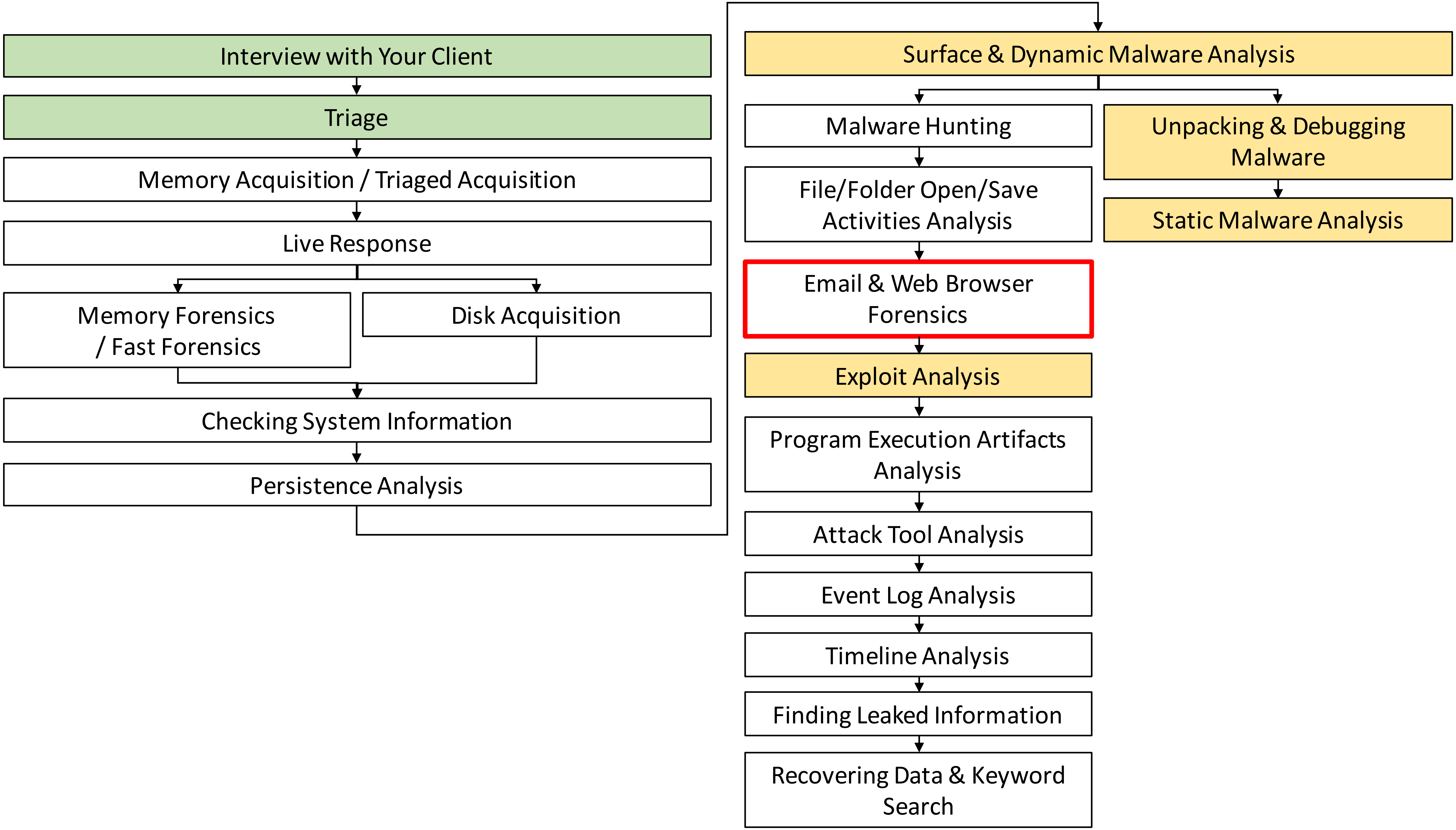
Web Browser Forensics



Interview with Your Client

Triage

Memory Acquisition / Triaged Acquisition

Live Response

Memory Forensics / Fast Forensics

Disk Acquisition

Checking System Information

Persistence Analysis

Surface & Dynamic Malware Analysis

Malware Hunting

Unpacking & Debugging Malware

Static Malware Analysis

File/Folder Open/Save Activities Analysis

Email & Web Browser Forensics

Exploit Analysis

Program Execution Artifacts Analysis

Attack Tool Analysis

Event Log Analysis

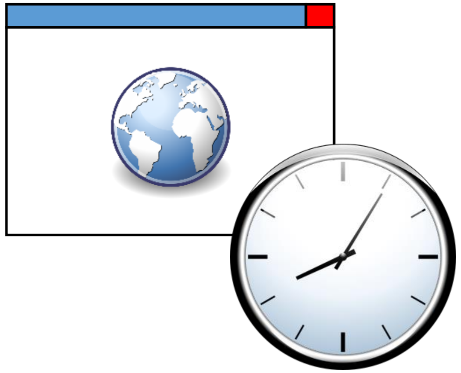
Timeline Analysis

Finding Leaked Information

Recovering Data & Keyword Search

Web Browser Forensics

- When you browse the Internet using the major web browsers, usually they will remain some sort of histories onto the user's profile.
- Histories might provide idea about what the attacker has watched during the attack.
  - Don't forget that the histories could be cleared.



Topics Covered in This Section

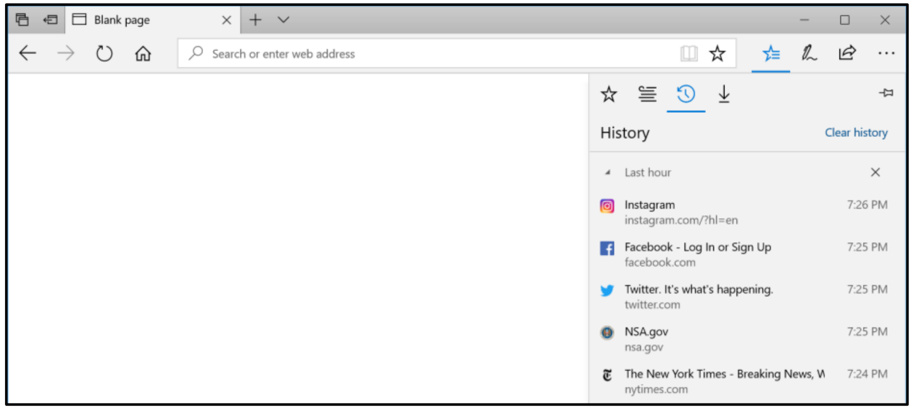
- Artifacts
  - Histories
  - Cache
  - Cookies

- Web Browsers
  - Microsoft Internet Explorer / Edge
  - Mozilla Firefox
  - Google Chrome

Histories

Histories

- When a browser opens a webpage, the visited URLs are recorded to the web browser.
- These histories remain until:
  - The expiration period is reached, or
  - It was cleared by the user.
- Since many applications use Web Browser as their frameworks, some web browser histories that are not a part of web browsing could be found.
  - For example, sometimes histories from the Windows Explorer could be found in the Internet Explorer histories.



