Browser Forensics

Thomas Benos

MSc UniWA, Cisco CyberOps
GR CSIRT Incident Responder
thomasbenos1291@gmail.com

Agenda

- Browser Artifacts Introduction
- IE & Microsoft Edge Browser Forensic Artifacts
- Mozilla Firefox Forensic Artifacts
- Google Chrome Forensic Artifacts

Browser Artifacts Introduction

Browser Artifacts Introduction

Browser Artifacts Introduction

- Browser History
- Cache
- Cookies
- Bookmarks
- Recovery Folders
- Typed URLs
- Autocomplete

Browser Artifacts – Questions to Answer

- What websites were visited?
  - History, Cache, Cookies, Recovery Folders, Typed URLs
- How many times?
  - History
- When?
  - History, Cookies, Cache, Recovery Folders
- What sites were saved?
  - Bookmarks
- What files were downloaded
  - Downloaded Folder, Cache
- Usernames?
  - Cookies, Cache, Recovery Folders, Autocomplete
- What was searched?
  - Autocomplete, Cache

IE & Microsoft Edge Browser Artifacts

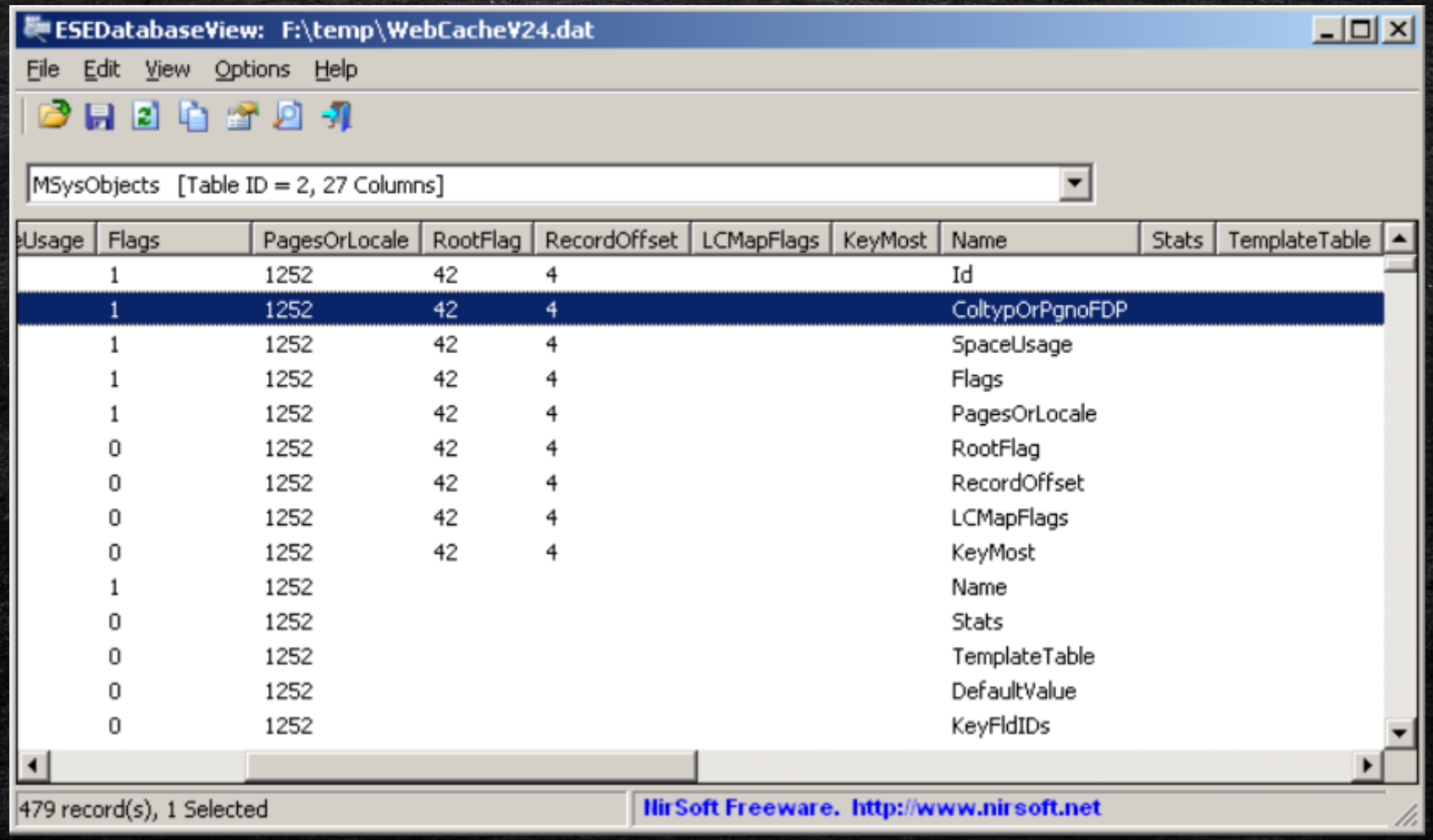
IE & Edge Artifacts – Data Locations

- Metadata (Cache, History, Cookies, Downloads):
  - %Appdata%\Local\Microsoft\Windows\WebCache\WebCacheV*.dat
- Storage
  - Cache:
    - %Appdata%\Local\Microsoft\Windows\InetCache\IE
    - %Appdata%\Local\Microsoft\Windows\InetCache\Low\IE
  - Cookies:
    - %Appdata%\Local\Microsoft\Windows\INetCookies
    - %Appdata%\Local\Microsoft\Windows\\INetCookies\Low
  - Edge:
    - %Appdata%\Local\Microsoft\Edge\UserData\{Default|ProfileName}\
      - History, Top Sites, \Network\Cookies (sqlite databases)
      - Cache\(individual files)

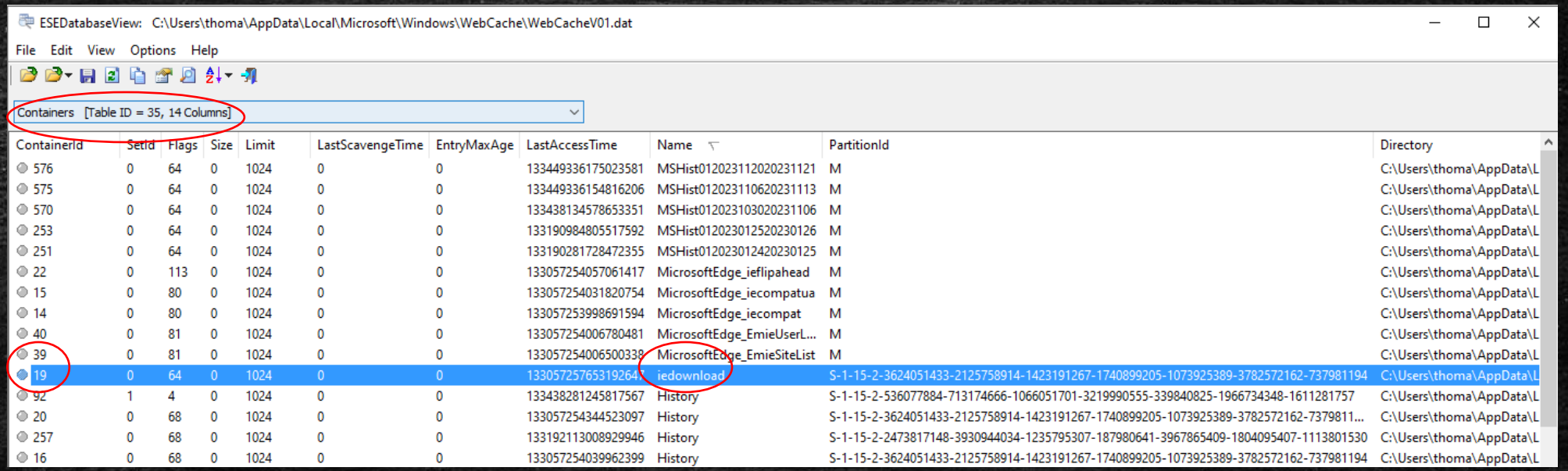
IE & Edge Artifacts – WebCacheV*.dat

- ESE DB (Remember! ESE dbs are dirty!)
  - esentutl /mh WebCacheV001.dat
  - esentutl /r WebCacheV001.dat /d
    - Transaction logs must be present in the dir
- History:
  - Sites visited by date and time, frequency, access to local files, user accounts
  - User can clear it
  - Also local files Accessed (Not directly opened with browser)

