddiskVolume4\Windows\System32\ApplicationFrameHost.exe		1047	S-1-5-21-1658346478-91125410-2641079694-1000	
1129	2/11/2023 1:22:00 PM	\Device\HarddiskVolume4\Windows\System32\WindowsPowerShell\v1.0\powershell.exe		410	S-1-5-21-1658346478-91125410-2641079694-1000	
1123	2/11/2023 1:22:00 PM	\Device\HarddiskVolume4\Windows\explorer.exe		404	S-1-5-21-1658346478-91125410-2641079694-1000	
880	2/8/2023 9:49:00 AM	\Device\HarddiskVolume4\Windows\System32\WindowsPowerShell\v1.0\powershell.exe		410	S-1-5-21-1658346478-91125410-2641079694-1000	
1442	2/11/2023 4:23:00 PM	\Device\HarddiskVolume4\Windows\System32\WindowsPowerShell\v1.0\powershell.exe		410	S-1-5-21-1658346478-91125410-2641079694-1000	
1114	2/11/2023 1:22:00 PM	Microsoft.AAD.BrokerPlugin_1000.19580.1000.0_neutral_neutral_cw5n1h2txyewy		407	S-1-5-21-1658346478-91125410-2641079694-1000	
998	2/11/2023 11:23:00 AM	Microsoft.AAD.BrokerPlugin_1000.19580.1000.0_neutral_neutral_cw5n1h2txyewy		407	S-1-5-21-1658346478-91125410-2641079694-1000	
1377	2/11/2023 3:24:00 PM	\Device\HarddiskVolume4\Windows\System32\WindowsPowerShell\v1.0\powershell.exe		410	S-1-5-21-1658346478-91125410-2641079694-1000	
1366	2/11/2023 3:24:00 PM	Microsoft.AAD.BrokerPlugin_1000.19580.1000.0_neutral_neutral_cw5n1h2txyewy		407	S-1-5-21-1658346478-91125410-2641079694-1000	
1253	2/11/2023 2:22:00 PM	\Device\HarddiskVolume4\Windows\System32\WindowsPowerShell\v1.0\powershell.exe		410	S-1-5-21-1658346478-91125410-2641079694-1000	
1005	2/11/2023 11:23:00 AM	\Device\HarddiskVolume4\Users\User\AppData\Local\Microsoft\OneDrive\23.023.0129.0002\Microsoft.SharePoint.exe		1044	S-1-5-21-1658346478-91125410-2641079694-1000	
1428	2/11/2023 4:23:00 PM	Microsoft.AAD.BrokerPlugin_1000.19580.1000.0_neutral_neutral_cw5n1h2txyewy		407	S-1-5-21-1658346478-91125410-2641079694-1000	
862	2/8/2023 9:49:00 AM	Microsoft.AAD.BrokerPlugin_1000.19580.1000.0_neutral_neutral_cw5n1h2txyewy		407	S-1-5-21-1658346478-91125410-2641079694-1000	
1444	2/11/2023 4:23:00 PM	\Device\HarddiskVolume4\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe		963	S-1-5-21-1658346478-91125410-2641079694-1000	
876	2/8/2023 9:49:00 AM	\Device\HarddiskVolume4\Users\User\AppData\Local\Microsoft\OneDrive\OneDrive.exe		963	S-1-5-21-1658346478-91125410-2641079694-1000	