Last hour

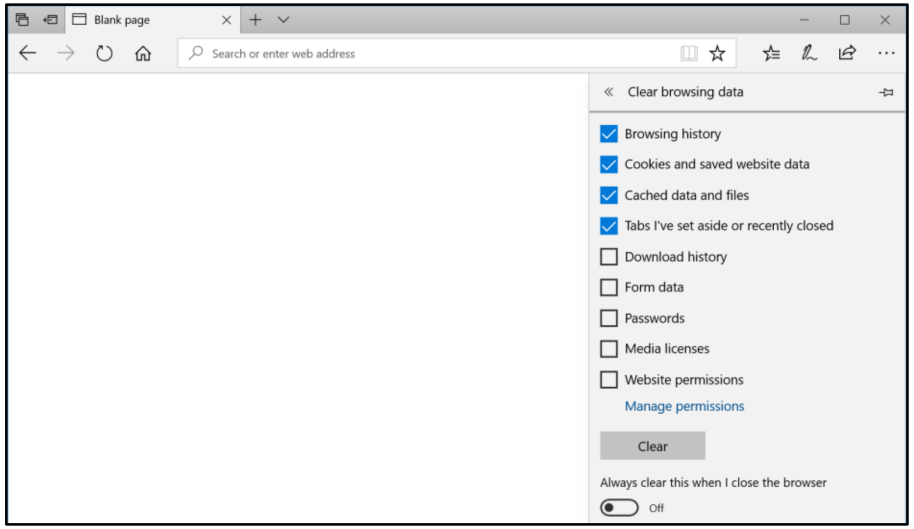
Instagram 7:26 PM
instagram.com/?hl=en

Facebook - Log In or Sign Up 7:25 PM
facebook.com

Twitter. It's what's happening. 7:25 PM
twitter.com

NSA.gov 7:25 PM
nsa.gov

The New York Times - Breaking News, W 7:24 PM
nytimes.com



☑ Browsing history
☑ Cookies and saved website data
☑ Cached data and files
☑ Tabs I've set aside or recently closed
☐ Download history
☐ Form data
☐ Passwords
☐ Media licenses
☐ Website permissions

Always clear this when I close the browser
Off

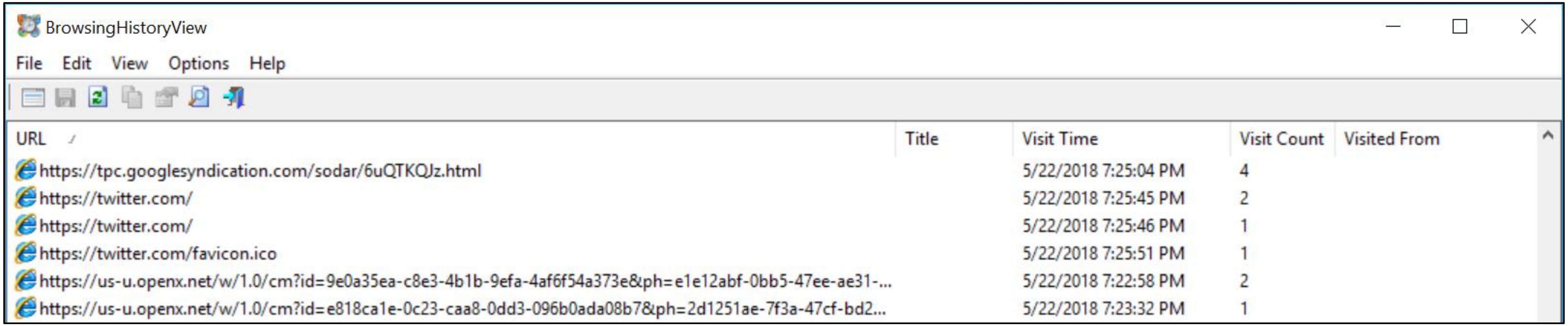
History Locations

- Location, format, and contents of browser histories differ for each browser.
  - Internet Explorer (10 or 11) / Edge:
    %LocalAppData%\Microsoft\Windows\WebCache\WebCacheV01.dat
    - %LocalAppData% is the environment variable for “\Users\<username>\AppData\Local”.
  - Firefox:
    “moz_places” table (SQLite3 format) of
    %AppData%\Mozilla\Firefox\Profiles\<Profile ID>\places.sqlite
  - Chrome:
    It is in SQLite3 format, and kept in “visits” and “urls” tables of
    %Appdata%\Google\Chrome\User Data\Default\History

Exercise: Observation of Histories

Observation of Histories

- Browser history files are in certain format (not a plain text).
    - Using tools is much easier than reading them with binary editors.
- One of the example tools: BrowsingHistoryView by Nirsoft
    - Available for free at: https://www.nirsoft.net/utils/browsing_history_view.html



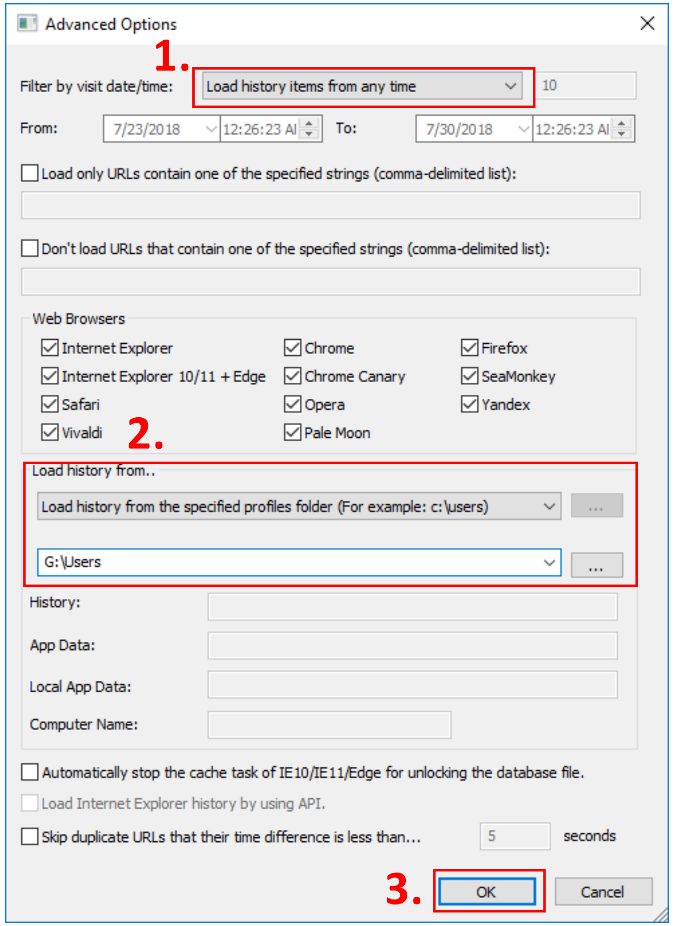
URL	Title	Visit Time	Visit Count	Visited From
https://tpc.googlesyndication.com/sodar/6uQTKQJz.html		5/22/2018 7:25:04 PM	4	
https://twitter.com/		5/22/2018 7:25:45 PM	2	
https://twitter.com/		5/22/2018 7:25:46 PM	1	
https://twitter.com/favicon.ico		5/22/2018 7:25:51 PM	1	
https://us-u.openx.net/w/1.0/cm?id=9e0a35ea-c8e3-4b1b-9efa-4af6f54a373e&ph=e1e12abf-0bb5-47ee-ae31-...		5/22/2018 7:22:58 PM	2	
https://us-u.openx.net/w/1.0/cm?id=e818ca1e-0c23-caa8-0dd3-096b0ada08b7&ph=2d1251ae-7f3a-47cf-bd2...		5/22/2018 7:23:32 PM	1	

Mounting E01 Image

- For this exercise, we will be using **Client-Win10-2_honda.E01** image.
  - Mount it with “**Write temporary**” option enabled.
- Execute “BrowsingHistoryView.exe” **as administrator** from tools folder.
  - Desktop > Shortcuts > 05_RootCauseAnalysis > 0504_InvestigatingWebBrowserActivities > tools > BrowsingHistoryView.exe
  - Right click the shortcut and select “Run as administrator”.

