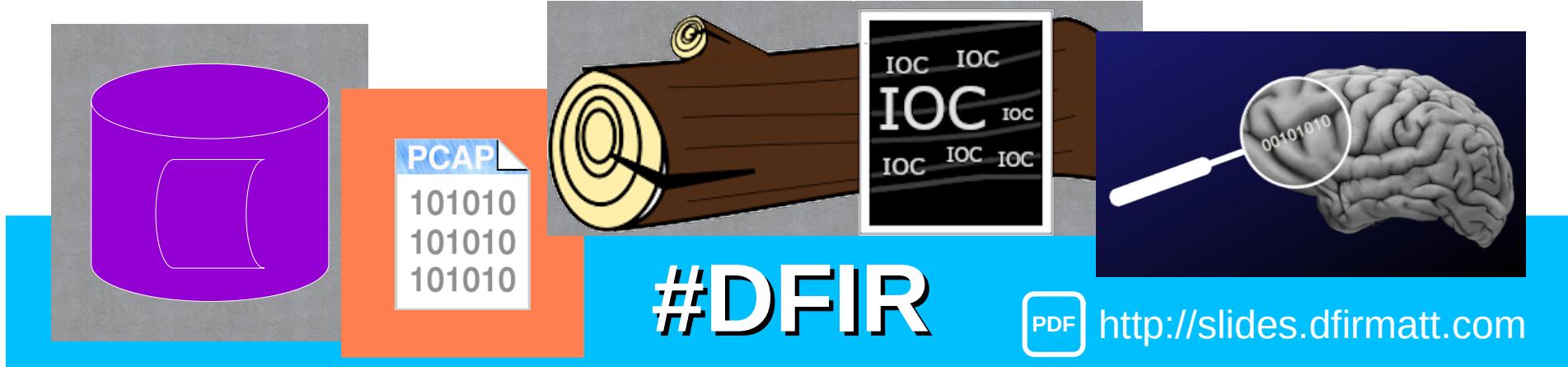


# These Artifacts aren't Fiction



CiNPA  
Security SIG

Matt Scheurer  
Tuan Phan



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 Info Security Researcher
- Professional Experience
  - eDiscovery, Forensics Investigation, 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.

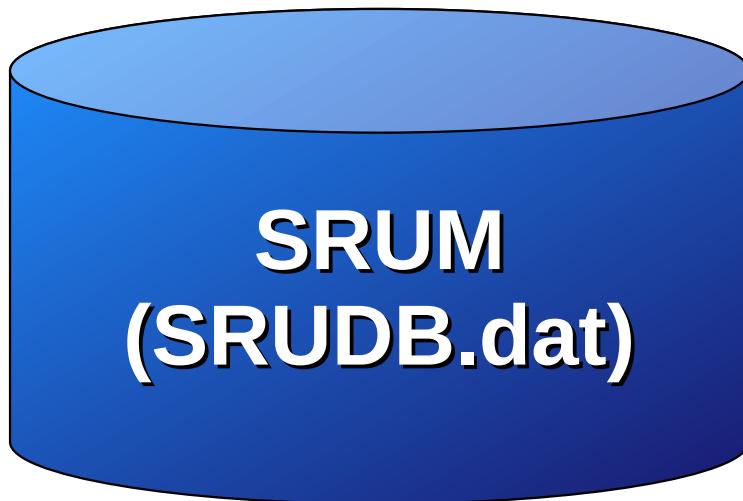
# Out-of-Scope Topics

- 3<sup>rd</sup> party “Forensically Sound” tools for
  - Memory Capture (a.k.a. a “Memory Dumps”)
  - Disk Imaging Tools
- 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 from 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/app_resources_usage_view.html)
  - [https://www.nirsoft.net/utils/network\\_usage\\_view.html](https://www.nirsoft.net/utils/network_usage_view.html)

# SRUDB.dat Example Output

Record ID	Timestamp	App Name	App Description	App ID	User SID	Foreground
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	
1998	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

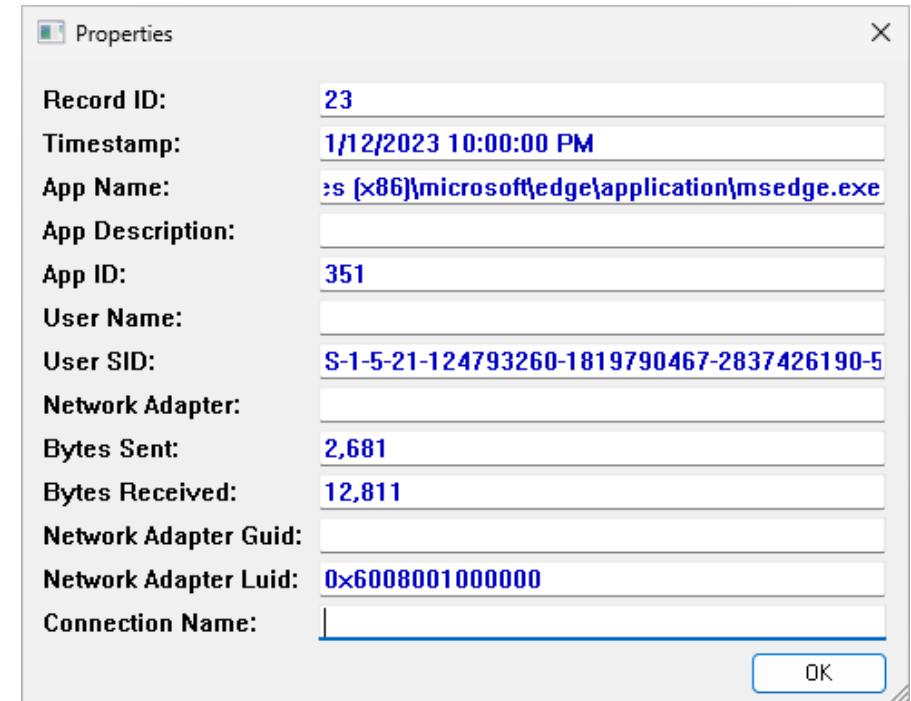
May include the following application execution details:

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

Properties	
Record ID:	1012
Timestamp:	2/11/2023 11:23:00 AM
App Name:	im Files\Windows NT\Accessories\wordpad.exe
App Description:	
App ID:	1049
User Name:	
User SID:	S-1-5-21-1658346478-91125410-2641079694-10
Foreground Cycle Time:	
Background Cycle Time:	
Face Time:	00:12:53
Foreground Context Switches:	74,092
Background Context Switches:	0
Foreground Bytes Read:	24,786,432
Foreground Bytes Written:	102,400
Foreground Read Operations:	749
Foreground Write Operations:	25

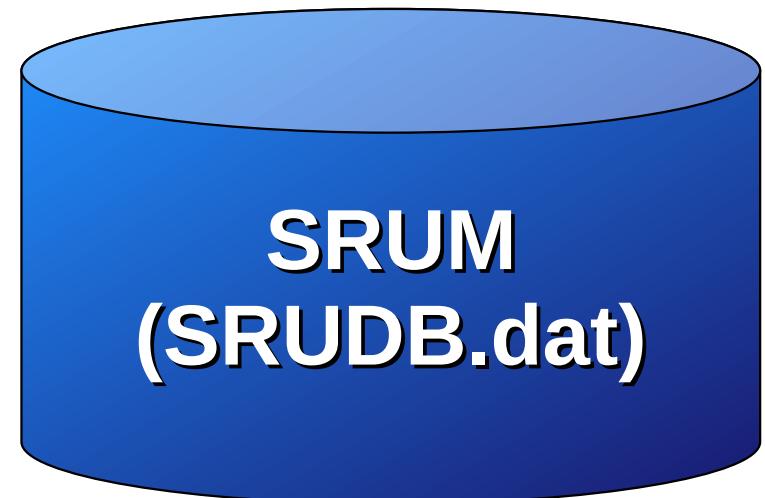
# Network Resource Usage

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 timelineing of system events.



# Web Browser Artifacts

- What they are
  - Where they are
    - Why these are important
    - How they are parsed



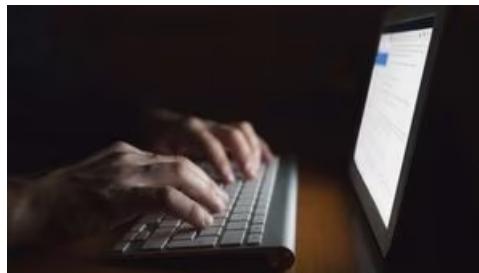
# What & Where

- These artifacts are the data left behind by a web browser, when visiting a website
- Computers store a variety of detailed information from visited websites
  - Different browsers store their artifacts/files in different locations

# Why these are important

Essential for digital forensic examiners and  
Incident Response

- These artifacts help to identify
  - The source of malicious attack traffic
  - Proxy policy violation



# Investigation Tooling

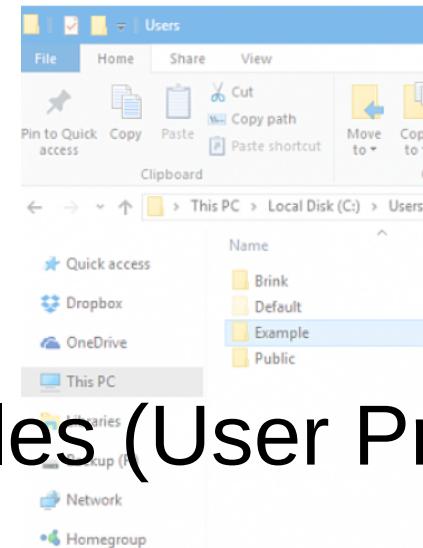
## Data Extraction & Analysis Tools

- Free and Open-Source Software
  - Browser History Examiner (BHE) - Foxtron
  - BrowsingHistoryView - Nirsoft
  - BrowserDownloadView- Nirsoft
  - DB Browser for SQLite
  - Hindsight
- Various 3<sup>rd</sup> party commercial forensic tools



# Artifact Sources

- Suspect Hard Drives
- Forensic Clones
  - Hard Drive Images
- Memory Dumps
- Databases and Other Files (User Profile)



# High-Value Artifacts

Most Notably...

- History/URLs
  - Typed URLs
  - Searches
- Cache
- Logins
- Cookies

- Form values
  - Auto-fill

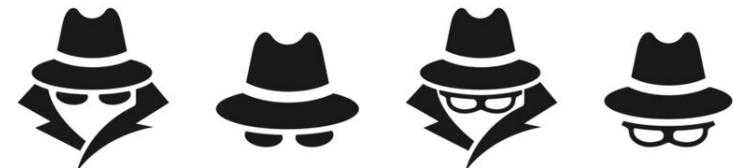
- Downloads
- Favorites
  - a.k.a. Bookmarks



# Private Browsing



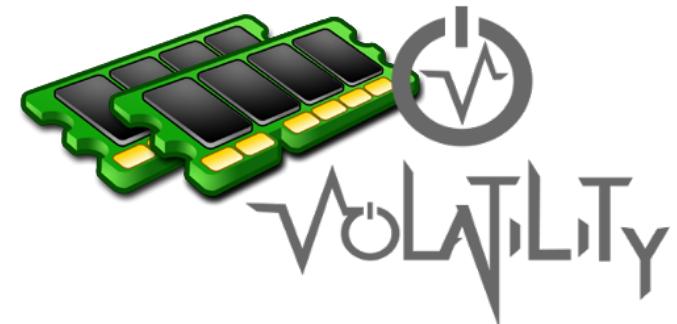
Private (a.k.a. incognito) browsing modes allow users to surf the web without retaining browser history, cache, cookie files, and more.