Application Resources Usage

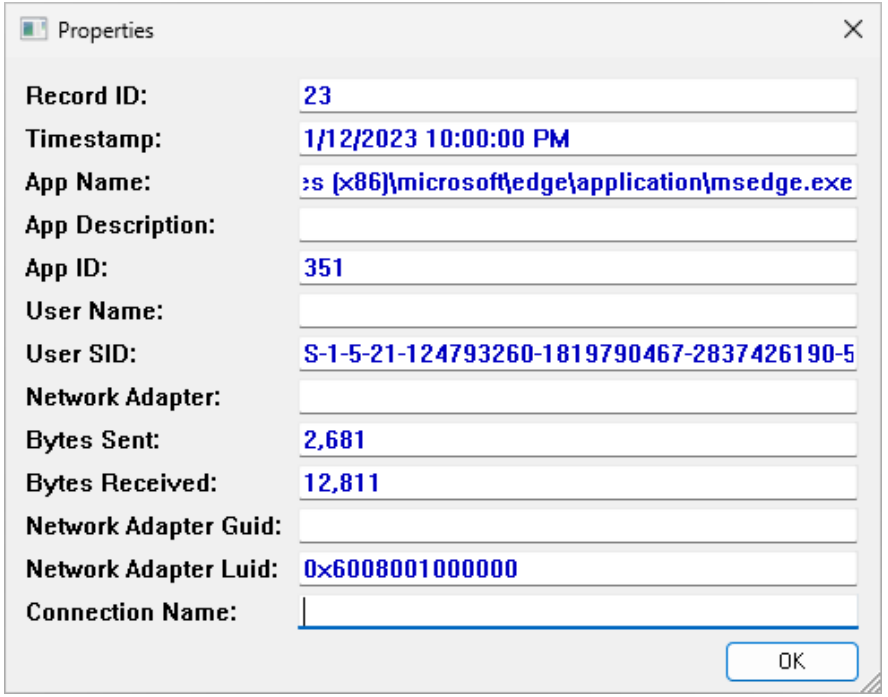
May include the following application execution details:

Timestamp, Application Name, User SID, cycle times, bytes read and written, number of read and write operations, and more.



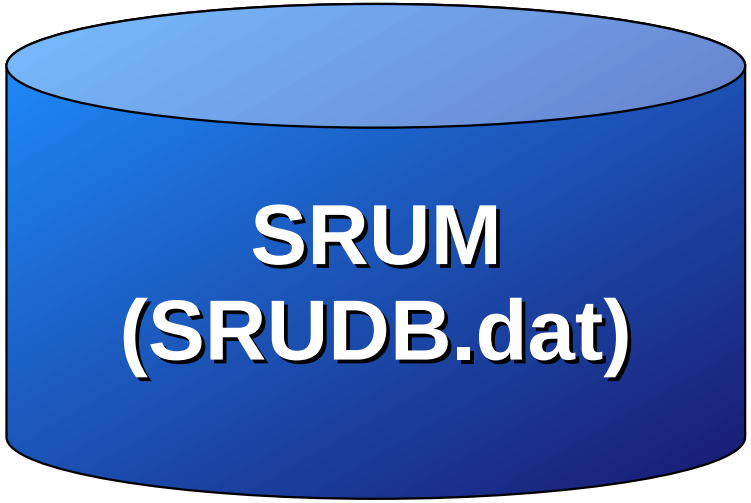
Network Resource Usage

May include: the timestamp, name and description of the service or application, the name and SID of the user, the network adapter, and the total number of bytes sent and received by the specified service or application.



SRUM Database Conclusions

The Windows SRUM database helps us with identifying file execution, user attribution, activity correlation, and time lining of system events.



Web Browser Artifacts

Analyzing artifacts related to web browser usage from a suspect's system is essential for digital forensic examiners and computer forensic investigators.

Data Extraction & Analysis Tools

- Free and Open-Source Software
  - **Browser History Examiner (BHE)**
  - **BrowsingHistoryView**
  - **DB Browser for SQLite**
  - **Hindsight**
- Various 3rd party commercial forensic tools

Artifact Sources

- Hard Drives
- Forensic Clones
  - Hard Drive Images
- Memory Dumps
- Databases and Other Files

High-Value Artifacts

- History
- Typed URLs
- Cache
- Cookies
- Session Restore
- Searches

- Form values
  - Auto-fill
  - Contents
  - Searches, etc.
- Downloads
- Favorites
  - a.k.a. Bookmarks

Private Browsing

Private (a.k.a. incognito) browsing modes allow users to surf the web without retaining browser history and associated cache and cookie files.

Memory Dumps

One step in collecting high-value web browser artifacts is through live-capturing an image of the system’s physical memory.

Memory dumps also include private browsing-mode session artifacts otherwise unavailable on those systems.

History

A web browser’s “History” records websites visited by date and time. Details are stored for each local user’s account, records number of times visited (frequency), and tracks access of local system files.