Opening BrowsingHistoryView

- When you open the application, “Advanced Options” dialog is shown.
  1. Select “Load history items from any time” in “Filter by visit date/time” field.
     - You can specify the date/time if you know when the incident happened.
  2. Select “Load history from the specified profiles folder”, and enter “G:\Users” for “Load history from” section.
  3. Press OK when ready.



Filter by visit date/time: Load history items from any time 10

From: 7/23/2018 12:26:23 AI To: 7/30/2018 12:26:23 AI

□ Load only URLs contain one of the specified strings (comma-delimited list):

□ Don't load URLs that contain one of the specified strings (comma-delimited list):

Web Browsers

☑ Internet Explorer
☑ Internet Explorer 10/11 + Edge
☑ Safari
☑ Vivaldi
☑ Chrome
☑ Chrome Canary
☑ Opera
☑ Pale Moon
☑ Firefox
☑ SeaMonkey
☑ Yandex

Load history from..

Load history from the specified profiles folder (For example: c:\users)

G:\Users

History:

App Data:

Local App Data:

Computer Name:

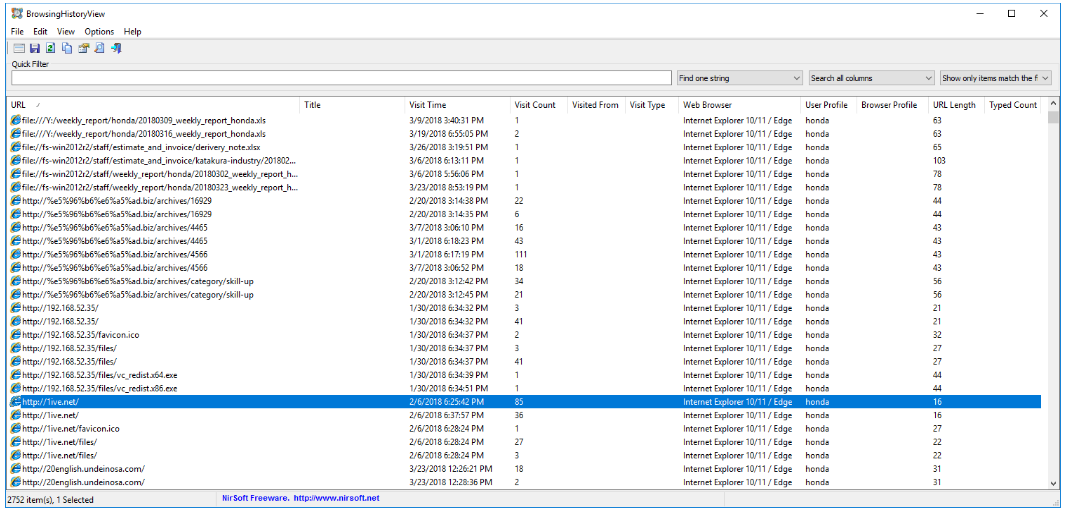
□ Automatically stop the cache task of IE10/IE11/Edge for unlocking the database file.

□ Load Internet Explorer history by using API.

□ Skip duplicate URLs that their time difference is less than... 5 seconds

List of Histories

- You should be able to see the list of web browser histories.
    - If the list is empty, check that:
        - You’ve configured the Advanced Options as instructed. It can be reconfigured from “Options” menu.
        - You’ve executed the application as administrator.
- You can sort by clicking the title row.
    - Sort by **<u>Visit Time</u>** to see them as a timeline.
- You can filter the contents.
  Select “Use Quick Filter” under “View” menu.



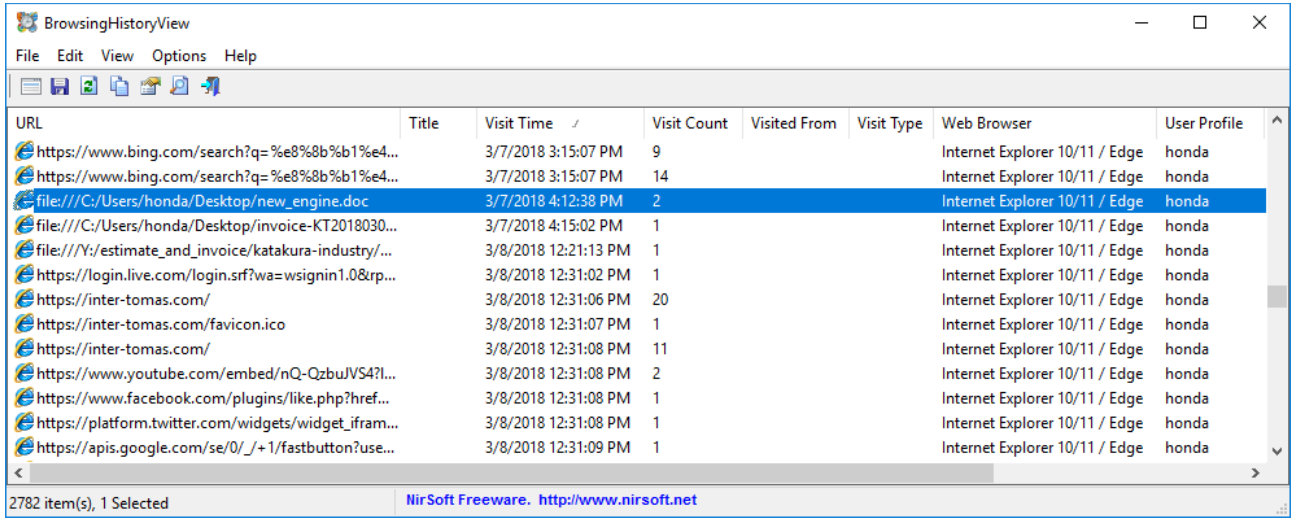
URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Web Browser	User Profile	Browser Profile	URL Length	Typed Count
file:///Y:/weekly_report/honda/20180309_weekly_report_honda.xls		3/9/2018 3:40:31 PM	1			Internet Explorer 10/11 / Edge	honda		63	
file:///Y:/weekly_report/honda/20180316_weekly_report_honda.xls		3/19/2018 6:55:05 PM	2			Internet Explorer 10/11 / Edge	honda		63	
file://fs-win2012r2/staff/estimate_and_invoice/derivery_note.xlsx		3/26/2018 3:19:51 PM	1			Internet Explorer 10/11 / Edge	honda		65	
file://fs-win2012r2/staff/estimate_and_invoice/katakura-industry/201802...		3/6/2018 6:13:11 PM	1			Internet Explorer 10/11 / Edge	honda		103	
file://fs-win2012r2/staff/weekly_report/honda/20180302_weekly_report_h...		3/6/2018 5:56:06 PM	1			Internet Explorer 10/11 / Edge	honda		78	
file://fs-win2012r2/staff/weekly_report/honda/20180323_weekly_report_h...		3/23/2018 8:53:19 PM	1			Internet Explorer 10/11 / Edge	honda		78	
http://%e5%96%b6%e6%a5%ad.biz/archives/16929		2/20/2018 3:14:38 PM	22			Internet Explorer 10/11 / Edge	honda		44	
http://%e5%96%b6%e6%a5%ad.biz/archives/16929		2/20/2018 3:14:35 PM	6			Internet Explorer 10/11 / Edge	honda		44	
http://%e5%96%b6%e6%a5%ad.biz/archives/4465		3/7/2018 3:06:10 PM	16			Internet Explorer 10/11 / Edge	honda		43	
http://%e5%96%b6%e6%a5%ad.biz/archives/4465		3/1/2018 6:18:23 PM	43			Internet Explorer 10/11 / Edge	honda		43	
http://%e5%96%b6%e6%a5%ad.biz/archives/4566		3/1/2018 6:17:19 PM	111			Internet Explorer 10/11 / Edge	honda		43	
http://%e5%96%b6%e6%a5%ad.biz/archives/4566		3/7/2018 3:06:52 PM	18			Internet Explorer 10/11 / Edge	honda		43	
http://%e5%96%b6%e6%a5%ad.biz/archives/category/skill-up		2/20/2018 3:12:42 PM	34			Internet Explorer 10/11 / Edge	honda		56	
http://%e5%96%b6%e6%a5%ad.biz/archives/category/skill-up		2/20/2018 3:12:45 PM	21			Internet Explorer 10/11 / Edge	honda		56	
http://192.168.52.35/		1/30/2018 6:34:32 PM	3			Internet Explorer 10/11 / Edge	honda		21	
http://192.168.52.35/		1/30/2018 6:34:32 PM	41			Internet Explorer 10/11 / Edge	honda		21	
http://192.168.52.35/favicon.ico		1/30/2018 6:34:37 PM	2			Internet Explorer 10/11 / Edge	honda		32	
http://192.168.52.35/files/		1/30/2018 6:34:37 PM	3			Internet Explorer 10/11 / Edge	honda		27	
http://192.168.52.35/files/		1/30/2018 6:34:37 PM	41			Internet Explorer 10/11 / Edge	honda		27	
http://192.168.52.35/files/vc_redist.x64.exe		1/30/2018 6:34:39 PM	1			Internet Explorer 10/11 / Edge	honda		44	
http://192.168.52.35/files/vc_redist.x86.exe		1/30/2018 6:34:51 PM	1			Internet Explorer 10/11 / Edge	honda		44	
http://1ive.net/		2/6/2018 6:25:42 PM	85			Internet Explorer 10/11 / Edge	honda		16	
http://1ive.net/		2/6/2018 6:37:57 PM	36			Internet Explorer 10/11 / Edge	honda		16	
http://1ive.net/favicon.ico		2/6/2018 6:28:24 PM	1			Internet Explorer 10/11 / Edge	honda		27	
http://1ive.net/files/		2/6/2018 6:28:24 PM	27			Internet Explorer 10/11 / Edge	honda		22	
http://1ive.net/files/		2/6/2018 6:28:24 PM	3			Internet Explorer 10/11 / Edge	honda		22	
http://20english.undeinosa.com/		3/23/2018 12:26:21 PM	18			Internet Explorer 10/11 / Edge	honda		31	
http://20english.undeinosa.com/		3/23/2018 12:28:36 PM	2			Internet Explorer 10/11 / Edge	honda		31	