IE & Edge Artifacts – ESEDatabaseView

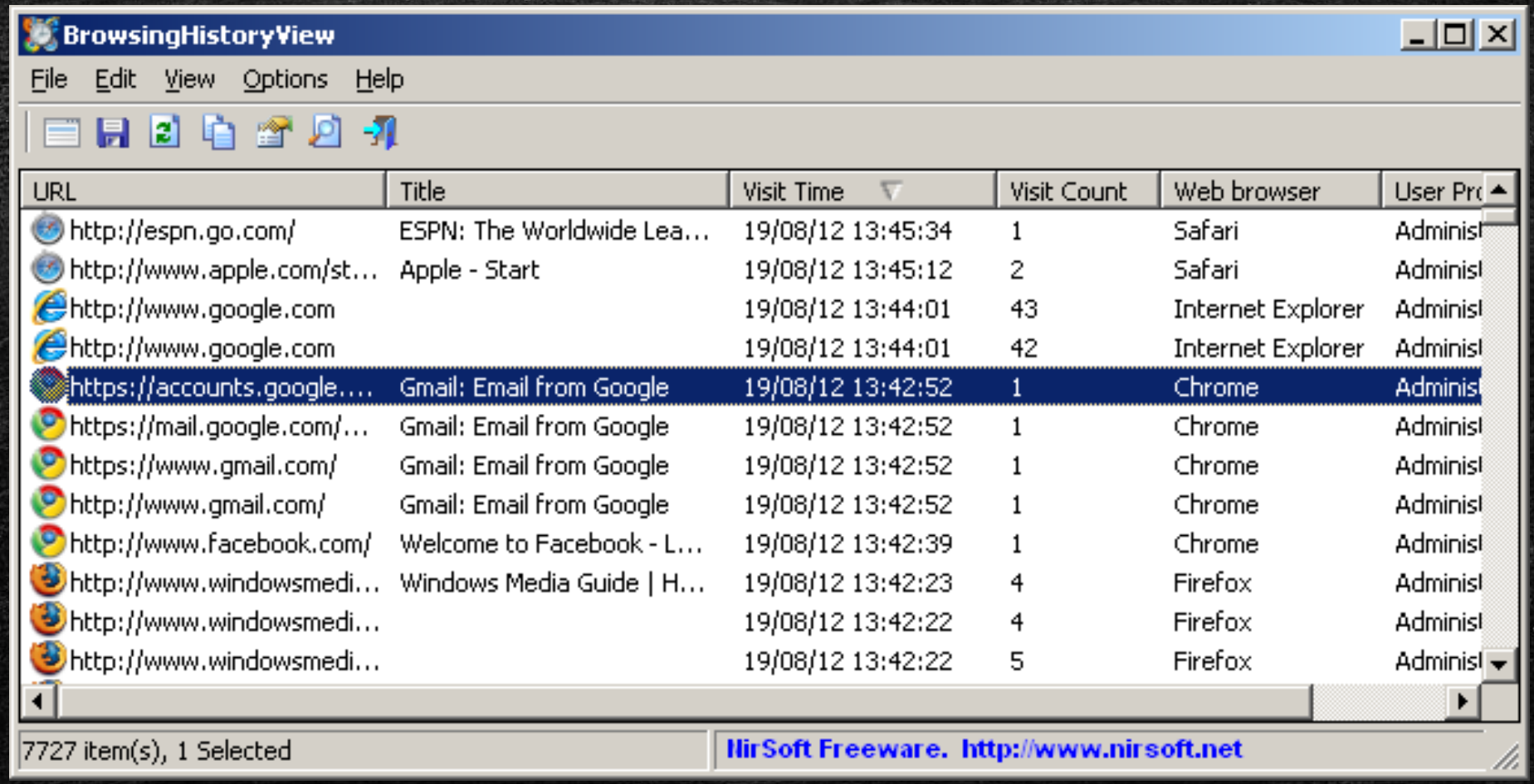


IE & Edge Artifacts – ESEDatabaseView



ContainerId	SetId	Flags	Size	Limit	LastScavengeTime	EntryMaxAge	LastAccessTime	Name	PartitionId	Directory
576	0	64	0	1024	0	0	133449336175023581	MSHist012023112020231121	M	C:\Users\thoma\AppData\L
575	0	64	0	1024	0	0	133449336154816206	MSHist012023110620231113	M	C:\Users\thoma\AppData\L
570	0	64	0	1024	0	0	133438134578653351	MSHist012023103020231106	M	C:\Users\thoma\AppData\L
253	0	64	0	1024	0	0	133190984805517592	MSHist012023012520230126	M	C:\Users\thoma\AppData\L
251	0	64	0	1024	0	0	133190281728472355	MSHist012023012420230125	M	C:\Users\thoma\AppData\L
22	0	113	0	1024	0	0	133057254057061417	MicrosoftEdge_ieflipahead	M	C:\Users\thoma\AppData\L
15	0	80	0	1024	0	0	133057254031820754	MicrosoftEdge_iecompatua	M	C:\Users\thoma\AppData\L
14	0	80	0	1024	0	0	133057253998691594	MicrosoftEdge_iecompat	M	C:\Users\thoma\AppData\L
40	0	81	0	1024	0	0	133057254006780481	MicrosoftEdge_EmieUserL...	M	C:\Users\thoma\AppData\L
39	0	81	0	1024	0	0	133057254006500338	MicrosoftEdge_EmieSiteList	M	C:\Users\thoma\AppData\L
19	0	64	0	1024	0	0	133057257653192647	iedownload	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194	C:\Users\thoma\AppData\L
92	1	4	0	1024	0	0	133438281245817567	History	S-1-15-2-536077884-713174666-1066051701-3219990555-339840825-1966734348-1611281757	C:\Users\thoma\AppData\L
20	0	68	0	1024	0	0	133057254344523097	History	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-7379811...	C:\Users\thoma\AppData\L
257	0	68	0	1024	0	0	133192113008929946	History	S-1-15-2-2473817148-3930944034-1235795307-187980641-3967865409-1804095407-1113801530	C:\Users\thoma\AppData\L
16	0	68	0	1024	0	0	133057254039962399	History	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194	C:\Users\thoma\AppData\L

IE & Edge Artifacts – BrowsingHistoryView



IE & Edge Artifacts – Cache

- Locally stored web page components.
- Can be a snapshot in time.
  - Pages visited
  - Actual files viewed
  - Timestamps: First Viewed (Creation) & Last Viewed (Access)
    - Modified: Content changed in web server
    - Expiry Time: age out of pages
- Default size: 250MB
- Files: InetCache (IE), Cache (Edge)
- Metadata: WebCacheV*.dat
  - Filename
  - FileSize
  - SecureDirectory
  - AccessCount
  - URL

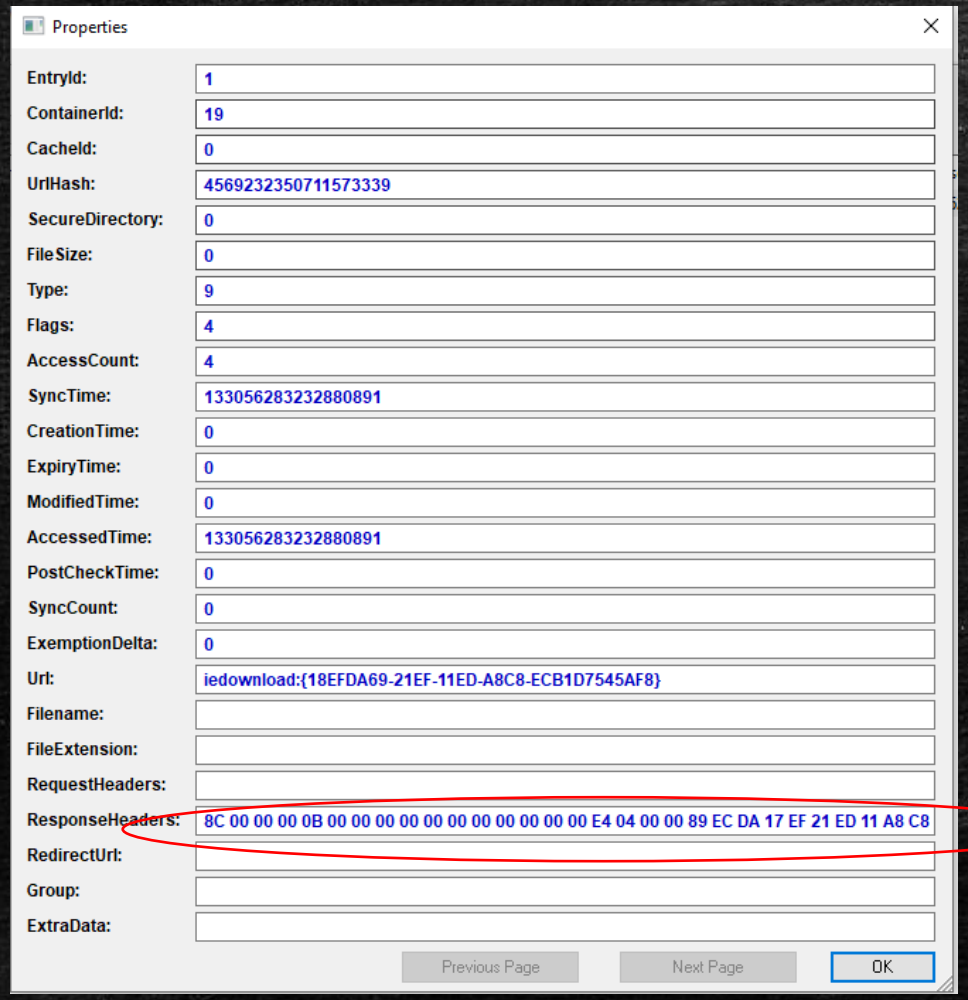
IE & Edge Artifacts – Cookies

- Small pieces of data – enable websites to remember info about the user
- Sites Visited
  - Filename
  - URL
  - User Account
  - Access Count
  - Creation Time
  - ModifiedTime
  - AccessedTime
  - Expiry date
- Only Persistent Cookies remain - Session Cookies remain only in memory
- Cookie Metadata:
  - WebCacheV*.dat (Cookies table, IE 10+)
  - %AppData%\Roaming\Microsoft\Windows\Cookies\(Low\)index.dat (IE4 – IE9)
  - \Network\Cookies (sqlite database, Edge)