# Memory Dumps

“Memory Dumps” are a snapshot of memory captured for memory analysis

- When a RAM dump is captured, it contains data relating to all running processes and other web browser artifacts at the time of the memory capture



# History/URLs

This artifact reveals navigation history of the user, which may be used to identify if a user visited malicious websites.

Browser History Examiner

Artifact	Records
Bookmarks	192
Cached Files	20861
Cached Images	8652
Cached Web Pages	898
Cookies	1489
Downloads	121
Email Addresses	35
Favicons	1226
Form History	314
Logins	11
Searches	406
Session Tabs	48
thumbnails	20
<b>Website Visits</b>	<b>2945</b>

Website Visits Report Preview

Date Visited	Title	URL	Visit Type	Visit Count	Calculated
02/11/2015 14:39:40	BBC Sport - Formula 1 2015 driver line-ups: All you	http://www.bbc.co.uk/sport/0/formula1/30427769	Link	1	1
02/11/2015 14:39:40	BBC Sport - Formula 1 2015 driver line-ups: All you	http://www.bbc.co.uk/sport/formula1/30427769	Link	1	1
02/11/2015 14:39:39	BBC Sport - Formula 1 2015: All you need to know	http://www.bbc.co.uk/sport/0/formula1/30913845	Link	1	1
02/11/2015 14:39:39	BBC Sport - Formula 1 2015: All you need to know	http://www.bbc.co.uk/sport/formula1/30913845	Link	1	1
02/11/2015 14:39:38	BBC Sport - Formula 1 gossip: Hamilton, Rosberg, A	http://www.bbc.co.uk/sport/0/formula1/gossip/	Link	1	1
02/11/2015 14:39:38	BBC Sport - Formula 1 gossip: Hamilton, Rosberg, A	http://www.bbc.co.uk/sport/0/formula1/gossip/	Link	1	1
02/11/2015 14:39:38	BBC Sport - Formula 1 gossip: Hamilton, Rosberg, A	http://www.bbc.co.uk/sport/formula1/gossip	Link	1	1
02/11/2015 14:39:36	BBC Sport - 2015 Formula 1 calendar	http://www.bbc.co.uk/sport/0/formula1/race-calen	Link	1	1
02/11/2015 14:39:36	BBC Sport - 2015 Formula 1 calendar	http://www.bbc.co.uk/sport/0/formula1/race-calen	Link	1	1
02/11/2015 14:39:36	BBC Sport - 2015 Formula 1 calendar	http://www.bbc.co.uk/sport/formula1/race-calenda	Link	1	1
02/11/2015 14:39:36	Standings - Drivers' World Championship - Formul	http://www.bbc.co.uk/sport/formula1/drivers-worl	Link	1	1
02/11/2015 14:39:36	Standings - Drivers' World Championship - Formul	http://www.bbc.co.uk/sport/formula1/standings	Link	1	1
02/11/2015 14:39:33	Results - 2015 - Formula 1 - BBC Sport	http://www.bbc.co.uk/sport/formula1/2015/results	Link	1	1
02/11/2015 14:39:33	Results - 2015 - Formula 1 - BBC Sport	http://www.bbc.co.uk/sport/formula1/results	Link	1	1
02/11/2015 14:39:26	BBC Sport - Formula 1	http://www.bbc.co.uk/sport/0/formula1/	Link	1	1
02/11/2015 14:39:26	BBC Sport - Formula 1	http://www.bbc.co.uk/sport/0/formula1	Link	1	1
02/11/2015 14:39:26	BBC Sport - Formula 1	http://www.bbc.co.uk/sport/formula1	Link	1	1
02/11/2015 14:37:44	Results	https://www.formula1.com/content/fom-website/e	Link	2	2
02/11/2015 14:37:42	Inside F1	https://www.formula1.com/content/fom-website/e	Link	2	2
02/11/2015 14:37:41	Teams	https://www.formula1.com/content/fom-website/e	Link	2	2

Filter by keyword: formula1  
Advanced

Filter by date: From: 19/10/2015 To: 03/11/2015

Filter by time: From: Select a time To: Select a time

# Example History Artifact Paths

## Microsoft Edge

- \Users\<username>\AppData\Local\Microsoft\Edge\User Data\Default
- \Users\<username>\AppData\Local\Microsoft\Edge\User Data\Default\Cache