2752 item(s), 1 Selected

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

What You Can Find

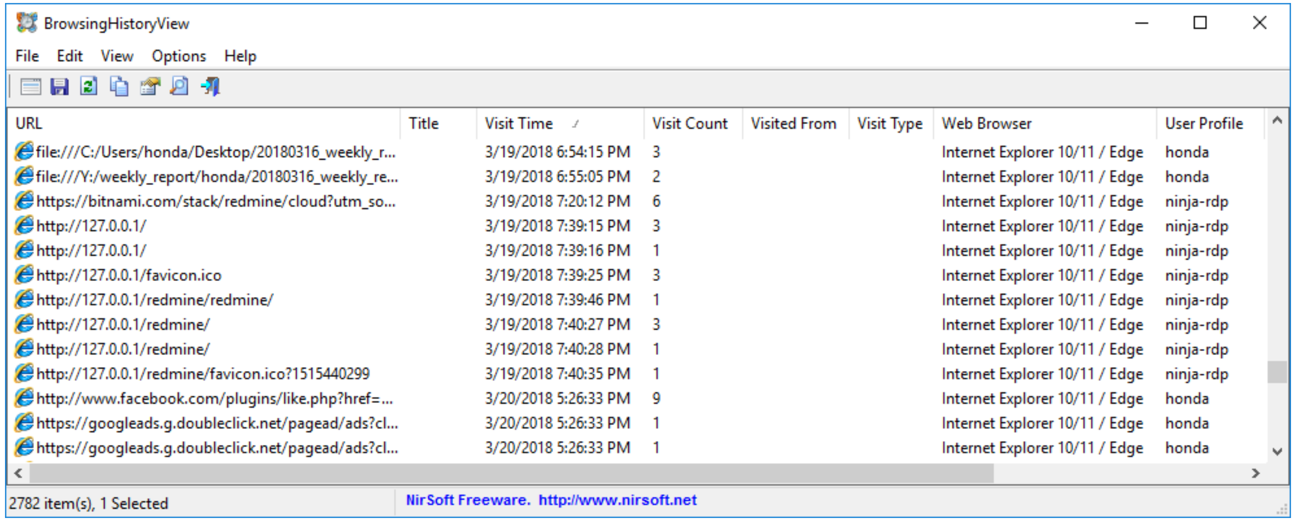
- URLs that starts with “file:///” are files on the local disk or on the network shares.
  - On March 7, 2018 at 4:12PM, user **honda** has opened a file **new_engine.doc** on the user’s **Desktop**.
- You should be able to see histories from users **honda** and **ninja-rdp**.
  - In this network, ninja-rdp is a special account. These special accounts are indicators that should be watched carefully.



URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Web Browser	User Profile
https://www.bing.com/search?q=%e8%8b%b1%e4...		3/7/2018 3:15:07 PM	9			Internet Explorer 10/11 / Edge	honda
https://www.bing.com/search?q=%e8%8b%b1%e4...		3/7/2018 3:15:07 PM	14			Internet Explorer 10/11 / Edge	honda
file:///C:/Users/honda/Desktop/new_engine.doc		3/7/2018 4:12:38 PM	2			Internet Explorer 10/11 / Edge	honda
file:///C:/Users/honda/Desktop/invoice-KT2018030...		3/7/2018 4:15:02 PM	1			Internet Explorer 10/11 / Edge	honda
file:///Y:/estimate_and_invoice/katakura-industry/...		3/8/2018 12:21:13 PM	1			Internet Explorer 10/11 / Edge	honda
https://login.live.com/login.srf?wa=wsignin1.0&rp...		3/8/2018 12:31:02 PM	1			Internet Explorer 10/11 / Edge	honda
https://inter-tomas.com/		3/8/2018 12:31:06 PM	20			Internet Explorer 10/11 / Edge	honda
https://inter-tomas.com/favicon.ico		3/8/2018 12:31:07 PM	1			Internet Explorer 10/11 / Edge	honda
https://inter-tomas.com/		3/8/2018 12:31:08 PM	11			Internet Explorer 10/11 / Edge	honda
https://www.youtube.com/embed/nQ-QzbuJVS4?l...		3/8/2018 12:31:08 PM	2			Internet Explorer 10/11 / Edge	honda
https://www.facebook.com/plugins/like.php?href...		3/8/2018 12:31:08 PM	1			Internet Explorer 10/11 / Edge	honda
https://platform.twitter.com/widgets/widget_ifram...		3/8/2018 12:31:08 PM	1			Internet Explorer 10/11 / Edge	honda
https://apis.google.com/se/0/_/+1/fastbutton?use...		3/8/2018 12:31:09 PM	1			Internet Explorer 10/11 / Edge	honda