IE & Edge Artifacts – Download History

- WebCacheV*: ESEDatabaseView Container: **iedownload**
  - Filename
  - File size
  - Originating URL
  - Referring URL
  - Download Destination
  - Time of Download
- You can convert the Response Headers to ASCII (notepad++, CyberChef)

IE & Edge Artifacts – Download History



http://thewaltdisneycompany.com/investors/financial-information/sec-filings -> **Referer**

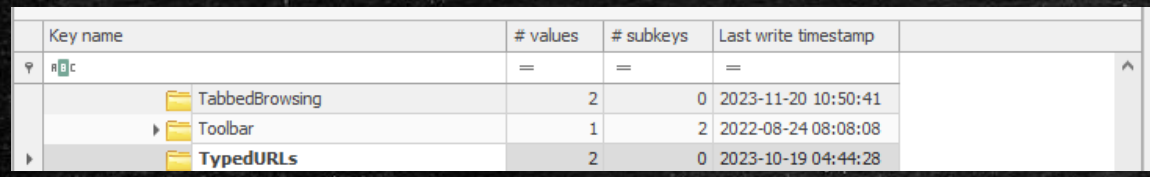
application/pdf -> **Content Type**

C:\Users\user\AppData\Local\Microsoft\Windows\TemporearyInternetFiles\Low\Content.IE5\....\file.pdf **-> Download URL**

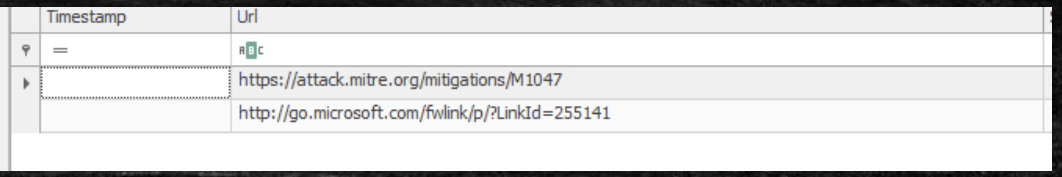
http://thewaltdisneycompany.com/sites/default/files/reports/file.pdf **-> Save Location**

IE & Edge Artifacts – Typed URLs

- NTUSER.dat\Software\Microsoft\InternetExplorer\TypedURLs
  - Not updated by clicking a link
  - Used for the autocomplete function of the Browser
- Last used time (IE 10+):
  - NTUSER.dat\Software\Microsoft\InternetExplorer\TypedURLsTime



Key name	# values	# subkeys	Last write timestamp
TabbedBrowsing	2	0	2023-11-20 10:50:41
Toolbar	1	2	2022-08-24 08:08:08
TypedURLs	2	0	2023-10-19 04:44:28



Timestamp	Url
	https://attack.mitre.org/mitigations/M1047
	http://go.microsoft.com/fwlink/p/?LinkId=255141

IE & Edge Artifacts – AutoComplete & Windows Vault

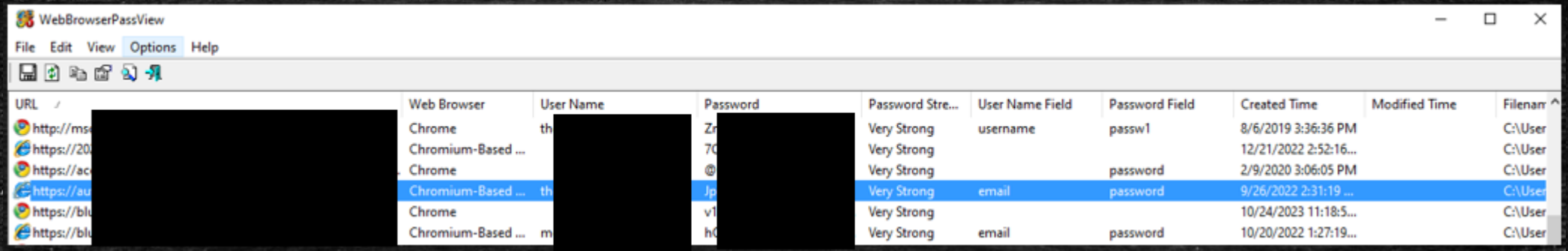
- User: %AppData%\{Local|Roaming}\Microsoft\Vault{GUID}
- System: %System32%\config\systemprofile\Appdata\{Local|Roaming}\Vault\{GUID}

- .vpol: encryption keys for the records
- .vcrd: Credentials

- Credentials are secured by user's logon credentials
  - DataProtectionAPI (DPAPI)
  - Can be cracked

- WebBrowserPassView (all browsers)
- Windows Credential Manager

IE & Edge Artifacts – AutoComplete & Windows Vault



IE & Edge Artifacts – Bookmarks

- Specific URLs – user account – creation time – last access
- %UserProfile%\Favorites*.url
  - Everything added here is imported to the favorites on the browser
  - *[InternetShortcut]*
    URL="http://support.dell.com/support/index.aspx?c=us&l=en"
- Edge: %AppData%\Local\Packages\Microsoft.MicrosoftEdge_<APPID>\AC\MicrosoftEdge\User\Default\Data Store\Data\nouser1\120712-49\DBStore\Spartan.db (ESE DB)
  - Table name: Favorites
  - In the Spartan.db we can also find the Top Sites that are displayed in a new tab
- FireFox: places.sqlite (moz_bookmarks table)
- Chrome: Bookmarks
- FavoritesView (Nirsoft)
  - For all browsers

IE & Edge Artifacts – Session Recovery

- Used for automatic crash recovery
- Artifacts:
  - Opened tabs
  - Historical record of websites in each tab
  - Referring websites
  - Started and Ended Session
  - HTML/Javascript/XML
  - Form data
- Tool: StructureStorage Viewer (MiTec)

IE & Edge Artifacts – Session Recovery (IE)

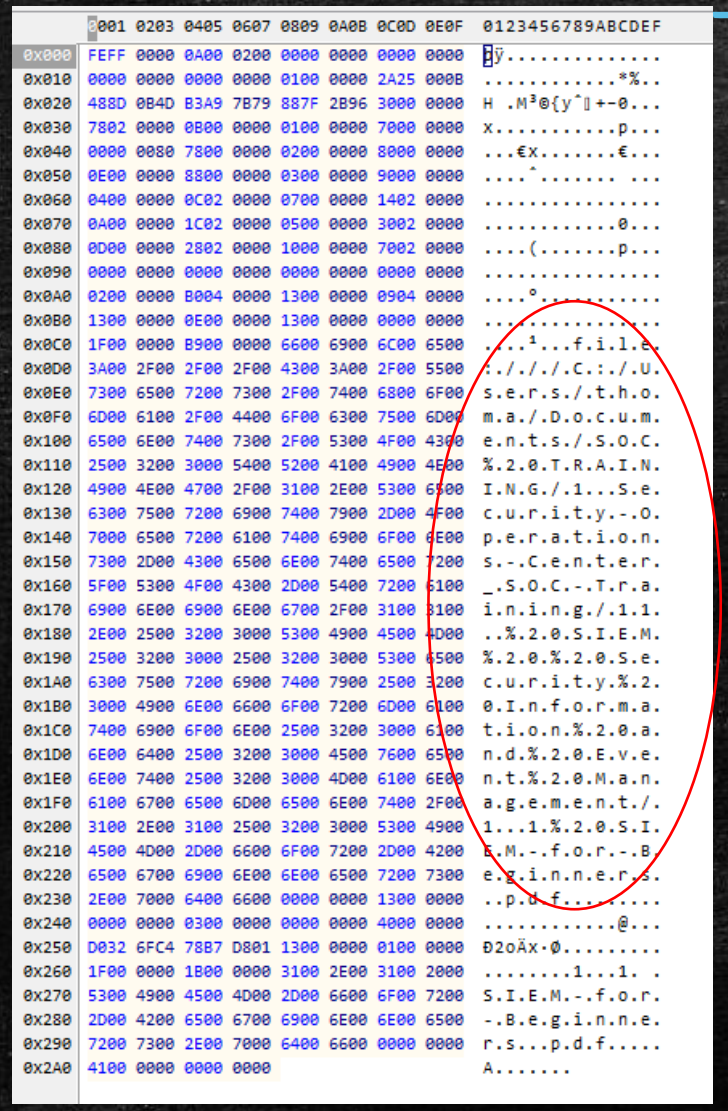
```
%USERPROFILE%/AppData/Local/Microsoft/Internet Explorer/Recovery/Active
(Current Session)
%USERPROFILE%/AppData/Local/Microsoft/Internet Explorer/Recovery/Last Active
(Last Session)
%USERPROFILE%/AppData/Local/Microsoft/Internet
Explorer/Recovery/Immersive/Active  (Current Session - Modern IE Application)
%USERPROFILE%/AppData/Local/Microsoft/Internet
Explorer/Recovery/Immersive/Last Active  (Last Session - Modern IE
Application)
%USERPROFILE%/Local Settings/Application Data/Microsoft/Internet
Explorer/Recovery/High/Active (Current Session - High Integrity)
%USERPROFILE%/Local Settings/Application Data/Microsoft/Internet
Explorer/Recovery/High/Last Active (Last Session - High Integrity)
```