Example History Database Paths

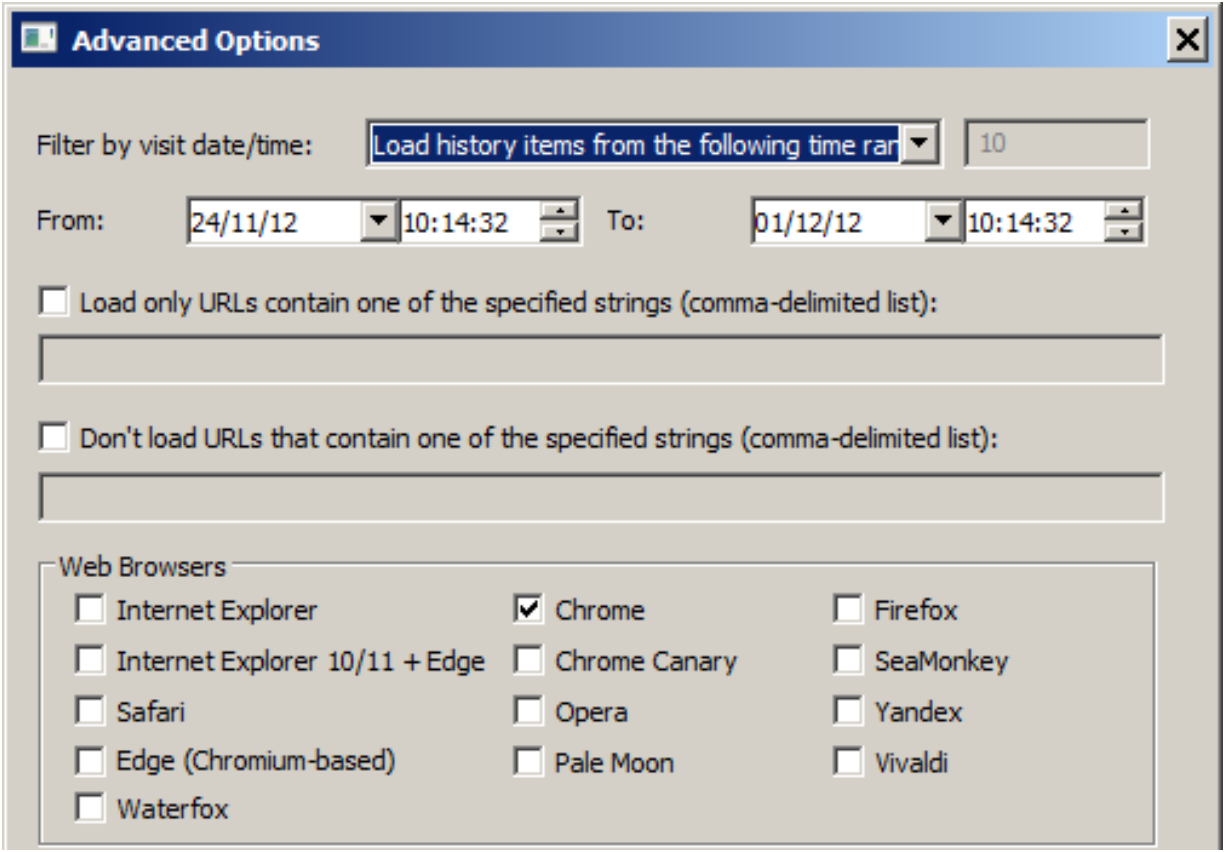
Microsoft Edge on Windows:
\Users\%username%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

Mozilla Firefox on Windows:
\Users\%username%\AppData\Roaming\Mozilla\Firefox\Profiles*[Hex]*.default\places.sqlite