2782 item(s), 1 Selected

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



URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Web Browser	User Profile
file:///C:/Users/honda/Desktop/20180316_weekly_r...		3/19/2018 6:54:15 PM	3			Internet Explorer 10/11 / Edge	honda
file:///Y:/weekly_report/honda/20180316_weekly_re...		3/19/2018 6:55:05 PM	2			Internet Explorer 10/11 / Edge	honda
https://bitnami.com/stack/redmine/cloud?utm_so...		3/19/2018 7:20:12 PM	6			Internet Explorer 10/11 / Edge	ninja-rdp
http://127.0.0.1/		3/19/2018 7:39:15 PM	3			Internet Explorer 10/11 / Edge	ninja-rdp
http://127.0.0.1/		3/19/2018 7:39:16 PM	1			Internet Explorer 10/11 / Edge	ninja-rdp
http://127.0.0.1/favicon.ico		3/19/2018 7:39:25 PM	3			Internet Explorer 10/11 / Edge	ninja-rdp
http://127.0.0.1/redmine/redmine/		3/19/2018 7:39:46 PM	1			Internet Explorer 10/11 / Edge	ninja-rdp
http://127.0.0.1/redmine/		3/19/2018 7:40:27 PM	3			Internet Explorer 10/11 / Edge	ninja-rdp
http://127.0.0.1/redmine/		3/19/2018 7:40:28 PM	1			Internet Explorer 10/11 / Edge	ninja-rdp
http://127.0.0.1/redmine/favicon.ico?1515440299		3/19/2018 7:40:35 PM	1			Internet Explorer 10/11 / Edge	ninja-rdp
http://www.facebook.com/plugins/like.php?href=...		3/20/2018 5:26:33 PM	9			Internet Explorer 10/11 / Edge	honda
https://googleads.g.doubleclick.net/pagead/ads?cl...		3/20/2018 5:26:33 PM	1			Internet Explorer 10/11 / Edge	honda
https://googleads.g.doubleclick.net/pagead/ads?cl...		3/20/2018 5:26:33 PM	1			Internet Explorer 10/11 / Edge	honda

2782 item(s), 1 Selected

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

Announcement

- When you browse through the application, you will find accesses to “1ive.net” and “out1ook.net” on February 6, 2018.
- The incident took place in March, and these events have nothing to do with the scenario.
  - They were recorded during our preparation process.

Cookies

Cookies

- Cookies can be considered as a source of web browsing history records
  - Each cookie has the following records that can help us indicating the web sites visited and building a timeline:
    - Domain of the web sites
    - Timestamp of web site access, and creation/modification timestamp of the cookie
    - Other cookie contents, which might have additional information

Cookie Locations

- Location, format, and contents of cookies differ for each browser.
  - Internet Explorer (10 or 11 on Windows 8 or later) / Edge (on Windows 10 up to 1703): **%LocalAppData%\Microsoft\Windows\INetCookies**
    - Individual text file for each cookie
  - Edge (on Windows 10 1709 or later): **%LocalAppData%\Microsoft\Windows\WebCache\WebCacheV01.dat**
    - Same file as History, in ESE database format.
  - Firefox: **%AppData%\Mozilla\Firefox\Profiles\<Profile ID>\cookies.sqlite**
    - Single file in SQLite3 format
  - Chrome: **%LocalAppData%\Google\Chrome\User Data\Default\Cookies**
    - Single file in SQLite3 format

Parsing Cookies

- Each browser has a method to show the cookie contents.
- To view cookie contents outside of the web browsers, the tools may be used.
  - “tools” folder on your Analysis Machine has the following tools from Nirsoft:
    - ChromeCookiesView
    - FlashCookiesView
    - IECookiesView
    - MozillaCookiesView

Cache

Cache

- Cache is another contents that may contain the web browser access histories.
- Even when the history records were cleared, there may be some chance of cache files remaining on the disk.

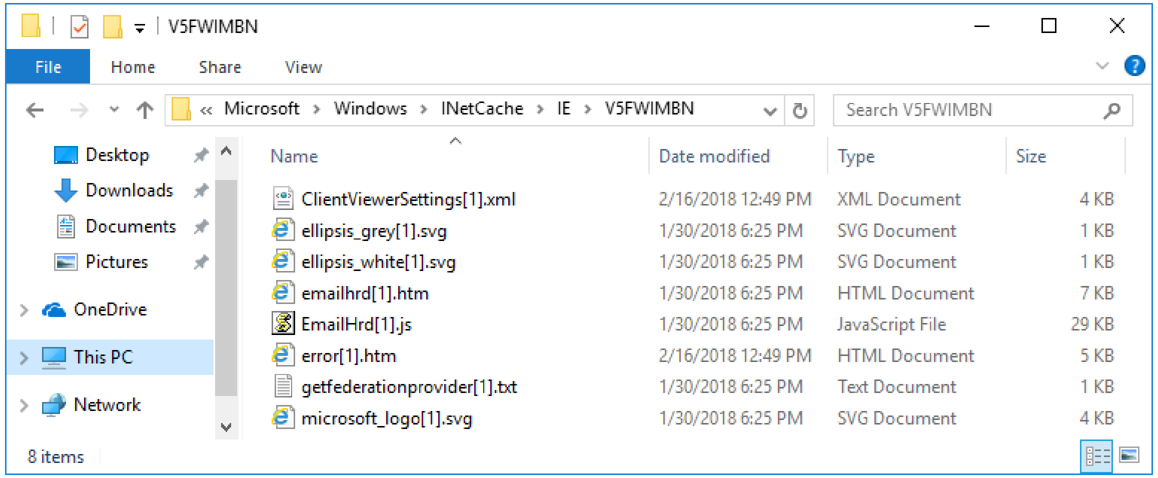
Cache Locations

- Location, format and management form of cache differs for each browser.
  - Internet Explorer (10 or 11) / Edge:
    - **%LocalAppData%\Microsoft\Windows\WebCache\WebCacheV01.dat**
    - It is in ESE database format.
  - Firefox:
    - **%LocalAppData%\Mozilla\Firefox\Profiles\<Profile Name>\CacheX**
    - The last character “X” is a number such as “2”.
    - Although their file names are in Firefox internal IDs, they are files that were downloaded from the websites.
  - Chrome:
    - **%LocalAppData%\Google\Chrome\User Data\Default\Cache**
    - Although they are named “f_” + numbers, they are files that were downloaded from the websites.

Exercise:
Observation of Cache

Observation of Cache

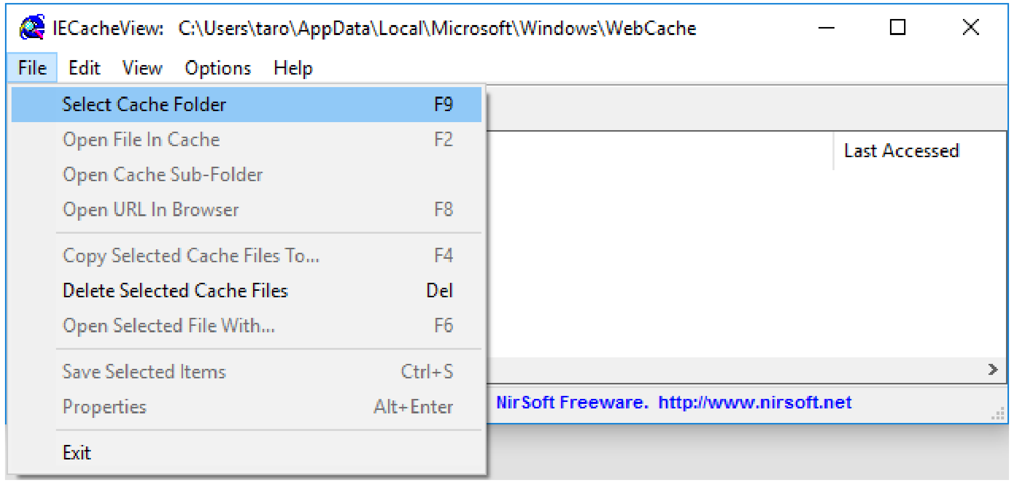
- Cache files are in different format for each browser.
- For Internet Explorer/Edge, cache files are actually the original files.
  - It is possible to directly open them on the Windows Explorer and see their contents.
  - On the other hand, the files are not organized by URLs, so it is difficult to figure out the right file for each URL.
- We will use a tool to observe them.