- XP (IE8 Only)

```
%USERPROFILE%/Local Settings/Application Data/Microsoft/Internet
Explorer/Recovery/Active
%USERPROFILE%/Local Settings/Application Data/Microsoft/Internet
Explorer/Recovery/LastActive
```

- Edge: %LocalAppData%\Microsoft\Edge\User Data\[Default|Profile X]\Sessions*

IE & Edge Artifacts – Session Recovery (Edge)



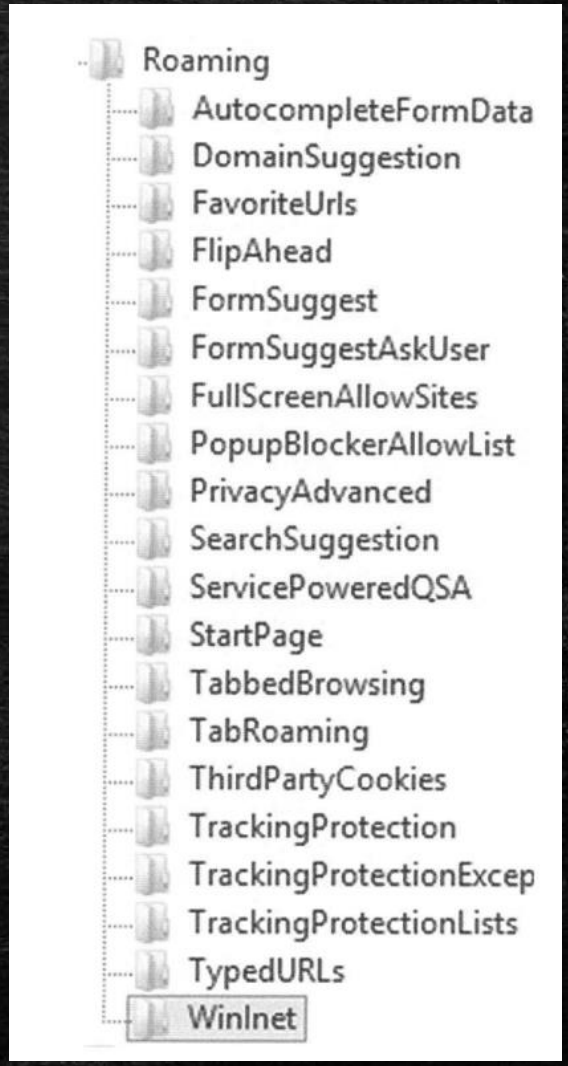
	0001 0203 0405 0607 0809 0A0B 0C0D 0E0F	0123456789ABCDEF
0x000	FEFF 0000 0A00 0200 0000 0000 0000 0000	þÿ..............
0x010	0000 0000 0000 0000 0100 0000 2A25 000B	............*%..
0x020	488D 0B4D B3A9 7B79 887F 2B96 3000 0000	H .M³©{y^▯+-0...
0x030	7802 0000 0B00 0000 0100 0000 7000 0000	x...........p...
0x040	0000 0080 7800 0000 0200 0000 8000 0000	...€x.......€...
0x050	0E00 0000 8800 0000 0300 0000 9000 0000	....ˆ....... ...
0x060	0400 0000 0C02 0000 0700 0000 1402 0000	....
0x070	0A00 0000 1C02 0000 0500 0000 3002 0000	............0...
0x080	0D00 0000 2802 0000 1000 0000 7002 0000	....(.......p...
0x090	0000 0000 0000 0000 0000 0000 0000 0000	....
0x0A0	0200 0000 B004 0000 1300 0000 0904 0000	....°...........
0x0B0	1300 0000 0E00 0000 1300 0000 0000 0000	....
0x0C0	1F00 0000 B900 0000 6600 6900 6C00 6500	....¹...f.i.l.e.
0x0D0	3A00 2F00 2F00 2F00 4300 3A00 2F00 5500	:././.C.:./.U.
0x0E0	7300 6500 7200 7300 2F00 7400 6800 6F00	s.e.r.s./.t.h.o.
0x0F0	6D00 6100 2F00 4400 6F00 6300 7500 6D00	m.a./.D.o.c.u.m.
0x100	6500 6E00 7400 7300 2F00 5300 4F00 4300	e.n.t.s./.S.O.C.
0x110	2500 3200 3000 5400 5200 4100 4900 4E00	%.2.0.T.R.A.I.N.
0x120	4900 4E00 4700 2F00 3100 2E00 5300 6500	I.N.G./.1...S.e.
0x130	6300 7500 7200 6900 7400 7900 2D00 4F00	c.u.r.i.t.y.-.O.
0x140	7000 6500 7200 6100 7400 6900 6F00 6E00	p.e.r.a.t.i.o.n.
0x150	7300 2D00 4300 6500 6E00 7400 6500 7200	s.-.C.e.n.t.e.r.
0x160	5F00 5300 4F00 4300 2D00 5400 7200 6100	_.S.O.C.-.T.r.a.
0x170	6900 6E00 6900 6E00 6700 2F00 3100 3100	i.n.i.n.g./.1.1.
0x180	2E00 2500 3200 3000 5300 4900 4500 4D00	..%.2.0.S.I.E.M.
0x190	2500 3200 3000 2500 3200 3000 5300 6500	%.2.0.%.2.0.S.e.
0x1A0	6300 7500 7200 6900 7400 7900 2500 3200	c.u.r.i.t.y.%.2.
0x1B0	3000 4900 6E00 6600 6F00 7200 6D00 6100	0.I.n.f.o.r.m.a.
0x1C0	7400 6900 6F00 6E00 2500 3200 3000 6100	t.i.o.n.%.2.0.a.
0x1D0	6E00 6400 2500 3200 3000 4500 7600 6500	n.d.%.2.0.E.v.e.
0x1E0	6E00 7400 2500 3200 3000 4D00 6100 6E00	n.t.%.2.0.M.a.n.
0x1F0	6100 6700 6500 6D00 6500 6E00 7400 2F00	a.g.e.m.e.n.t./.
0x200	3100 2E00 3100 2500 3200 3000 5300 4900	1...1.%.2.0.S.I.
0x210	4500 4D00 2D00 6600 6F00 7200 2D00 4200	E.M.-.f.o.r.-.B.
0x220	6500 6700 6900 6E00 6E00 6500 7200 7300	e.g.i.n.n.e.r.s.
0x230	2E00 7000 6400 6600 0000 0000 1300 0000	..p.d.f.........
0x240	0000 0000 0300 0000 0000 0000 4000 0000	............@...
0x250	D032 6FC4 78B7 D801 1300 0000 0100 0000	Ð2oÄx·Ø.........
0x260	1F00 0000 1B00 0000 3100 2E00 3100 2000	........1...1. .
0x270	5300 4900 4500 4D00 2D00 6600 6F00 7200	S.I.E.M.-.f.o.r.
0x280	2D00 4200 6500 6700 6900 6E00 6E00 6500	-.B.e.g.i.n.n.e.
0x290	7200 7300 2E00 7000 6400 6600 0000 0000	r.s...p.d.f.....
0x2A0	4100 0000 0000 0000	A.......