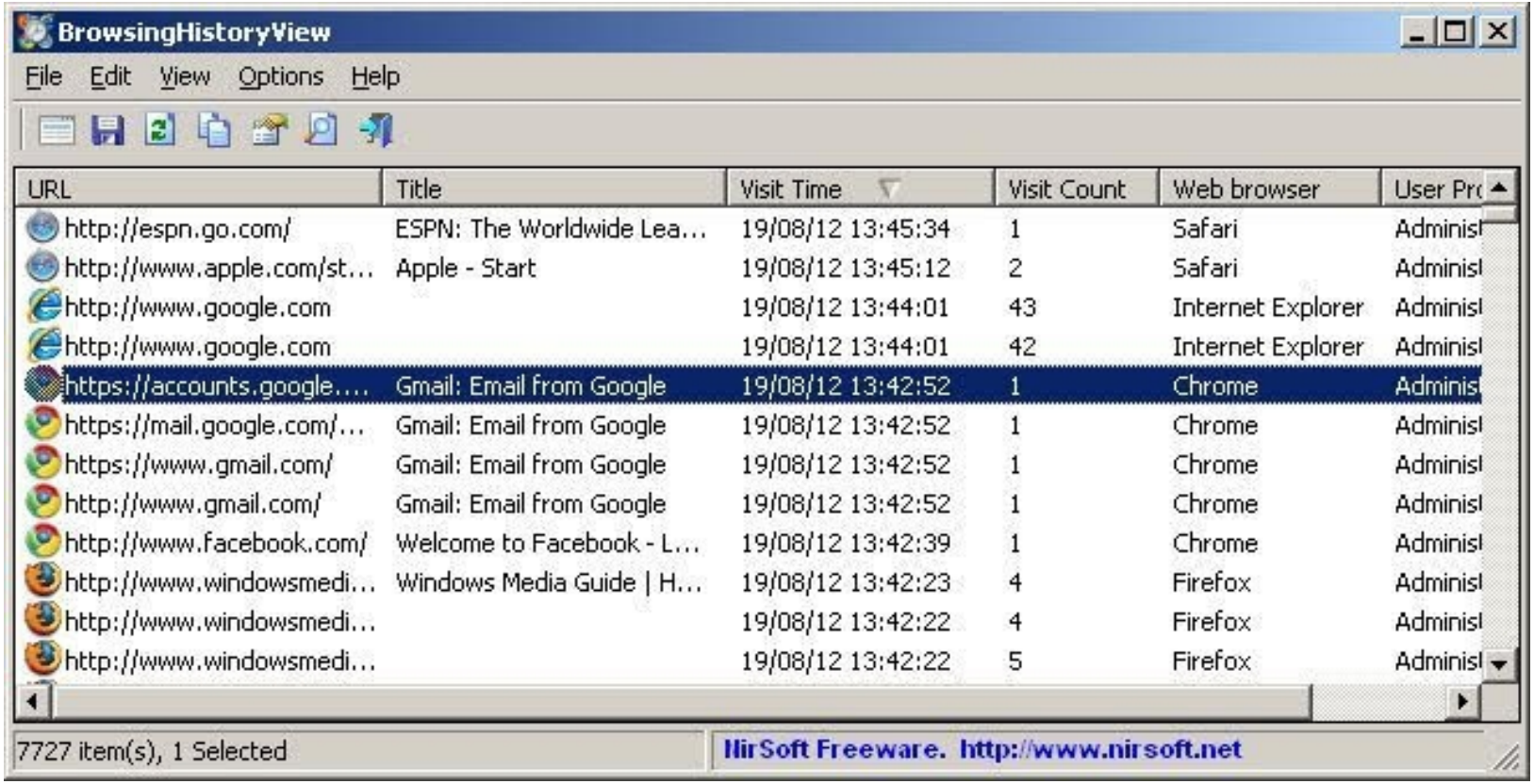
Google Chrome on Windows:
\Users\%username%\AppData\Local\Google\Chrome\User Data\Default\History

Safari on MacOS:
\Users\%username%\Library\Safari\History.db

History Extraction Example 1/5



History Extraction Example 2/5



History Extraction Example 3/5

Browsing History Items

A	B	C	D	E	F	G	H	I	J
Browsing History Items									
Created by using BrowsingHistoryView									
URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Web Browser	User Profile	Browser Profile	URL Length
http://windows.microsoft.com/en-U		3/22/2015 8:09:2	0		Link	Chrome	informant	Default	74
https://dl.google.com/update2/1.3.		3/22/2015 8:11:0	0		Link	Chrome	informant	Default	284
http://go.microsoft.com/fwlink/?Linl		3/22/2015 8:09:0	0		Link	Chrome	informant	Default	44
http://go.microsoft.com/fwlink/?Linl		3/22/2015 8:09:2	0		Link	Chrome	informant	Default	45
https://www.google.com/webhp?sc		3/22/2015 8:55:4	1	https://www.gooc	Link	Chrome	admin11	Default	84
http://iweb.dl.sourceforge.net/proje		3/25/2015 7:47:3	1			Internet Explorer	informant		84
https://www.gooc	security checkpo	3/24/2015 2:06:5	1		Link	Chrome	informant	Default	50
http://www.bing.c	Bing	3/24/2015 2:05:4	1		Reload	Chrome	informant	Default	20
https://news.gooc	Google News	3/24/2015 12:01:	1		Reload	Chrome	informant	Default	46
http://www.bing.c	Bing	3/24/2015 12:01:	1		Reload	Chrome	informant	Default	20

History Extraction Example 4/5

SQLite Database Browser - C:/Users/Administrator/AppData/Roaming/Mozilla/Firefox/Profiles/q3wdrb9w.d...