Name	Date modified	Type	Size
ClientViewerSettings[1].xml	2/16/2018 12:49 PM	XML Document	4 KB
ellipsis_grey[1].svg	1/30/2018 6:25 PM	SVG Document	1 KB
ellipsis_white[1].svg	1/30/2018 6:25 PM	SVG Document	1 KB
emailhrd[1].htm	1/30/2018 6:25 PM	HTML Document	7 KB
EmailHrd[1].js	1/30/2018 6:25 PM	JavaScript File	29 KB
error[1].htm	2/16/2018 12:49 PM	HTML Document	5 KB
getfederationprovider[1].txt	1/30/2018 6:25 PM	Text Document	1 KB
microsoft_logo[1].svg	1/30/2018 6:25 PM	SVG Document	4 KB

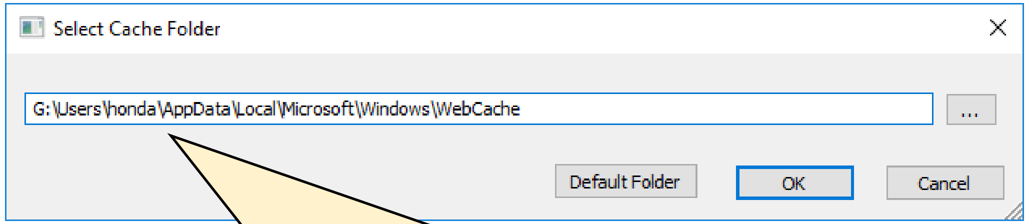
Opening IECacheView

- From the “tools” folder, launch “IECacheView.exe” **as administrator**.
  - It is another tool by NirSoft that shows Internet Explorer/Edge cache contents.
- Once opened, navigate to “Select Cache Folder” under “File” menu.
- Specify path to the honda’s cache folder.
  - Change the preceding “C” to “G”
  - Change “taro” to “honda”
  - Press OK when ready.



IECacheView: C:\Users\taro\AppData\Local\Microsoft\Windows\WebCache

File
Edit
View
Options
Help
Select Cache Folder F9
Open File In Cache F2
Open Cache Sub-Folder
Open URL In Browser F8
Copy Selected Cache Files To... F4
Delete Selected Cache Files Del
Open Selected File With... F6
Save Selected Items Ctrl+S
Properties Alt+Enter
Exit
Last Accessed
NirSoft Freeware. http://www.nirsoft.net



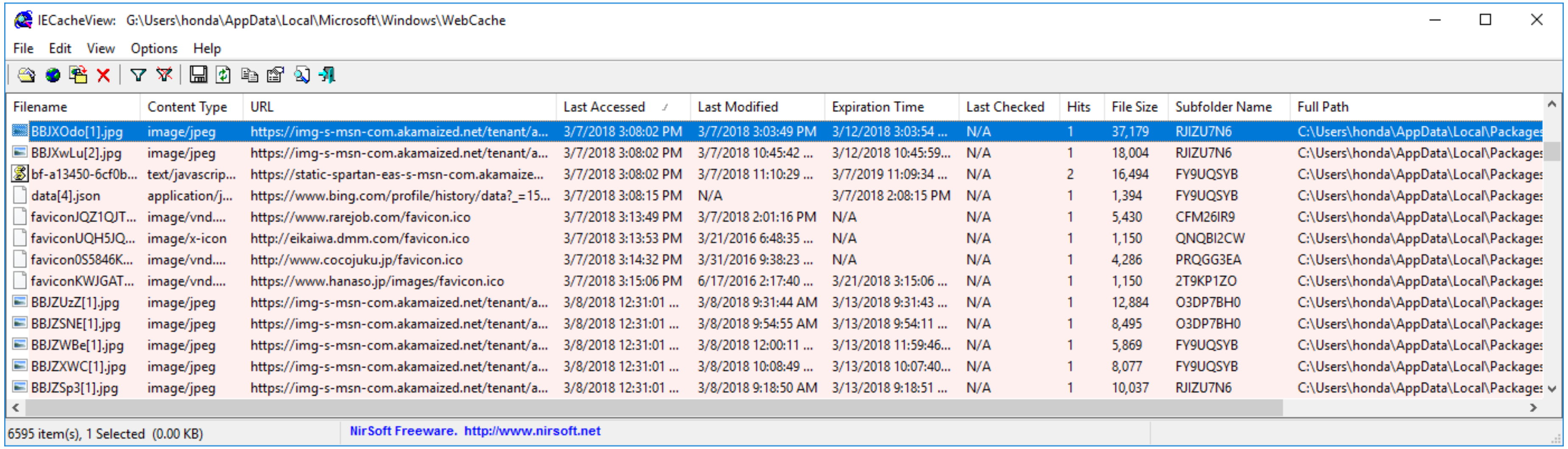
Select Cache Folder

G:\Users\honda\AppData\Local\Microsoft\Windows\WebCache

G:\Users\honda\AppData\Local
\Microsoft\Windows\WebCache

Looking into Cache

- You should be able to see the list of cache files.
  - All files are considered as “Missing” since the drive is mounted as **<u>G</u>**, not C.
  - If you modify the path to drive **<u>G</u>** and open the path, the files do exist.
- Sort by “**<u>Last Accessed</u>**” column to explore it as a timeline.
- You can search the list by pressing “Find” button on the toolbar, or selecting it from “Edit” menu.



IECacheView: G:\Users\honda\AppData\Local\Microsoft\Windows\WebCache
File
Edit
View
Options
Help