\Users\user_name\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxx\AC\MicrosoftEdge\User\Default\Recovery\(Active|LastActive)

Name	Date modified
{007EC186-236C-11ED-A8CB-ECB1D7545AF8}.dat	8/24/2022 8:17 AM
RecoveryStore.{007EC184-236C-11ED-A8CB-ECB1D7545AF8}.dat	8/24/2022 8:37 AM

IE & Edge Artifacts – Synchronization

- Is Sync enabled?
  - Software\Microsoft\Windows\CurrentVersion\SettingSync\Browsersettings\<Browser>
- Last Time Sync?
  - NTUser.dat\Software\Microsoft\Windows\CurrentVersion\SettingsSync\NameSpace\BrowserSettings\WinInet-Internet-Explorer\LastRoamed
- What is Synced and Where is it stored?
  - Software\Microsoft\InternetExplorer\Capabilities\Roaming
- Tab Sync:
  - %AppData%\Local\Microsoft\InternetExplorer\TabRoaming
    - GUIDs represent devices being synced. One is the local device
      - ✓ MachineInfo.dat: Information about the machine that data belong to.
    - Structured Storage Format (SS)
      - ✓ Structured Storage Viewer by MiTec



IE & Edge Artifacts – Sync Differentiation

- Typed URLs: Unlikely. Maybe the TypedURLsTime Key
- Favorites: Unlikely: Maybe time analysis
- Tabs: Yes: MachineInfo.dat and Tab dat files
- History: Yes:
  - By comparing SyncTime and Access Time (WebCacheV*.dat): More than 5 sec diff means another system.
  - If WebCacheV*{History[ExpiryTime]} ==0

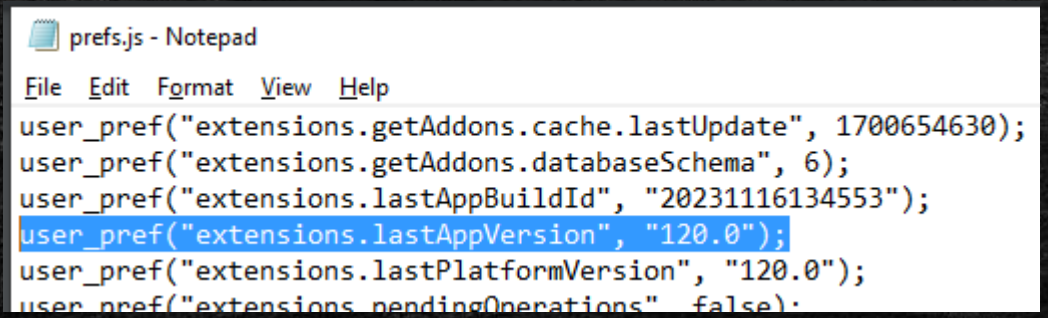
IE & Edge Artifacts – Clear History

- On local system:
  - All entries from WebCacheV*.dat are removed
  - All files in TabRoaming folder are deleted
- On Remote Systems:
  - Tabs belonging to System that conducted the history clear.
- Entries in Remote system WebCacheV*.dat, still persist.

Mozilla Firefox Browser Artifacts

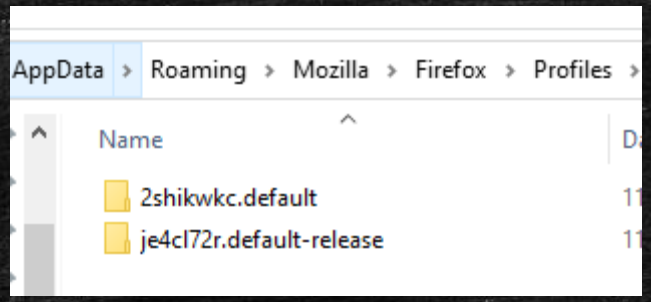
Firefox Artifacts

- Same artifacts
- Preferences: %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<random-text>.default-release\prefs.js
  - Settings
  - Privacy
  - Sync
  - Version



Firefox Artifacts

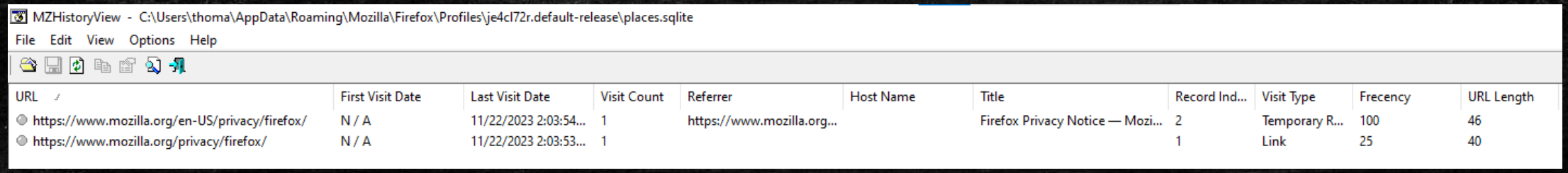
- History, Cookies, Bookmarks, AutoComplete:
  - %AppData%\Roaming\Mozilla\Firefox\Profiles\<randomLetters>.default
- Cache:
  - %AppData%\Local\Mozilla\Firefox\Profiles\<randomLetters>.default\cache2



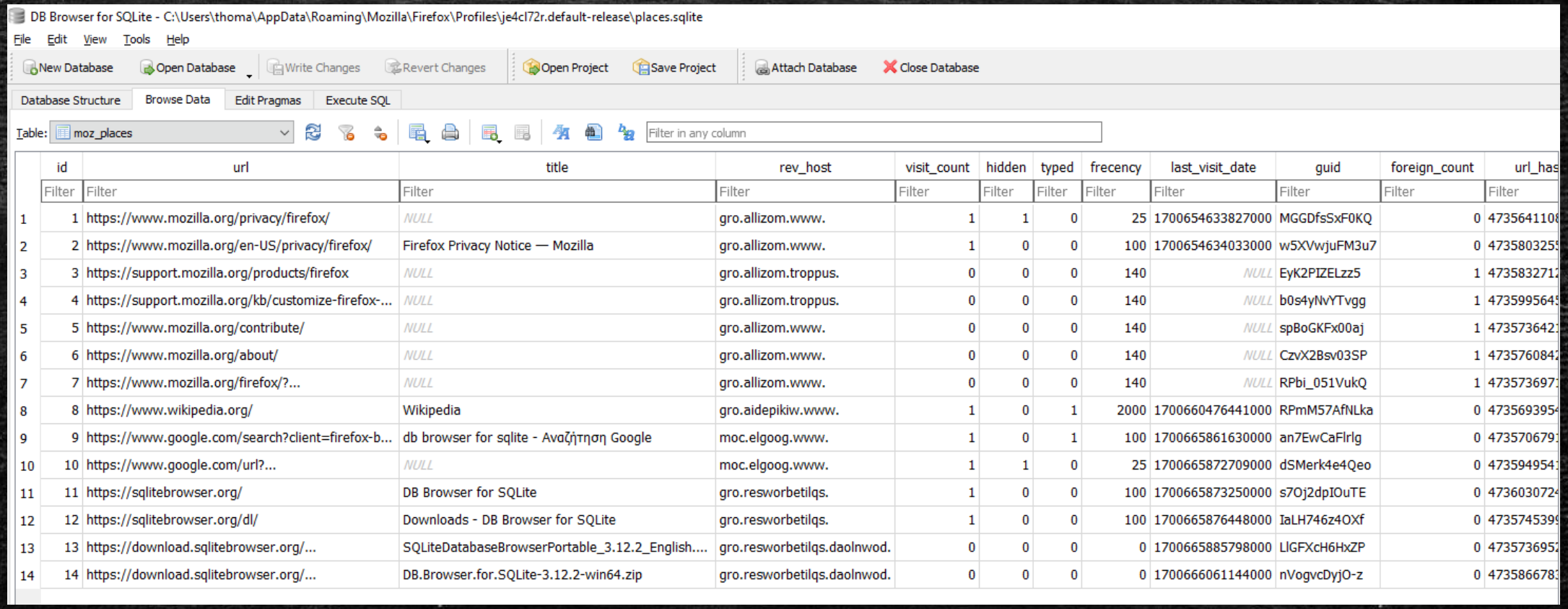
- SQLite Format:
  - places.sqlite: History, Bookmarks, Autocomplete, Downloads
  - formhistory.sqlite: Autocomplete form data
  - cookies.sqlite: Cookies
  - signons.sqlite: Usernames and Passwords
  - webappstore.sqlite: HTML5 Web storage
  - extensions.sqlite: Extension info

Firefox Artifacts - History

- browser.history.expiration.transient_current_max_pages (prefs.js)
- places.sqlite -> DB Browser for SQLite / MZHistoryView.
  - Place_id: same for both tables
  - URL visited: url (moz_places)
  - Title: title (moz_places)
  - First & Last visit: visit_date (moz_historyvisits)
  - Visit count: visit_count (moz_places)
  - If it was typed: typed (moz_places)
  - Page retrieved without any user action: hidden (moz_places)
  - Redirection page: from_visit (moz_historyvisits)
  - How was the page requested: visit_type (moz_historyvisits)