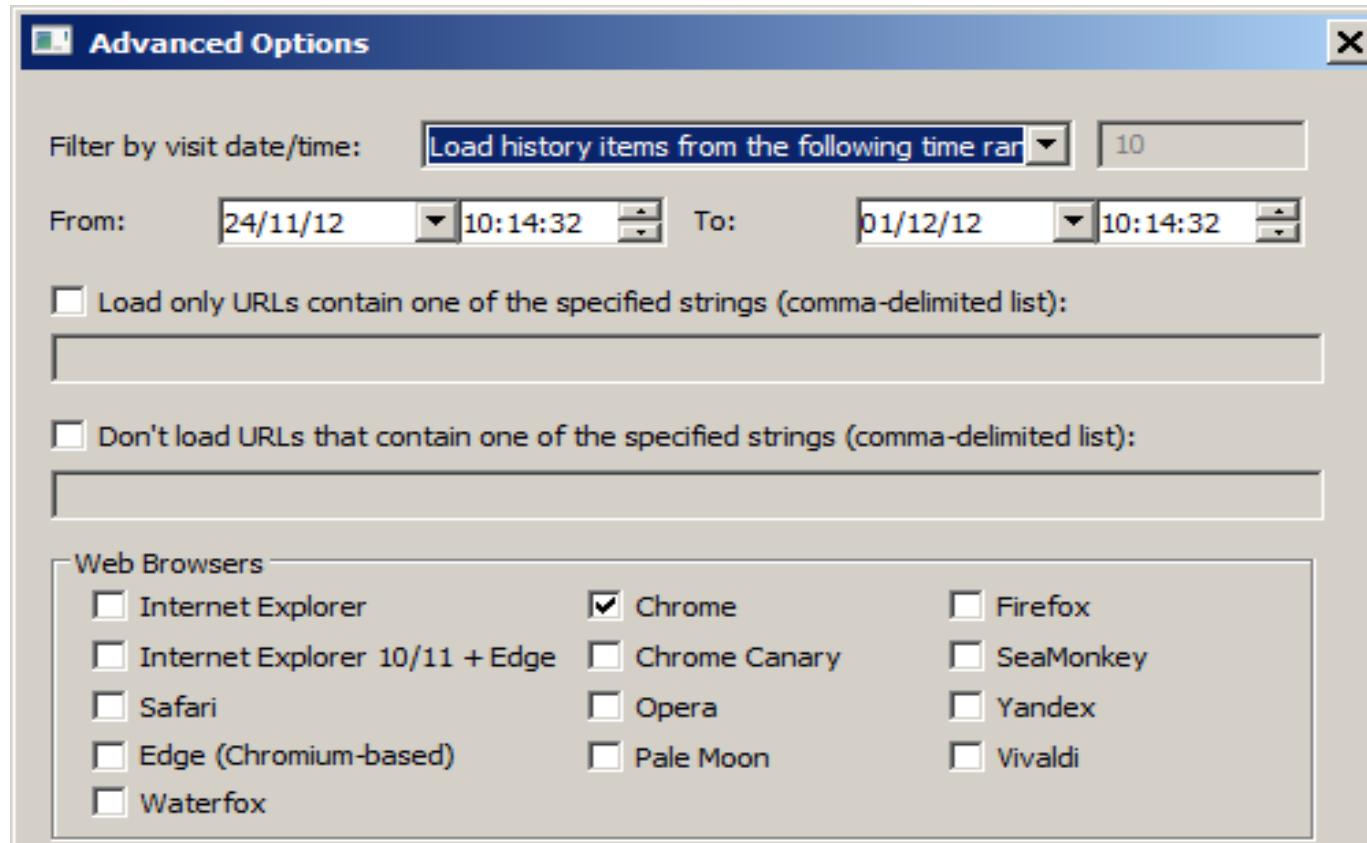
## Mozilla Firefox

- \Users\<username>\AppData\Roaming\Mozilla\Firefox\Profiles\<profile folder>
- \Users\<username>\AppData\Local\Mozilla\Firefox\Profiles\<profile folder>\cache2

## Google Chrome

- \Users\<username>\AppData\Local\Google\Chrome\User Data\Default
- \Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Cache

# History Parsed Example 1/4



# History Parsed Example 2/4

URL	Title	Visit Time	Visit Count	Web browser	User Pr
http://espn.go.com/	ESPN: The Worldwide Lea...	19/08/12 13:45:34	1	Safari	Administ
http://www.apple.com/st...	Apple - Start	19/08/12 13:45:12	2	Safari	Administ
http://www.google.com		19/08/12 13:44:01	43	Internet Explorer	Administ
http://www.google.com		19/08/12 13:44:01	42	Internet Explorer	Administ
https://accounts.google....	Gmail: Email from Google	19/08/12 13:42:52	1	Chrome	Adminis
https://mail.google.com/...	Gmail: Email from Google	19/08/12 13:42:52	1	Chrome	Adminis
https://www.gmail.com/	Gmail: Email from Google	19/08/12 13:42:52	1	Chrome	Adminis
http://www.gmail.com/	Gmail: Email from Google	19/08/12 13:42:52	1	Chrome	Adminis
http://www.facebook.com/	Welcome to Facebook - L...	19/08/12 13:42:39	1	Chrome	Adminis
http://www.windowsmedi...	Windows Media Guide   H...	19/08/12 13:42:23	4	Firefox	Adminis
http://www.windowsmedi...		19/08/12 13:42:22	4	Firefox	Adminis
http://www.windowsmedi...		19/08/12 13:42:22	5	Firefox	Adminis

7727 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

# History Parsed Example 3/4

A	B	C	D	E	F	G	H	I	J	
Browsing History Items										
<b>Browsing History Items</b>										
Created by using BrowsingHistoryView										
URL	→	Title	Visit Time	Visit Count	Visited From	Visit Type	Web Browser	User Profile	Browser Profile	URL Length
<a href="http://windows.microsoft.com/en-US">http://windows.microsoft.com/en-US</a>	3/22/2015 8:09:2		0		Link	Chrome	informant	Default		74
<a href="https://dl.google.com/update2/1_3">https://dl.google.com/update2/1_3</a>	3/22/2015 8:11:0		0		Link	Chrome	informant	Default		284
<a href="http://go.microsoft.com/fwlink/?LinkID=136104">http://go.microsoft.com/fwlink/?LinkID=136104</a>	3/22/2015 8:09:0		0		Link	Chrome	informant	Default		44
<a href="http://go.microsoft.com/fwlink/?LinkID=136104">http://go.microsoft.com/fwlink/?LinkID=136104</a>	3/22/2015 8:09:2		0		Link	Chrome	informant	Default		45
<a href="https://www.google.com/webhp?sc">https://www.google.com/webhp?sc</a>	3/22/2015 8:55:4		1	<a href="https://www.google.com/webhp?sc">https://www.google.com/webhp?sc</a>	Link	Chrome	admin11	Default		84
<a href="http://web.dl.sourceforge.net/project">http://web.dl.sourceforge.net/project</a>	3/25/2015 7:47:3		1			Internet Explorer	informant			84
<a href="https://www.google.com/">https://www.google.com/</a>	security checkpoint	3/24/2015 2:06:5	1		Link	Chrome	informant	Default		50
<a href="http://www.bing.com">http://www.bing.com</a>	Bing	3/24/2015 2:05:4	1		Reload	Chrome	informant	Default		20
<a href="https://news.google.com">https://news.google.com</a>	Google News	3/24/2015 12:01:1	1		Reload	Chrome	informant	Default		46
<a href="http://www.hindustantimes.com">http://www.hindustantimes.com</a>	Ringo	3/24/2015 12:01:1	1		Reload	Chrome	informant	Default		20

Exported to Excel for detailed inspection and analysis.