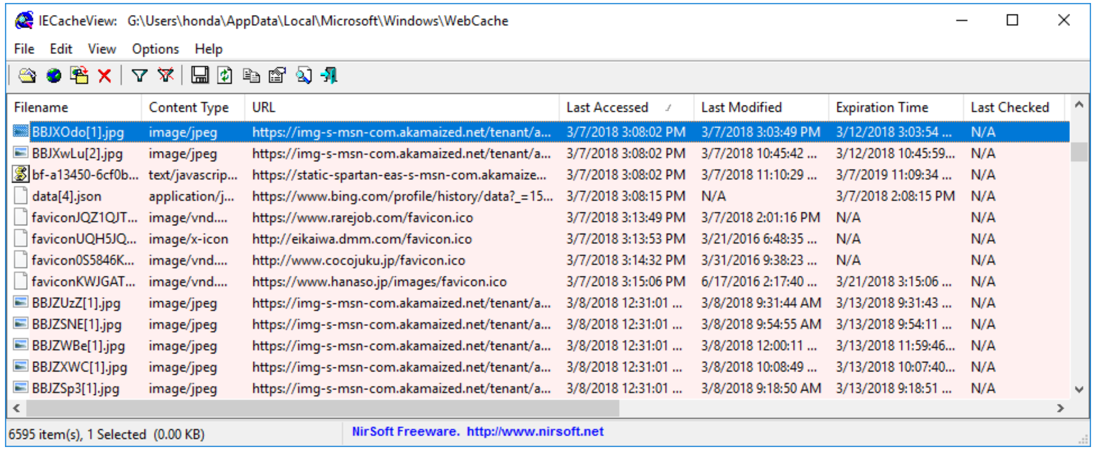
Filename	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hits	File Size	Subfolder Name	Full Path
BBJXOdo[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/7/2018 3:08:02 PM	3/7/2018 3:03:49 PM	3/12/2018 3:03:54 ...	N/A	1	37,179	RJIZU7N6	C:\Users\honda\AppData\Local\Packages
BBJXwLu[2].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/7/2018 3:08:02 PM	3/7/2018 10:45:42 ...	3/12/2018 10:45:59...	N/A	1	18,004	RJIZU7N6	C:\Users\honda\AppData\Local\Packages
bf-a13450-6cf0b...	text/javascrip...	https://static-spartan-eas-s-msn-com.akamaize...	3/7/2018 3:08:02 PM	3/7/2018 11:10:29 ...	3/7/2019 11:09:34 ...	N/A	2	16,494	FY9UQSYB	C:\Users\honda\AppData\Local\Packages
data[4].json	application/j...	https://www.bing.com/profile/history/data?_=15...	3/7/2018 3:08:15 PM	N/A	3/7/2018 2:08:15 PM	N/A	1	1,394	FY9UQSYB	C:\Users\honda\AppData\Local\Packages
faviconJQZ1QJT...	image/vnd....	https://www.rarejob.com/favicon.ico	3/7/2018 3:13:49 PM	3/7/2018 2:01:16 PM	N/A	N/A	1	5,430	CFM26IR9	C:\Users\honda\AppData\Local\Packages
faviconUQH5JQ...	image/x-icon	http://eikaiwa.dmm.com/favicon.ico	3/7/2018 3:13:53 PM	3/21/2016 6:48:35 ...	N/A	N/A	1	1,150	QNQBI2CW	C:\Users\honda\AppData\Local\Packages
favicon0S5846K...	image/vnd....	http://www.cocojuku.jp/favicon.ico	3/7/2018 3:14:32 PM	3/31/2016 9:38:23 ...	N/A	N/A	1	4,286	PRQGG3EA	C:\Users\honda\AppData\Local\Packages
faviconKWJGAT...	image/vnd....	https://www.hanaso.jp/images/favicon.ico	3/7/2018 3:15:06 PM	6/17/2016 2:17:40 ...	3/21/2018 3:15:06 ...	N/A	1	1,150	2T9KP1ZO	C:\Users\honda\AppData\Local\Packages
BBJZUzZ[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/8/2018 12:31:01 ...	3/8/2018 9:31:44 AM	3/13/2018 9:31:43 ...	N/A	1	12,884	O3DP7BH0	C:\Users\honda\AppData\Local\Packages
BBJZSNE[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/8/2018 12:31:01 ...	3/8/2018 9:54:55 AM	3/13/2018 9:54:11 ...	N/A	1	8,495	O3DP7BH0	C:\Users\honda\AppData\Local\Packages
BBJZWBe[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/8/2018 12:31:01 ...	3/8/2018 12:00:11 ...	3/13/2018 11:59:46...	N/A	1	5,869	FY9UQSYB	C:\Users\honda\AppData\Local\Packages
BBJZXWC[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/8/2018 12:31:01 ...	3/8/2018 10:08:49 ...	3/13/2018 10:07:40...	N/A	1	8,077	FY9UQSYB	C:\Users\honda\AppData\Local\Packages
BBJZSp3[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/8/2018 12:31:01 ...	3/8/2018 9:18:50 AM	3/13/2018 9:18:51 ...	N/A	1	10,037	RJIZU7N6	C:\Users\honda\AppData\Local\Packages

6595 item(s), 1 Selected (0.00 KB)

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

What You Can Find

- When we explored the browser histories, we were able to see the access to **<u>new_engine.doc</u>**.
- We **<u>cannot</u>** find the access to new_engine.doc in the browser cache.
  - Since the file was a local file, it appeared in the history, but it was not cached.
- Cache may not be perfect for finding access histories, but still useful when:
  - Histories were removed
  - Files are remaining in the history store.

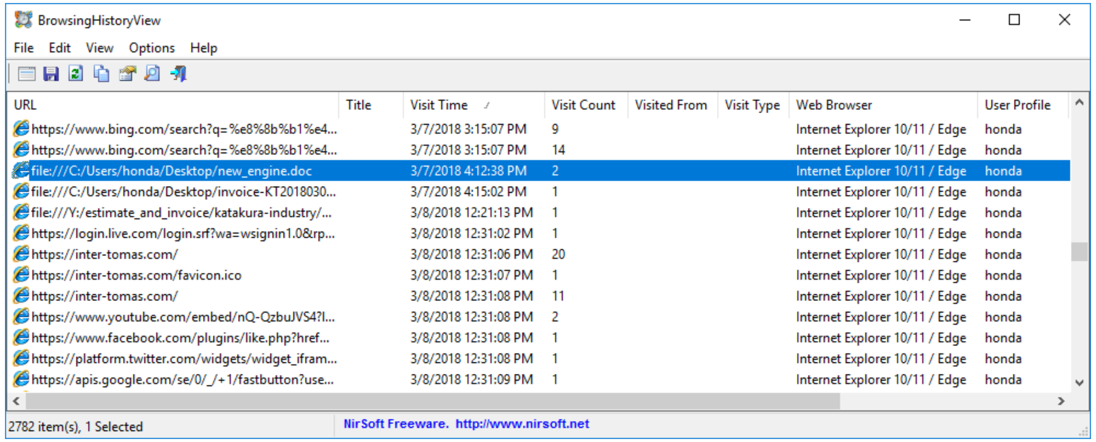


IECacheView: G:\Users\honda\AppData\Local\Microsoft\Windows\WebCache
File
Edit
View
Options
Help

Filename	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked
BBJXOdo[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/7/2018 3:08:02 PM	3/7/2018 3:03:49 PM	3/12/2018 3:03:54 ...	N/A
BBJXwLu[2].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/7/2018 3:08:02 PM	3/7/2018 10:45:42 ...	3/12/2018 10:45:59...	N/A
bf-a13450-6cf0b...	text/javascrip...	https://static-spartan-eas-s-msn-com.akamaize...	3/7/2018 3:08:02 PM	3/7/2018 11:10:29 ...	3/7/2019 11:09:34 ...	N/A
data[4].json	application/j...	https://www.bing.com/profile/history/data?_=15...	3/7/2018 3:08:15 PM	N/A	3/7/2018 2:08:15 PM	N/A
faviconJQZ1QJT...	image/vnd....	https://www.rarejob.com/favicon.ico	3/7/2018 3:13:49 PM	3/7/2018 2:01:16 PM	N/A	N/A
faviconUQH5JQ...	image/x-icon	http://eikaiwa.dmm.com/favicon.ico	3/7/2018 3:13:53 PM	3/21/2016 6:48:35 ...	N/A	N/A
favicon0S5846K...	image/vnd....	http://www.cocojuku.jp/favicon.ico	3/7/2018 3:14:32 PM	3/31/2016 9:38:23 ...	N/A	N/A
faviconKWJGAT...	image/vnd....	https://www.hanaso.jp/images/favicon.ico	3/7/2018 3:15:06 PM	6/17/2016 2:17:40 ...	3/21/2018 3:15:06 ...	N/A
BBJZUzZ[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/8/2018 12:31:01 ...	3/8/2018 9:31:44 AM	3/13/2018 9:31:43 ...	N/A
BBJZSNE[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/8/2018 12:31:01 ...	3/8/2018 9:54:55 AM	3/13/2018 9:54:11 ...	N/A
BBJZWBe[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/8/2018 12:31:01 ...	3/8/2018 12:00:11 ...	3/13/2018 11:59:46...	N/A
BBJZXWC[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/8/2018 12:31:01 ...	3/8/2018 10:08:49 ...	3/13/2018 10:07:40...	N/A
BBJZSp3[1].jpg	image/jpeg	https://img-s-msn-com.akamaized.net/tenant/a...	3/8/2018 12:31:01 ...	3/8/2018 9:18:50 AM	3/13/2018 9:18:51 ...	N/A