Firefox Artifacts - History



	id	url	title	rev_host	visit_count	hidden	typed	frecency	last_visit_date	guid	foreign_count	url_has
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://www.mozilla.org/privacy/firefox/	NULL	gro.allizom.www.	1	1	0	25	1700654633827000	MGGDfsSxF0KQ	0	4735641108
2	2	https://www.mozilla.org/en-US/privacy/firefox/	Firefox Privacy Notice — Mozilla	gro.allizom.www.	1	0	0	100	1700654634033000	w5XVwjuFM3u7	0	4735803255
3	3	https://support.mozilla.org/products/firefox	NULL	gro.allizom.troppus.	0	0	0	140	NULL	EyK2PIZELzz5	1	4735832712
4	4	https://support.mozilla.org/kb/customize-firefox-...	NULL	gro.allizom.troppus.	0	0	0	140	NULL	b0s4yNvYTvgg	1	4735995645
5	5	https://www.mozilla.org/contribute/	NULL	gro.allizom.www.	0	0	0	140	NULL	spBoGKFx00aj	1	4735736421
6	6	https://www.mozilla.org/about/	NULL	gro.allizom.www.	0	0	0	140	NULL	CzvX2Bsv03SP	1	4735760842
7	7	https://www.mozilla.org/firefox/?...	NULL	gro.allizom.www.	0	0	0	140	NULL	RPbi_051VukQ	1	4735736971
8	8	https://www.wikipedia.org/	Wikipedia	gro.aidepikiw.www.	1	0	1	2000	1700660476441000	RPmM57AfNLka	0	4735693954
9	9	https://www.google.com/search?client=firefox-b...	db browser for sqlite - Αναζήτηση Google	moc.elgoog.www.	1	0	1	100	1700665861630000	an7EwCaFlrlg	0	4735706791
10	10	https://www.google.com/url?...	NULL	moc.elgoog.www.	1	1	0	25	1700665872709000	dSMerk4e4Qeo	0	4735949541
11	11	https://sqlitebrowser.org/	DB Browser for SQLite	gro.resworbetilqs.	1	0	0	100	1700665873250000	s7Oj2dpIOuTE	0	4736030724
12	12	https://sqlitebrowser.org/dl/	Downloads - DB Browser for SQLite	gro.resworbetilqs.	1	0	0	100	1700665876448000	IaLH746z4OXf	0	4735745399
13	13	https://download.sqlitebrowser.org/...	SQLiteDatabaseBrowserPortable_3.12.2_English....	gro.resworbetilqs.daolnwod.	0	0	0	0	1700665885798000	LlGFXcH6HxZP	0	4735736952
14	14	https://download.sqlitebrowser.org/...	DB.Browser.for.SQLite-3.12.2-win64.zip	gro.resworbetilqs.daolnwod.	0	0	0	0	1700666061144000	nVogvcDyjO-z	0	4735866783

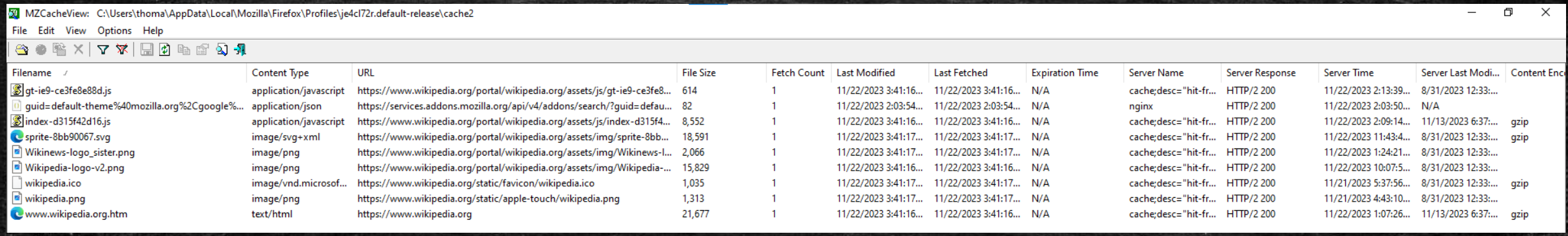
Firefox Artifacts – Visit Types

Id	Visit Type	Description
1	TRANSITION_LINK	The user followed a link and got a new top level window.
2	TRANSITION_TYPED	The user typed the page's URL in the URL bar or selected it from URL bar autocomplete results, clicked on it from a history query (from the History sidebar, History menu, or history query in the personal toolbar or Places organizer.
3	TRANSITION_BOOKMARK	The user followed a bookmark to get to the page.
4	TRANSITION_EMBED	Set when some inner content is loaded. This is true of all images on a page, and the contents of the iframe. It is also true of any content in a frame, regardless of whether or not the user clicked something to get there.
5	TRANSITION_REDIRECT_PERMANENT	The transition was a permanent redirect.
6	TRANSITION_REDIRECT_TEMPORARY	The transition was a temporary redirect.
7	TRANSITION_DOWNLOAD	The transition is a download.
8	TRANSITION_FRAMED_LINK	The user followed a link and got a visit in a frame.
9	TRANSITION_RELOAD	The page has been reloaded.

Firefox Artifacts - Cache

- %USERPROFILE%\AppData\Local\Mozilla\Firefox\Profiles\<randomLetters>.default\cache2
  - URL
  - Fetch Count
  - Missing: If the file referenced by metadata is present on not
  - Filename: Content file of the site
  - Content Type: The type of filed stored in the cache, for example, application/xml
  - File size: Size of the downloaded file
  - Last Modified time
  - Last Fetched Time
  - Response Header
- Files stored individually in /entries
- Tool for Mozilla Cache: MozillaCacheView (Nirsoft)

Firefox Artifacts - Cache



Filename	Content Type	URL	File Size	Fetch Count	Last Modified	Last Fetched	Expiration Time	Server Name	Server Response	Server Time	Server Last Modi...	Content Enc
gt-ie9-ce3fe8e88d.js	application/javascript	https://www.wikipedia.org/portal/wikipedia.org/assets/js/gt-ie9-ce3fe8...	614	1	11/22/2023 3:41:16...	11/22/2023 3:41:16...	N/A	cache;desc="hit-fr...	HTTP/2 200	11/22/2023 2:13:39...	8/31/2023 12:33:...	
guid=default-theme%40mozilla.org%2Cgoogle%...	application/json	https://services.addons.mozilla.org/api/v4/addons/search/?guid=defau...	82	1	11/22/2023 2:03:54...	11/22/2023 2:03:54...	N/A	nginx	HTTP/2 200	11/22/2023 2:03:50...	N/A	
index-d315f42d16.js	application/javascript	https://www.wikipedia.org/portal/wikipedia.org/assets/js/index-d315f4...	8,552	1	11/22/2023 3:41:16...	11/22/2023 3:41:16...	N/A	cache;desc="hit-fr...	HTTP/2 200	11/22/2023 2:09:14...	11/13/2023 6:37:...	gzip
sprite-8bb90067.svg	image/svg+xml	https://www.wikipedia.org/portal/wikipedia.org/assets/img/sprite-8bb...	18,591	1	11/22/2023 3:41:17...	11/22/2023 3:41:17...	N/A	cache;desc="hit-fr...	HTTP/2 200	11/22/2023 11:43:4...	8/31/2023 12:33:...	gzip
Wikinews-logo_sister.png	image/png	https://www.wikipedia.org/portal/wikipedia.org/assets/img/Wikinews-l...	2,066	1	11/22/2023 3:41:17...	11/22/2023 3:41:17...	N/A	cache;desc="hit-fr...	HTTP/2 200	11/22/2023 1:24:21...	8/31/2023 12:33:...	
Wikipedia-logo-v2.png	image/png	https://www.wikipedia.org/portal/wikipedia.org/assets/img/Wikipedia-...	15,829	1	11/22/2023 3:41:16...	11/22/2023 3:41:16...	N/A	cache;desc="hit-fr...	HTTP/2 200	11/22/2023 10:07:5...	8/31/2023 12:33:...	
wikipedia.ico	image/vnd.microsof...	https://www.wikipedia.org/static/favicon/wikipedia.ico	1,035	1	11/22/2023 3:41:17...	11/22/2023 3:41:17...	N/A	cache;desc="hit-fr...	HTTP/2 200	11/21/2023 5:37:56...	8/31/2023 12:33:...	gzip
wikipedia.png	image/png	https://www.wikipedia.org/static/apple-touch/wikipedia.png	1,313	1	11/22/2023 3:41:17...	11/22/2023 3:41:17...	N/A	cache;desc="hit-fr...	HTTP/2 200	11/21/2023 4:43:10...	8/31/2023 12:33:...	
www.wikipedia.org.htm	text/html	https://www.wikipedia.org	21,677	1	11/22/2023 3:41:16...	11/22/2023 3:41:16...	N/A	cache;desc="hit-fr...	HTTP/2 200	11/22/2023 1:07:26...	11/13/2023 6:37:...	gzip

Firefox Artifacts – Cookies & Session Restore

- %AppData%\Roaming\Mozilla\Firefox\Profiles\<randomLetters>.default**cookies.sqlite**
- Tool: MozillaCookiesView (Nirsoft)
  - Host, name, isSecure, value, creationTime, lastAccessed

- Session Restore
  - \AppData\Roaming\Mozilla\Firefox\Profiles\<random-letters>.default-release\sessionstore-backups
    - previous.jsonlz4 (backup from previous session)
    - recovery.jsonlz4 (latest version – runtime)
    - recovery.baklz4 (previous version - runtime)
    - upgrade.jsonlz4 (backup during upgrade)
  - .jsonlz4 -> decompress with dejsonlz4.exe
  - https://codebeautify.org/jsonviewer -> beautify the json

Firefox Artifacts – Session Restore

- Url
- Title
- hasUserInteraction
- lastAccessed
- closedAt

Firefox Artifacts – Extensions

- %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<random-name>.default-release\
- extensions.json (need json beautifier)
- extensions.sqlite, addons.sqlite (Firefox 25-)
- extensions.rdf (Firefox 3-)
  - Name
  - Version
  - SourceURI
  - InstallDate
  - UpdateDate
  - Active