File Edit View Help

Database Structure | Browse Data | Execute SQL

Table: moz_bookmarks

New Record | Delete Record

	id	type	fk	parent	position	title	keyword_id	folder_type	dateAdded	lastModifie
1	1	2		0	0				1268183651449000	126818365
2	2	2		1	0	Bookmarks Menu			1268183651450000	12685043
3	3	2		1	1	Bookmarks Toolbar			1268183651450000	126818365
4	4	2		1	2	Tags			1268183651450000	126818365
5	5	2		1	3	Unsorted Bookmarks			1268183651451000	126818365
6	6	1	1	3	0	Most Visited			1268183651580000	126818365
7	7	1	2	2	0	Recently Bookmarke			1268183651581000	126818365
8	8	1	3	2	1	Recent Tags			1268183651582000	126818365
9	9	3		2	2				1268183651582000	126818365
10	10	1	4	2	3	Get Bookmark Add-c			1268183651590000	126818365

History Extraction Example 5/5

DB Browser for SQLite - C:/Users/[redacted]/AppData/Local/Google/Chrome/User Data/Default/History

File Edit View Help

New Database | Open Database | Write Changes | Revert Changes

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: urls

New Record | Delete Record

	id	url	title	visit_count	typed_count	last_visit_time	hidde
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	178	https://support.google.com/chrome/answer/157179?hl=en	Keyboard sho...	1	0	13100885771...	0
2	177	https://support.google.com/chrome/?p=help&ctx=keyboard#topic=3227...		1	0	13100885763...	0
3	176	https://support.google.com/chrome/?p=help&ctx=keyboard	Chrome Help	1	0	13100885762...	0
4	175	https://accounts.google.com/ServiceLogin?service=mail&continue=https...		1	0	13100177054...	0
5	174	https://accounts.google.com/ServiceLogin?service=mail&continue=https...	Gmail	1	0	13100177054...	0
6	173	https://www.google.com/intl/en/mail/help/about.html	Gmail - Free ...	1	0	13100177050...	0
7	172	https://mail.google.com/intl/en/mail/help/about.html	Gmail - Free ...	1	0	13100177050...	0
8	171	https://accounts.google.com/ServiceLogin?service=mail&passive=true&...	Gmail - Free ...	1	0	13100177050...	0
9	170	https://mail.google.com/mail/	Gmail - Free ...	1	0	13100177050...	0
10	169	http://192.168.1.1/unauth.cgi		1	0	13099135295...	0
11	168	http://192.168.1.1/apply.cgi?/reboot_waiting.htm%20timestamp=40342...		1	0	13099135163...	1
12	167	http://192.168.1.1/reboot.htm		1	0	13099135161...	1
13	166	http://192.168.1.1/RST_status.htm		1	0	13099135161	1

|< < 1 - 13 of 61 > >| Go to: 1

DB Sche&ma

Name	Type
Tables (9)	
downloads	
downloads_url_chains	
keyword_search_terms	
meta	
segment_usage	
segments	
urls	
visit_source	
visits	
Indices (13)	
keyword_search_terms_index1	
keyword_search_terms_index2	
keyword_search_terms_index3	
segment_usage_time_slot_segment_id	
segments_name	
segments_url_id	
segments_usage_seg_id	
sqlite_autoindex_downloads_url_chains_1	
sqlite_autoindex_meta_1	
urls_url_index	
visits_from_index	
visits_time_index	
visits_url_index	
Views (0)	
Triggers (0)	

SQL Log | Plot | DB Schema

UTF-8

Typed URLs

This artifact has the full URLs typed or inserted in the browser address bar. Example paths include:

- **Mozilla Firefox on Windows**
  - \Users\%username%\AppData\Roaming\Mozilla\Firefox\Profiles*[Hex]*.default\places.sqlite (Firefox, Windows)
- **Google Chrome on Windows**
  - \Users\%username%\AppData\Local\Google\Chrome\User Data\Default\History

Searches

This artifact shows what the user has searched.