# History Parsed Example 4/4

The screenshot shows the DB Browser for SQLite interface with the following details:

- Title Bar:** DB Browser for SQLite - C:/Users/[REDACTED]/AppData/Local/Google/Chrome/User Data/Default/History
- Menu Bar:** File, Edit, View, Help
- Toolbar:** New Database, Open Database, Write Changes, Revert Changes
- Database Structure Tab:** Shows the "urls" table.
- Table "urls":** Contains 61 rows of data. The columns are: id, url, title, visit\_count, typed\_count, last\_visit\_time, and hidden. A sample of the data is shown below:

	id	url	title	visit_count	typed_count	last_visit_time	hidden
1	178	https://support.google.com/chrome/answer/157179?hl=en	Keyboard sho...	1	0	13100885771...	0
2	177	https://support.google.com/?p=help&cbx=keyboard#topic=3227...		1	0	13100885763...	0
3	176	https://support.google.com/chrome/?p=help&cbx=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

- DB Schema Tab:** Shows the database schema with 9 tables and 13 indices.

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)	

Parsed with a GUI SQLite database browser

# Typed Addresses/URLs

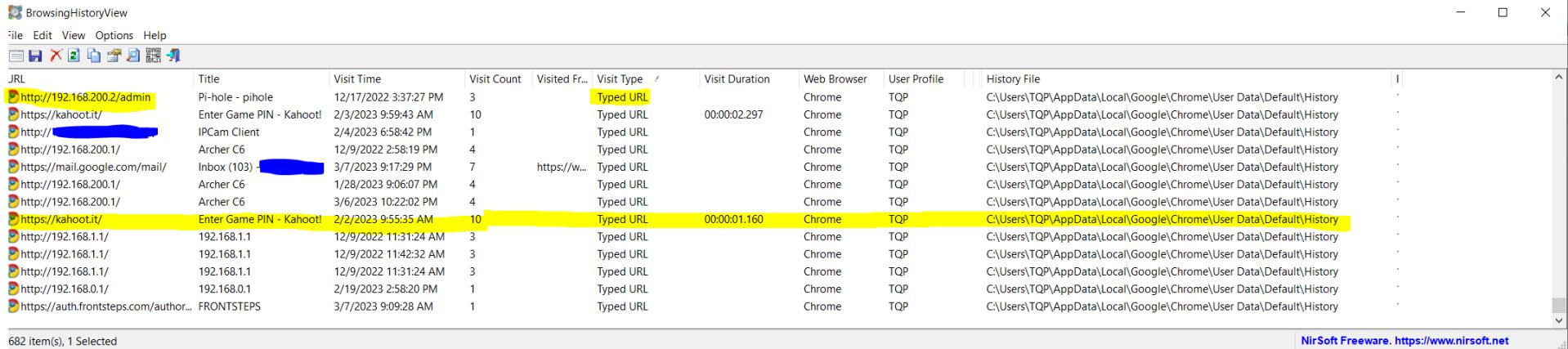
This artifact contains any URL that is typed into the browser address bar.



Also found within the Windows registry (NTUSER.DAT)

- Software\Microsoft\InternetExplorer\TypedURLs

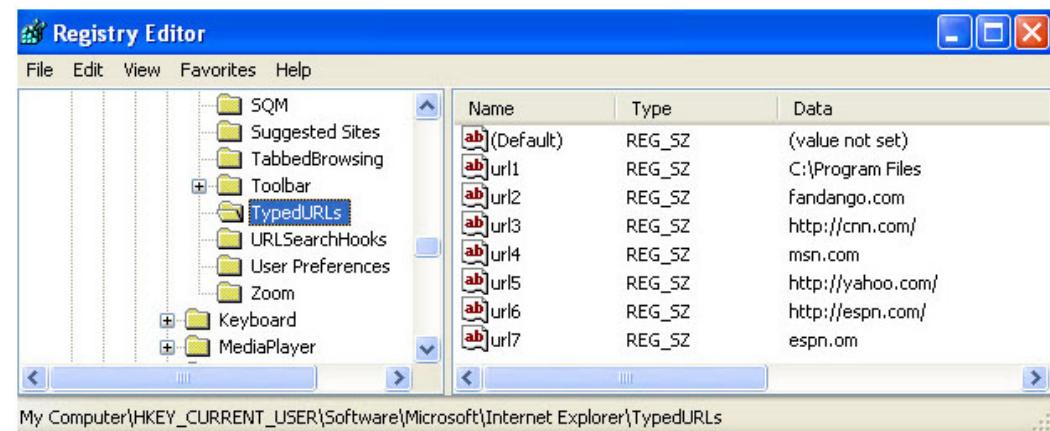
# Typed URLs Parsed Example



The screenshot shows a software application window titled "BrowsingHistoryView". The menu bar includes File, Edit, View, Options, and Help. The main table displays a list of browser visits. The columns are: JRL, Title, Visit Time, Visit Count, Visited Fr..., Visit Type, Visit Duration, Web Browser, User Profile, and History File. Several rows are highlighted with yellow background, specifically the first two rows and the row for "Enter Game PIN - Kahoot!". The "Visit Type" column for these rows is labeled "Typed URL". The "History File" column for these rows points to the same file: C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History.