Firefox Artifacts – Download History

- Download folder: prefs.js – Downloads by default
- places.sqlite (Firefox 26+)
- downloads.sqlite (Firefox 3-25)
- Table: moz_annos
  - place_id (refer to moz_places -> place_id) – Filename, source
  - Directory saved (anno_attribute_id 1)
  - endTime (anno_attribute_id 2)
  - fileSize (anno_attribute_id 2)
  - state (anno_attribute_id 2)
- Tools: FirefoxDownloadsView, DCode

id	place_id	anno_attribute_id	content	flags	expiration	type	dateAdded	lastModified
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	13	1	file:///C:/Users/thoma/Downloads/SQLiteDatabaseBrowserPortable_3.12.2_English.paf(1).exe	0	4	3	1700665887877000	1700665887877000
2	13	2	{"state":1,"deleted":false,"endTime":1700665893607,"fileSize":25348656}	0	4	3	1700665893822000	1700665893822000
3	14	1	file:///C:/Users/thoma/Downloads/DB.Browser.for.SQLite-3.12.2-win64.zip	0	4	3	1700666061299000	1700666061299000
4	14	2	{"state":1,"deleted":false,"endTime":1700666067542,"fileSize":20446868}	0	4	3	1700666067587000	1700666067587000

Firefox Artifacts – Synchronization

- Check prefs.js for services.sync.engine.<sync_service> (Account is needed)
- What is synced?
  - Bookmarks, history, passwords, tabs, preferences, add-ons, Form history, some cookies, Downloads (visit_type = 7)
- What is not synced?
  - Download History Details, Most cookies, Web Storage, Cache, WebStore, Favicons
- Indicators of sync in history
  - visit_type = 1 & from_visit_ID=0
  - No Data in description & preview_image_url
  - No entries in favicon.sqlite, webappstore.sqlite, cookies or cache files
  - visit_type=7 and no moz_annos

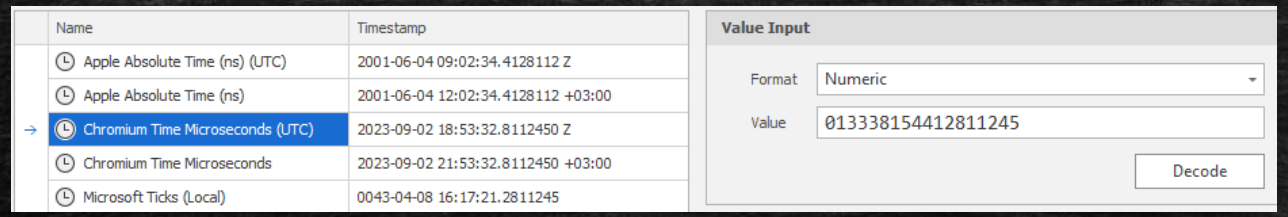
Firefox Artifacts – Synchronization

- On local system:
  - places.sqlite
  - Formhistory.sqlite
  - cookies.sqlite
  - Cache2
  - Sessionstore-backups folder
- On Remote Systems:
  - All existing data & synced data persist.
  - Delete Page & Forget About this Site removes entries in both

Google Chrome Browser Artifacts

Chrome Artifacts

- %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default
- Formats:
  - SQLite (Majority) – WebKit timestamps



  - SELECT datetime((visit_time/1000000),'unixepoch','localtime') FROM visits
  - JSON (preferences, bookmarks, loaded extensions)
  - SNSS (Session restore)

- History: 90 days
  - History, Download History, Autocomplete, Segments
- Top Sites: Most visited pages, populated by Segments

Chrome Artifacts – History

- Tables
  - **Downloads** – path, time, size, mime type
  - **keyword_search_terms**: typed searches
  - **Segments** & **segment_usage**: Most visited sites
  - **visit_source**: source of URL info(local, sync, imported)
    - Sync=0, Browsed=1, Extension=3, Imported=3,4,5
  - **Urls**, **visits**: browser history

```
1  SELECT a.id, a.name, a.url_id, b.segment_id, SUM(b.visit_count)
2  as total_visit_count FROM segments a JOIN segment_usage b
3  ON a.id = b.segment_id
4  GROUP BY name
5  ORDER BY total_visit_count DESC
```

	id	name	url_id	segment_id	total_visit_count
1	31	http://mailer.hndgs.mil.gr/	935	31	47
2	13	http://sdna.gr/	925	13	31
3	9	http://mail.google.com/mail/u/0/	1313	9	26
4	36	http://facebook.com/	11636	36	23
5	10	http://gazzetta.gr/	898	10	23

Chrome Artifacts – History (urls, visits)

- **url** (complete URL visited, with parameters - urls)
- **Title** (Title of the page visited – urls)
- **visit_time** (historical times of the site visited - visits)
- **last_visit_time** (most recent visit - urls)
- **visit_count** (number of visits - urls)
- **typed_count** (user typed - urls)
- **from_visit** (what page led the user to this one - visits)
- **visit_duration** (how long it was viewed - visits)
- **transition** (how was the page requested - visits) – must be decoded
  - Convert to hex - *268435458 (decimal) = 0x10000002*
  - AND the value with oxFF - 0x10000002 AND 0x000000FF = 0x00000002

- Important urls & visits tables must be correlated (urls.id = visits.url)
  - *SELECT * FROM urls JOIN visits on urls.id = visits.url WHERE urls.url LIKE '%wikipedia%*

Chrome Artifacts – History (Transition)

Id	Transition Type	Description
0	link	Clicked a link
1	typed	Typed url
2	auto_Bookmark	Suggestion in Chrome UI (not user favorite)
3	auto_Subframe	Loaded in a top-level-frame (advertisement)
4	manual_subframe	Request to load content in non-top-level-frame
5	generated	Suggested based on user typing but user didn't see URL
6	auto_toplevel	Home page or command line
7	form_Submit	Submitted form
8	reload	Refreshed page
9	keyword	Typed keyword
10	keyword Generated	URL generated from keyword

Chrome Artifacts – Preferences

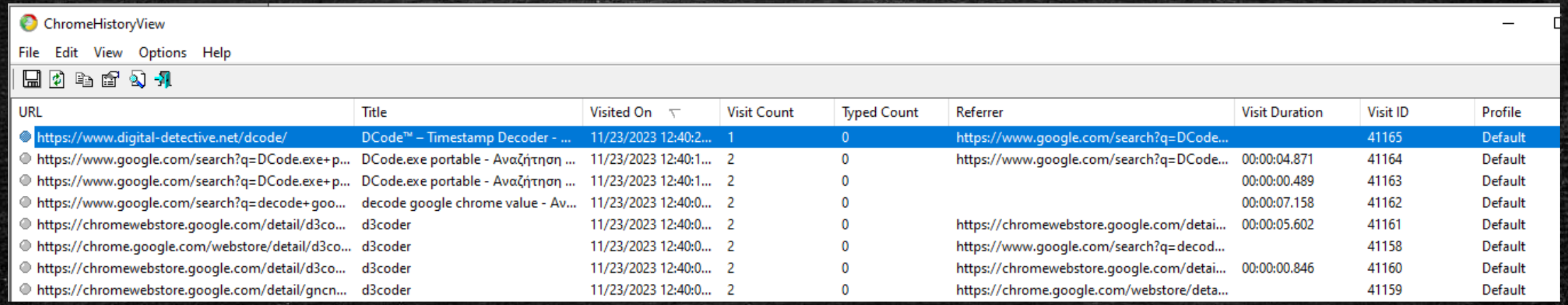
- JSON file in Default folder – needs beautifier
  - **clear_data**: Evidence of objects cleared
  - **network_qualities**: Network names the system connected to
  - **savefile**: Last location that a file was saved
  - **selectfile**: Last location a file was opened
  - **content_settings**: sites visited & settings on this site
  - **per_host_zoom_level**: Sites zoomed by user
    - Not cleared by History Clear
  - **geolocation**: Sites allowed to geolocate the browser
  - **media_engagement**: Media plays on the site
  - **site_engagement**: User engagement with the site resources
  - **sound**: Muted sites by user
  - **account_info**: Google account logged into the browser
  - **signedin_time**: Last time logged in
  - **last_synced_time**: last synced time

Chrome Artifacts – Cache & Cookies

- Cache:
  - %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Cache
  - ChromeCacheView (Nirsoft)

- Cookies:
  - %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Cookies (SQLite)
  - Cookies are encrypted with DPAPI (Windows user authentication) – Live system
  - Tool: Hindsight (gets both cache and cookies)
    - host_key (domain)
    - name
    - value & encrypted_value (contents)
    - creation_utc & last_access_utc (first and last time used)

Chrome Artifacts – Cache & Cookies



URL	Title	Visited On	Visit Count	Typed Count	Referrer	Visit Duration	Visit ID	Profile
https://www.digital-detective.net/dcode/	DCode™ – Timestamp Decoder - ...	11/23/2023 12:40:2...	1	0	https://www.google.com/search?q=DCode...		41165	Default
https://www.google.com/search?q=DCode.exe+p...	DCode.exe portable - Αναζήτηση ...	11/23/2023 12:40:1...	2	0	https://www.google.com/search?q=DCode...	00:00:04.871	41164	Default
https://www.google.com/search?q=DCode.exe+p...	DCode.exe portable - Αναζήτηση ...	11/23/2023 12:40:1...	2	0		00:00:00.489	41163	Default
https://www.google.com/search?q=decode+goo...	decode google chrome value - Av...	11/23/2023 12:40:0...	2	0		00:00:07.158	41162	Default
https://chromewebstore.google.com/detail/d3co...	d3coder	11/23/2023 12:40:0...	2	0	https://chromewebstore.google.com/detai...	00:00:05.602	41161	Default
https://chrome.google.com/webstore/detail/d3co...	d3coder	11/23/2023 12:40:0...	2	0	https://www.google.com/search?q=decod...		41158	Default
https://chromewebstore.google.com/detail/d3co...	d3coder	11/23/2023 12:40:0...	2	0	https://chromewebstore.google.com/detai...	00:00:00.846	41160	Default
https://chromewebstore.google.com/detail/gncn...	d3coder	11/23/2023 12:40:0...	2	0	https://chrome.google.com/webstore/deta...		41159	Default

Chrome Artifacts – Cache & Cookies

Hindsight

Web Artifact Analysis

Hindsight is a free tool for analyzing web artifacts. To get started, select the 'Input Type' below and fill out the 'Input Path' field. Review the plugins and options on the right, and hit the 'Run' button at the bottom.