Here is an example artifact path:

- **Google Chrome on Windows**
  - \Users\%username%\AppData\Local\Google\Chrome\User Data\Default\History

Downloads

Downloaded files are typically (though user-configurable) stored in each user’s “Downloads” folder by default. Investigators would inspect the contents from an investigation subject’s downloaded files.

Future Trends

Many forensic tools target a vendor specific web browser. Vendor-agnostic browser tools today lack accurate artifact extraction. Ideally, forensic tools should support cross-vendor platform and browser analysis, and automate correlation of data based on timestamps for integrated artifact analysis.

I anticipate a growing need in performing forensic analysis within web browsers on mobile devices.

Conclusions

While web browsers play a pivotal role in Internet access, they continue being targeted by threat actors.

Tracing evidence from Web browser utilization is an important process in digital forensic investigations. Analyzing a trace from a Web browser’s use helps us understand the objective, methods, and criminal activities of a suspect. When an investigator is examining a suspect’s system, the Web browser’s log details remain a key artifact of our investigations.

PowerShell Artifacts Collection

PowerShell cmdlets and commands useful for digital forensics, artifact collection, and eDiscovery.

The Inspiration

Use of “Living Off The Land Binaries and Scripts” (**LOLBAS**) is a notable trend among Offensive Security practitioners and threat actors alike...

Objectives

- Leverage PowerShell to collect digital forensic artifacts from the endpoint being investigated
- Presentation order based on **RFC 3227**
  - Guidelines for Evidence Collection and Archiving
    - https://www.rfc-editor.org/rfc/rfc3227.html
    - Section: 2.1 Order of Volatility

Reminder: Data Preservation

- Avoid commands that will alter the system, system data, and access times
  - Some Examples (**NOTE:** Not an all-inclusive list)
    - “Clear-”, “Debug-”, “Disable-”, “Enable-”, “Expand-”, “Import”, “Install-”, “New-”, “Register-”, “Remove-”, “Save-”, “Set-”, “Unregister-”, “Update-”, “Write-”, etc.
- Avoid importing or installing external or 3rd party modules

Warning!

Be prepared to defend running PowerShell as "**Administrator**" if you decide to do so.

- We'll touch on <u>potentially</u> justifiable use-cases momentarily...

PowerShell Logging

The following syntax timestamps the start and end of our data collection process. All input activity and output results are logged to a file.

```
Start-Transcript -Path "[PATH\FILENAME.EXT]" -NoClobber

Stop-Transcript (NOTE: When the investigation is complete)
```

PowerShell Version

There are a number of automatic variables in PowerShell that store state information. Run the following to display the relevant PowerShell version information:

```
$PSVersionTable

(NOTE: Includes “PSEdition” in PowerShell 5.1 and above)
```

PowerShell Pro Tip!

PowerShell truncates lengthy text output results by default...

Think of these "**Format-List**" variations as verbose output options:

Verbose:	`| Format-List`
Very Verbose:	`| Format-List *`
Very Very Verbose:	`| Format-List -Property *`

System Time

Frequently time-stamping command activity during an investigation before and after each step is recommended. Here are some examples...

```
Get-Date
Get-TimeZone
Get-Uptime -Since (NOTE: Requires PowerShell v6.0+)
Get-ComputerInfo -Property “OsLastBootUpTime”
Get-ComputerInfo -Property “OsUptime”
```

UTC / GMT Time

Investigations are often easier when correlating timestamps using a neutral timezone of reference. The following variable outputs the time in UTC:

```
$Time = Get-Date
$Time.ToUniversalTime()
```

Hashing Files

```
Get-FileHash [FILENAME.EXT] -Algorithm [VALUE]
```

- Value options
  - **SHA1**
  - **SHA256**
  - **SHA384**
  - **SHA512**
  - **MD5**

Volatile Network Artifacts

The following PowerShell cmdlets are useful for collecting the routing table, ARP, network traffic details, and DNS cache respectively:

```
Get-NetRoute
Get-NetNeighbor
Get-NetTCPConnection
Get-NetUDPEndpoint
Get-DnsClientCache
```

Processes and Services

The following cmdlets are useful for obtaining a list of running processes and services on the endpoint being investigated:

```
Get-Process

Get-Service
```