JRL	Title	Visit Time	Visit Count	Visited Fr...	Visit Type	Visit Duration	Web Browser	User Profile	History File
http://192.168.200.2/admin	Pi-hole - pihole	12/17/2022 3:37:27 PM	3		Typed URL		Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
https://kahoot.it/	Enter Game PIN - Kahoot!	2/3/2023 9:59:43 AM	10		Typed URL	00:00:02.297	Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
http://[REDACTED]	IPCam Client	2/4/2023 6:58:42 PM	1		Typed URL		Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
http://192.168.200.1/	Archer C6	12/9/2022 2:58:19 PM	4		Typed URL		Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
https://mail.google.com/mail/	Inbox (103) [REDACTED]	3/7/2023 9:17:29 PM	7	https://w...	Typed URL		Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
http://192.168.200.1/	Archer C6	1/28/2023 9:06:07 PM	4		Typed URL		Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
http://192.168.200.1/	Archer C6	3/6/2023 10:22:02 PM	4		Typed URL		Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
https://kahoot.it/	Enter Game PIN - Kahoot!	2/2/2023 9:55:35 AM	10		Typed URL	00:00:01.160	Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
http://192.168.1.1/	192.168.1.1	12/9/2022 11:31:24 AM	3		Typed URL		Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
http://192.168.1.1/	192.168.1.1	12/9/2022 11:42:32 AM	3		Typed URL		Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
http://192.168.1.1/	192.168.1.1	12/9/2022 11:31:24 AM	3		Typed URL		Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
http://192.168.0.1/	192.168.0.1	2/19/2023 2:58:20 PM	1		Typed URL		Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History
https://auth.frontsteps.com/author...	FRONTSTEPS	3/7/2023 9:09:28 AM	1		Typed URL		Chrome	TQP	C:\Users\TQP\AppData\Local\Google\Chrome\User Data\Default\History

Artifact from Registry:



The screenshot shows the Windows Registry Editor. The left pane shows a tree view of registry keys under "HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer". One of the keys is "TypedURLs", which is expanded to show its subkeys: SQM, Suggested Sites, TabbedBrowsing, Toolbar, URLSearchHooks, User Preferences, Zoom, Keyboard, and MediaPlayer. The right pane displays a table of registry values for the "TypedURLs" key. The table has columns: Name, Type, and Data. There are seven entries, each starting with "ab" and ending with "url1" through "url7". The "Data" column contains various URLs such as "C:\Program Files", "fandango.com", "http://cnn.com/", "msn.com", "http://yahoo.com/", "http://espn.com/", and "espn.com".

Name	Type	Data
ab(Default)	REG_SZ	(value not set)
ab:url1	REG_SZ	C:\Program Files
ab:url2	REG_SZ	fandango.com
ab:url3	REG_SZ	http://cnn.com/
ab:url4	REG_SZ	msn.com
ab:url5	REG_SZ	http://yahoo.com/
ab:url6	REG_SZ	http://espn.com/
ab:url7	REG_SZ	espn.com

# Browser Cache

Contains cache data from various websites such as: image files, JavaScript files, etc.

- Example artifact paths
  - Chrome & EDGE Cache is stored using an Index file ('index'), a number of Data Block files ('data\_#'), and a number of separate data files ('f\_#####')
  - Firefox Cache is stored using a Cache Map File ('\_CACHE\_MAP\_'), three Cache Block files ('\_CACHE\_00#\_'), and a number of separate data files. The cache structure was changed in Firefox version 32 and named 'Cache v2'

# Cache Parsed

Browser History Examiner

File Options Filter Report Tools Help

Artefact Records Cached Images Report Preview

Artefact	Records
Bookmarks	192
Cached Files	20861
<b>Cached Images</b>	<b>8652</b>
Cached Web Pages	898
Cookies	1489
Downloads	121
Email Addresses	35
Favicons	1226
Form History	314
Logins	11
Searches	406
Session Tabs	48
thumbnails	20
Website Visits	2945

Last Fetched Content Type URL Fetch Count File Size (Bytes) Web Browser

Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser
02/11/2015 15:18:03	image/jpeg	http://www.formula1.com/content/fom-website/en/championsl	38952	Chrome	
02/11/2015 15:18:13	image/jpeg	http://www.formula1.com/content/fom-website/en/championsl	36550	Chrome	
02/11/2015 15:18:24	image/jpeg	https://www.formula1.com/content/fom-website/en/champions	35465	Chrome	
02/11/2015 15:18:10	image/jpeg	http://www.formula1.com/content/fom-website/en/championsl	29973	Chrome	
02/11/2015 15:20:32	image/jpeg	http://www.formula1.com/content/fom-website/en/video/2015,	28316	Chrome	
02/11/2015 15:18:24	image/jpeg	https://www.formula1.com/content/fom-website/en/champions	27190	Chrome	
02/11/2015 15:18:04	image/jpeg	http://www.formula1.com/content/fom-website/en/championsl	26488	Chrome	
02/11/2015 15:17:50	image/jpeg	http://www.formula1.com/content/fom-website/en/latest/featu	25334	Chrome	
02/11/2015 15:20:31	image/jpeg	http://www.formula1.com/content/fom-website/en/latest/head	25214	Chrome	
02/11/2015 15:18:02	image/jpeg	http://www.formula1.com/content/fom-website/en/championsl	24777	Chrome	
02/11/2015 15:18:02	image/jpeg	http://www.formula1.com/content/fom-website/en/championsl	23777	Chrome	
02/11/2015 15:17:50	image/jpeg	http://www.formula1.com/content/fom-website/en/championsl	23195	Chrome	
02/11/2015 15:18:01	image/jpeg	http://www.formula1.com/content/fom-website/en/championsl	22517	Chrome	
02/11/2015 15:20:31	image/jpeg	http://www.formula1.com/content/fom-website/en/latest/featu	21714	Chrome	
02/11/2015 15:18:02	image/jpeg	http://www.formula1.com/content/fom-website/en/championsl	20793	Chrome	
02/11/2015 15:18:11	image/jpeg	http://www.formula1.com/content/fom-website/en/championsl	19447	Chrome	