Inputs

Input Type: Chrome **Profile Path:** C:\Users\thoma\AppData\Local\Google\Chrome\User Data
Cache Path:

Description: Chrome is a free web browser from Google that runs on Windows, macOS, Linux, ChromeOS, iOS, and Android. Each user's web history and configuration information is stored under their user directory, so there may be multiple sets of browser data on the system.

Available Decryption: Windows Mac Linux

Default Locations:

Windows XP:	\[userdir]\Local Settings\Application Data\Google\Chrome\User Data
Vista/7/8/10/11:	\[userdir]\AppData\Local\Google\Chrome\User Data
Linux:	\[userdir]/.config/google-chrome
OSX/macOS:	\[userdir]/Library/Application Support/Google/Chrome/Default
iOS:	\Applications\com.google.chrome.ios\Library\Application Support\Google\Chrome
Android:	/userdata/data/com.android.chrome/app_chrome

Plugin Selector

- Chrome Extension Names [v20210424]
- Generic Timestamp Decoder [v20160907]
- Google Analytics Cookie Parser [v20170130]
- Google Searches [v20160912]
- Load Balancer Cookie Decoder [v20200213]
- Quantcast Cookie Parser [v20160907]
- Query String Parser [v20170225]
- Time Discrepancy Finder [v20170129]

Options Selector

Log Path: hindsight.log
Timezone: Pacific [-8/-7]
Copy files before opening?
Temp Path: hindsight-temp

Run

Results

Hindsight - Web Artifact Analysis

Summary

Input Path: C:\Users\thoma\AppData\Local\Google\Chrome\User Data
Input Type: Chrome
Profile Paths:
- C:\Users\thoma\AppData\Local\Google\Chrome\User Data\Default

Plugin Results

Chrome Extension Names [v20210424]:	- 2 extension URLs parsed -
Generic Timestamp Decoder [v20160907]:	- 0 timestamps parsed -
Google Analytics Cookie Parser [v20170130]:	- 0 cookies parsed -
Google Searches [v20160912]:	- 2171 searches parsed -
Load Balancer Cookie Decoder [v20200213]:	- 0 cookies parsed -
Quantcast Cookie Parser [v20160907]:	- 0 cookies parsed -
Query String Parser [v20170225]:	- 2099 query strings parsed -
Time Discrepancy Finder [v20170129]:	- 0 differences parsed -

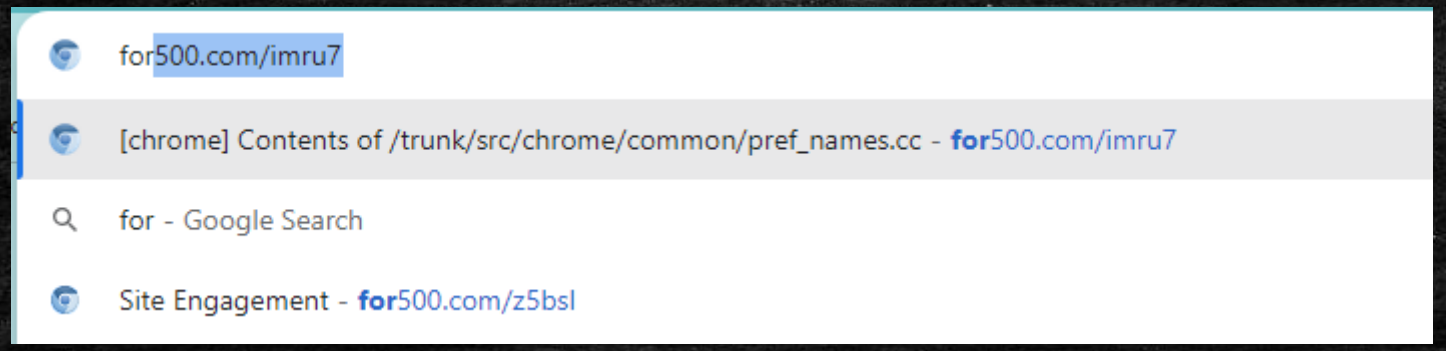
Parsed Artifacts

Detected Chrome version:	111
URL records:	10591
Download records:	222
Cache records:	0
GPU Cache records:	0
Cookie records:	0
Local Storage records:	10642
Bookmark records:	58
Autofill records:	477
Login Data records:	120
Preference Items:	744
Extensions:	7
Extension Cookie records:	0
Session Storage records:	655
Site Characteristics records:	0
File System Items:	7
HSTS records:	58

Save XLSX | Save JSONL | Save SQLite DB
View SQLite DB in Browser
Start New Analysis Session

Chrome Artifacts – AutoComplete

- History
  - ➢ keyword_search_terms table
- WebData
  - ➢ Typed into web forms
- Shortcuts
  - ➢ Typed into omnibox (address bar)
- NetworkActionPredictor
  - ➢ Suggestions in typing to the user & hit success



Chrome Artifacts – Session Recovery

- CurrentSession & Last Session db
- CurrentTabs & LastTabs db
- SNSS format
- Commercial tool to parse it: Axiom
- Free tool: Strings (Sysinternals)

```
SNSS
chrome://newtab/
New Tab
chrome://new-tab-page/
html
about:blank
chrome://new-tab-page/
<!--framePath //<!--frame0-->-->
chrome://new-tab-page
562042ac-5af5-4a1b-a49c-d31361254794
6e0f51b3-46ca-40ff-b714-dde9676ce401
chrome://new-tab-page/
3cdc4695-044f-4ec4-ad87-e94fc907babc
26465d9a-b174-4457-b5e2-4213eab6776c
chrome://new-tab-page/
https://www.google.com/search?q=samparse+v.20120722&oq=samparse+v.20120722&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDEyNThqMGo3q
AIAsAIA&sourceid=chrome&ie=UTF-8&
```

Chrome Artifacts – Synchronization

- chrome://sync-internals/ - Currently synchronized data
- Preferences file as mentioned
- What is synced?
  - History, Bookmarks, Preferences, Extensions, Passwords, WebData(Auto-complete), Top Sites, Tabs
- What is NOT synced?
  - Download history
  - Cookies
  - keyword_search_terms
  - Omnibox typed
  - Network Action Predictor
- Synced URLs in History -> visit_source = 0
- Cannot determine bookmarks, preferences, extensions, Top Sites, auto-complete

Chrome Artifacts – Clear History

- What persists on local system:
  - Some Web Data
  - SyncData maintains all previously synced data
  - Bookmarks
- What persists On Remote Systems:
  - Bookmarks
  - Partially cleared Top Sites
  - Some Web Data
  - Local Download History, Cookies, tabs
  - SyncData maintains all previously synced data

HTML 5 – DOM Artifacts

- Document Object Model – A web Storage with Cookie like information specific for every domain
- Preferences, Keywords, Usernames, Visit tracking, offline files
- Cleared with cookies
- No expiration date
- 10 MB for every domain
- Firefox: Webappstore.sqlite
- IE: %AppData%\Local\Microsoft\Internet Explorer\DOMStore
- Edge: %AppData%\Local\Packages\microsoft.microsoftedge_\AC\ \MicrosoftEdge\User\Default\DOMStore
- Chrome: Individual sqlite for each site

Chrome and Firefox Private Browsing

- What is not saved
  - History
  - Cookies
- Cookies are created as sessions in memory
- Typed URLs & Form Data not saved
- For IE & Edge Cache files and Session Recovery Files are created but deleted (SOFT) at the end of the session (InPrivate Browsing: YES)
  - Can be recovered via file undeletion
  - In case of a crash these files are not deleted at all
- Chrome & Firefox have less artifacts
  - Some local file access, downloaded files & bookmarks still remain
- All data (History, Cookies, Form Data etc) can be recovered from memory and PageFile
- SQLite Databases hold remnants of records, easily recoverable

Thank you for your patience!