Less Volatile Network Artifacts

The following PowerShell cmdlets are useful for collecting the system network configuration settings and network adapter properties:

```
Get-DnsClient
Get-DnsClientServerAddress
Get-NetIPAddress
Get-NetIPConfiguration
Get-NetAdapter
```

Users and Groups

Unfortunately, PowerShell does **not** offer a “Get-LoggedOnUsers” cmdlet or similar. The following will obtain host user and group details:

```
Get-WmiObject Win32_LoggedOnUser | Select Antecedent -Unique
Query User (NOTE: Not an actual cmdlet, but better!)

Get-LocalGroup | Select *
Get-LocalUser | Select *

Get-ChildItem C:\Users
```

Execution Policy Settings

Use the following commands to obtain the current PowerShell execution policy and the execution policy for each scope in order of precedence:

```
Get-ExecutionPolicy

Get-ExecutionPolicy -List
```

Clipboard and Auto-runs

Use the following commands to retrieve text stored in the Windows clipboard and a list of Windows startup items:

```
Get-Clipboard (NOTE: Currently logged in user account)

Get-CimInstance Win32_StartupCommand
```

Host Details

Use the following to collect additional details such as installed drivers, programs, hotfixes, disk drives, system details, and other OS information:

```
Get-Windows-Driver -Online -All (NOTE: Requires running as ‘Administrator’)
Get-Package
Get-HotFix
Get-PSDrive
Get-ComputerInfo
```

The Open Files Conundrum

There are significant challenges in obtaining open file details using native PowerShell...

```
Get-SmbOpenFile

NOTES: Requires running as ‘Administrator'. Only works for files
that are remotely accessed

OpenFiles /Query
The system global flag 'maintain objects list' needs to be
enabled to see local opened files.

OpenFiles /Local On (NOTE: Requires running as 'Administrator')
This will take effect after the system is restarted.
```

More PowerShell Tips & Tricks

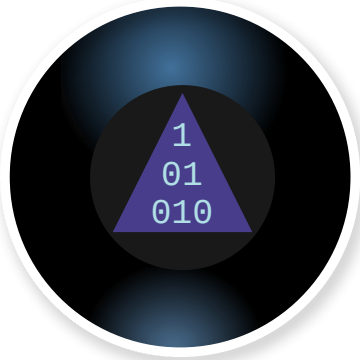
These commands and cmdlets barely scratch the surface of PowerShell capabilities in alignment with our objectives of collecting and preservation of data with minimal impacts and changes to the host operating system that we are investigating.

Further reading:

https://learn.microsoft.com/en-us/powershell/

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/

Questions



Thank you for attending!

TECHNOLOGY FIRST®

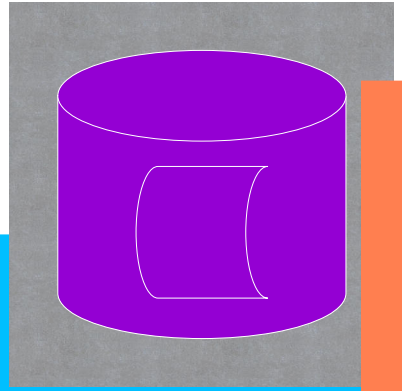
Ohio Information Security Conference

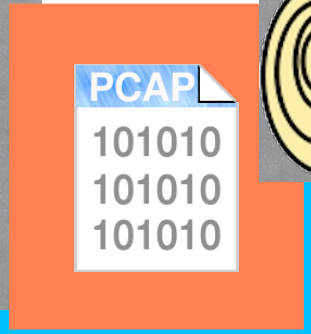
March 1, 2023 | Sinclair Conference Center

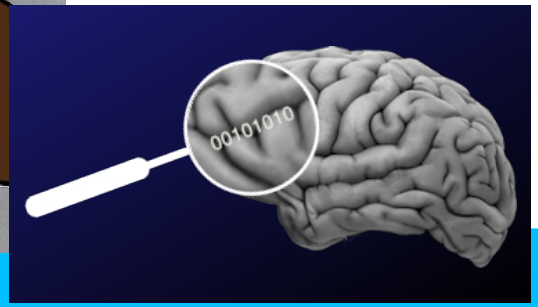
Matt Scheurer

Tuan Phan

Dayton, Ohio







#DFIR

PDF http://slides.dfirmatt.com