Filter by keyword: formula1 Advanced

Filter by date: From: 19/10/2015 To: 03/11/2015

Filter by time: From: Select a time To: Select a time

Filter by web browser: All

Filter, Undo, Clear

Page 4 of 8 Viewing 219/13140 records

www.foxtonforensics.com Time zone: UTC, DST Enabled Date format: dd/mm/yyyy

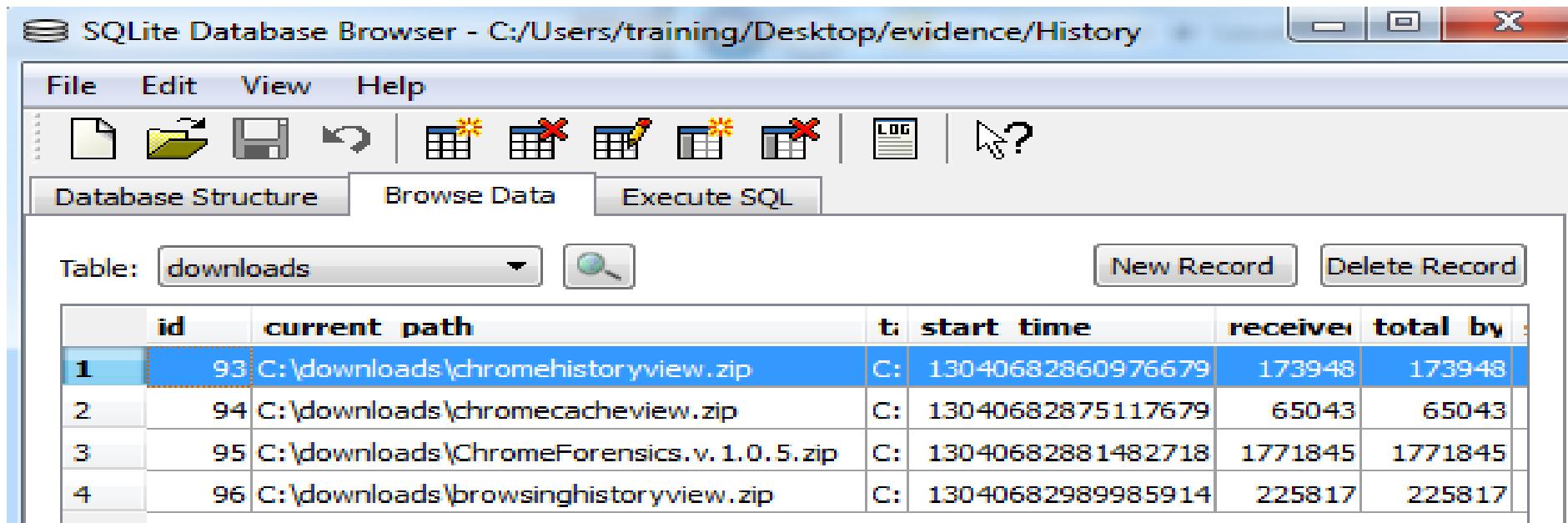
# Downloads

Provides the file system location where a user's file downloads were saved

- Example artifact paths
  - Chrome & EDGE Downloads are stored in the 'History' SQLite database, within the 'downloads' and 'downloads\_url\_chains' tables
  - Firefox Downloads are stored in the 'places.sqlite' database, within the 'moz\_anno' table and associated URL information is stored within the 'moz\_places' table

# Download Parsed Example 1/2

## SQLite database browser GUI



The screenshot shows the SQLite Database Browser interface. The title bar reads "SQLite Database Browser - C:/Users/training/Desktop/evidence/History". The menu bar includes File, Edit, View, and Help. The toolbar contains icons for file operations like Open, Save, and Print, as well as database management icons. Below the toolbar are three tabs: "Database Structure", "Browse Data" (which is selected), and "Execute SQL". The main area displays a table named "downloads". The table has columns: id, current\_path, t, start\_time, receiver, total, by, and state. The data shows four rows of download entries:

	<b>id</b>	<b>current_path</b>	<b>t</b>	<b>start_time</b>	<b>receiver</b>	<b>total</b>	<b>by</b>	<b>state</b>
1	93	C:\downloads\chromehistoryview.zip	C:	13040682860976679	173948	173948		0
2	94	C:\downloads\chromecacheview.zip	C:	13040682875117679	65043	65043		0
3	95	C:\downloads\ChromeForensics.v.1.0.5.zip	C:	13040682881482718	1771845	1771845		0
4	96	C:\downloads\browsinghistoryview.zip	C:	13040682989985914	225817	225817		0

Download State: The 'value' appears in the 'History' SQLite database → 'downloads' table → 'state' column.

# Download Parsed Example 2/2

Filename	Download URL	Web Page URL	Start Time	End Time	Download Size	Downloaded
TCPView.zip	https://download.sysinternals.c...	https://docs.microsoft.com/...	06/01/20 11:41:21	06/01/20 1...	291,606	00:00:0
ProcessMonitor.zip	https://download.sysinternals.c...	https://docs.microsoft.com/...	06/01/20 11:41:07	06/01/20 1...	1,567,005	00:00:0
ProcessExplorer...	https://download.sysinternals.c...	https://docs.microsoft.com/...	06/01/20 11:41:00	06/01/20 1...	2,007,844	00:00:0
nirsoft_package...	https://download.nirsoft.net/nir...	https://launcher.nirsoft.net...	06/01/20 11:40:07	06/01/20 1...	31,371,134	00:00:0
uninstallview-x6...	http://www.nirsoft.net/utils/unin...	http://www.nirsoft.net/utils...	06/01/20 11:37:36	06/01/20 1...	111,036	00:00:0
uninstallview.zip	http://www.nirsoft.net/utils/unin...	http://www.nirsoft.net/utils...	06/01/20 11:37:32	06/01/20 1...	91,377	00:00:0
appnetworkcoun...	http://www.nirsoft.net/utils/app...	http://www.nirsoft.net/utils...	06/01/20 11:37:15	06/01/20 1...	63,475	00:00:0
wifiinfoview.zip	http://www.nirsoft.net/utils/wifi...	http://www.nirsoft.net/utils...	06/01/20 11:36:50	06/01/20 1...	361,269	00:00:0
Sysmon.zip	https://download.sysinternals.c...	https://docs.microsoft.com/...	06/01/20 11:36:28	06/01/20 1...	1,740,363	00:00:0
PSTools.zip	https://download.sysinternals.c...	https://docs.microsoft.com/...	06/01/20 11:35:54	06/01/20 1...	3,187,562	00:00:0
DebugView.zip	https://download.sysinternals.c...	https://docs.microsoft.com/...	06/01/20 11:35:42	06/01/20 1...	475,424	00:00:0
DebugView.zip	https://download.sysinternals.c...	https://docs.microsoft.com/...	06/01/20 11:35:15	06/01/20 1...	475,424	00:00:0
SysinternalsSuit...	https://download.sysinternals.c...	https://docs.microsoft.com/...	06/01/20 11:35:03	06/01/20 1...	30,403,934	00:00:0
VirtualBox-6.1.0...	https://download.virtualbox.org...	https://www.virtualbox.org...	06/01/20 11:34:40	06/01/20 1...	111,891,976	00:00:2

406 item(s), 1 Selected

NirSoft Freeware. <https://www.nirsoft.net>

# Future Trends

- I anticipate a growing need in performing forensic analysis within web browsers on mobile devices and in Cloud environments
- As we look toward the future, two trends are likely to emerge
  - Technology & eBusiness will continue to evolve, with data privacy efforts creating new challenges for investigators
  - Increases in cybercrime creating demand for talented forensic practitioners in this career field

# Conclusions

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

Analyzing a web browser's artifacts help the investigator understand the objective, methods, and criminal activities/insider threats.

Examining a suspect's system, the web browser's log details remain a key artifact of most 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...



We too, or is it  
two? ...Can play  
at that game!

# 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 3<sup>rd</sup> party modules

# Warning!



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

- We'll touch on potentially 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, Auto-runs, and Tasks

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

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

```
Get-CimInstance Win32_StartupCommand
```

```
Get-ScheduledTask
```

# 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

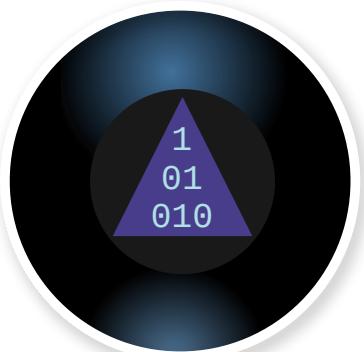
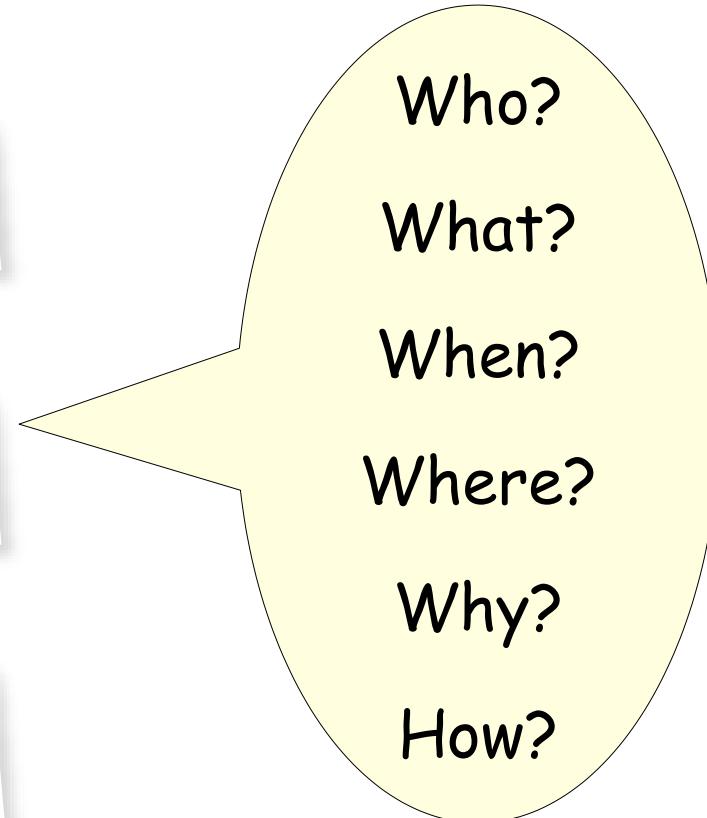
These commands and cmdlets barely scratch the surface of PowerShell capabilities in alignment with our objectives of collecting and preservation of data with minimal impacts and changes to the host operating system that we are investigating.

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!



# CiNPA

## Security SIG

Matt Scheurer  
Tuan Phan