6595 item(s), 1 Selected (0.00 KB)

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



URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Web Browser	User Profile
https://www.bing.com/search?q=%e8%8b%b1%e4...		3/7/2018 3:15:07 PM	9			Internet Explorer 10/11 / Edge	honda
https://www.bing.com/search?q=%e8%8b%b1%e4...		3/7/2018 3:15:07 PM	14			Internet Explorer 10/11 / Edge	honda
file:///C:/Users/honda/Desktop/new_engine.doc		3/7/2018 4:12:38 PM	2			Internet Explorer 10/11 / Edge	honda
file:///C:/Users/honda/Desktop/invoice-KT2018030...		3/7/2018 4:15:02 PM	1			Internet Explorer 10/11 / Edge	honda
file:///Y:/estimate_and_invoice/katakura-industry/...		3/8/2018 12:21:13 PM	1			Internet Explorer 10/11 / Edge	honda
https://login.live.com/login.srf?wa=wsignin1.0&rp...		3/8/2018 12:31:02 PM	1			Internet Explorer 10/11 / Edge	honda
https://inter-tomas.com/		3/8/2018 12:31:06 PM	20			Internet Explorer 10/11 / Edge	honda
https://inter-tomas.com/favicon.ico		3/8/2018 12:31:07 PM	1			Internet Explorer 10/11 / Edge	honda
https://inter-tomas.com/		3/8/2018 12:31:08 PM	11			Internet Explorer 10/11 / Edge	honda
https://www.youtube.com/embed/nQ-QzbuJVS4?l...		3/8/2018 12:31:08 PM	2			Internet Explorer 10/11 / Edge	honda
https://www.facebook.com/plugins/like.php?href...		3/8/2018 12:31:08 PM	1			Internet Explorer 10/11 / Edge	honda
https://platform.twitter.com/widgets/widget_ifram...		3/8/2018 12:31:08 PM	1			Internet Explorer 10/11 / Edge	honda
https://apis.google.com/se/0/_/+1/fastbutton?use...		3/8/2018 12:31:09 PM	1			Internet Explorer 10/11 / Edge	honda

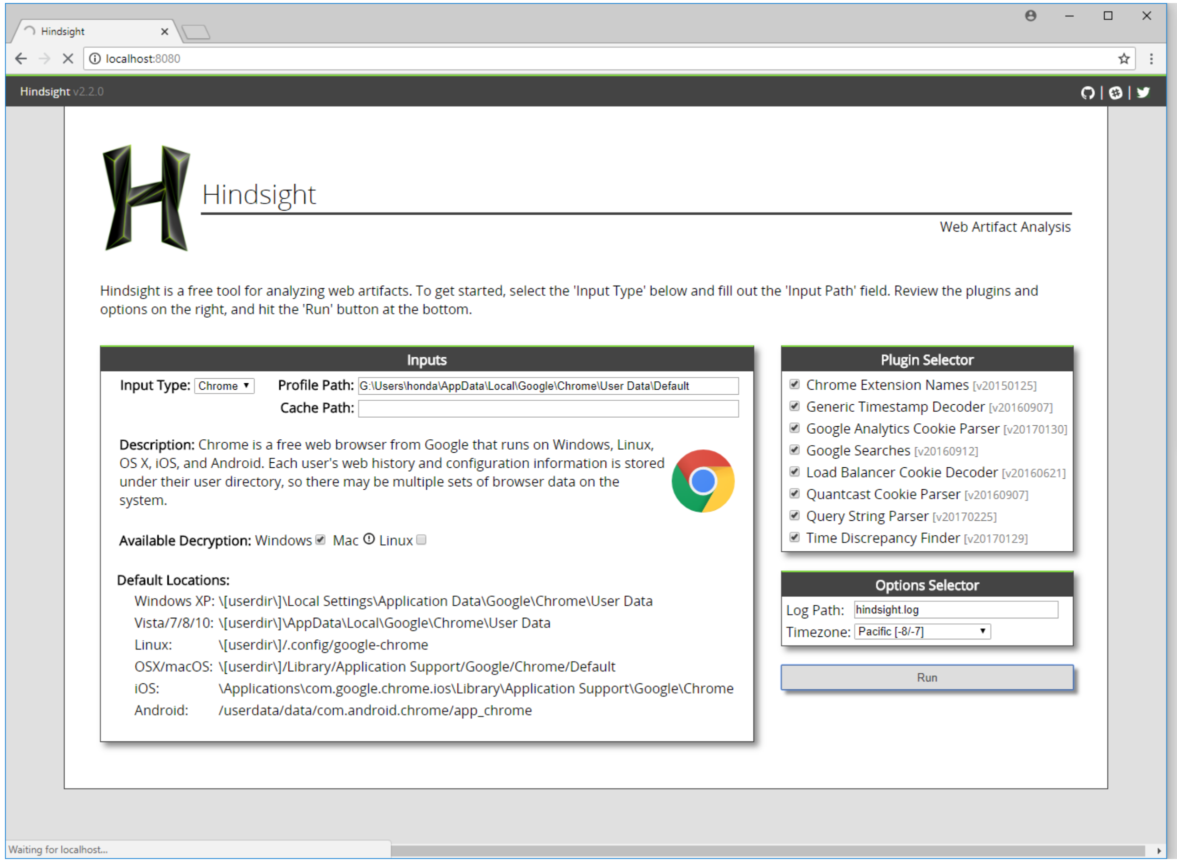
2782 item(s), 1 Selected

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

Quick Overview of Some Other Tools

Hindsight (1/2)

- A tool aimed to analyze Chrome and Brave browsers.



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: G:\Users\honda\AppData\Local\Google\Chrome\User Data\Default

Cache Path:

Description: Chrome is a free web browser from Google that runs on Windows, Linux, OS X, 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: \[userdir\]\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
```

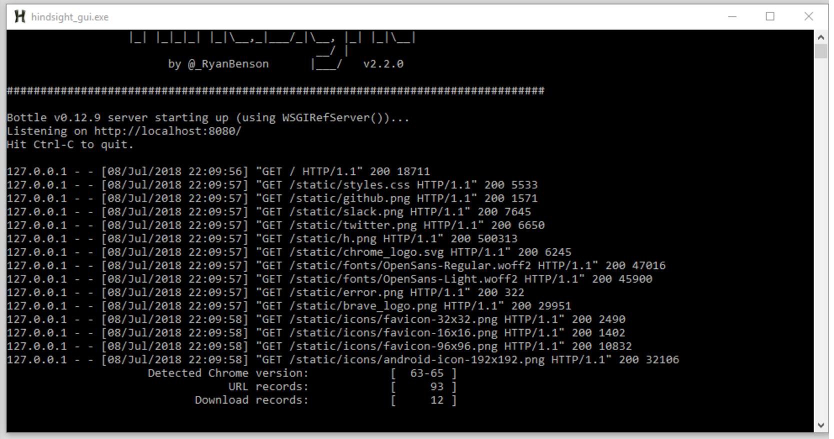
Plugin Selector

- ☑ Chrome Extension Names [v20150125]
- ☑ Generic Timestamp Decoder [v20160907]
- ☑ Google Analytics Cookie Parser [v20170130]
- ☑ Google Searches [v20160912]
- ☑ Load Balancer Cookie Decoder [v20160621]
- ☑ Quantcast Cookie Parser [v20160907]
- ☑ Query String Parser [v20170225]
- ☑ Time Discrepancy Finder [v20170129]

Options Selector

Log Path: hindsight.log

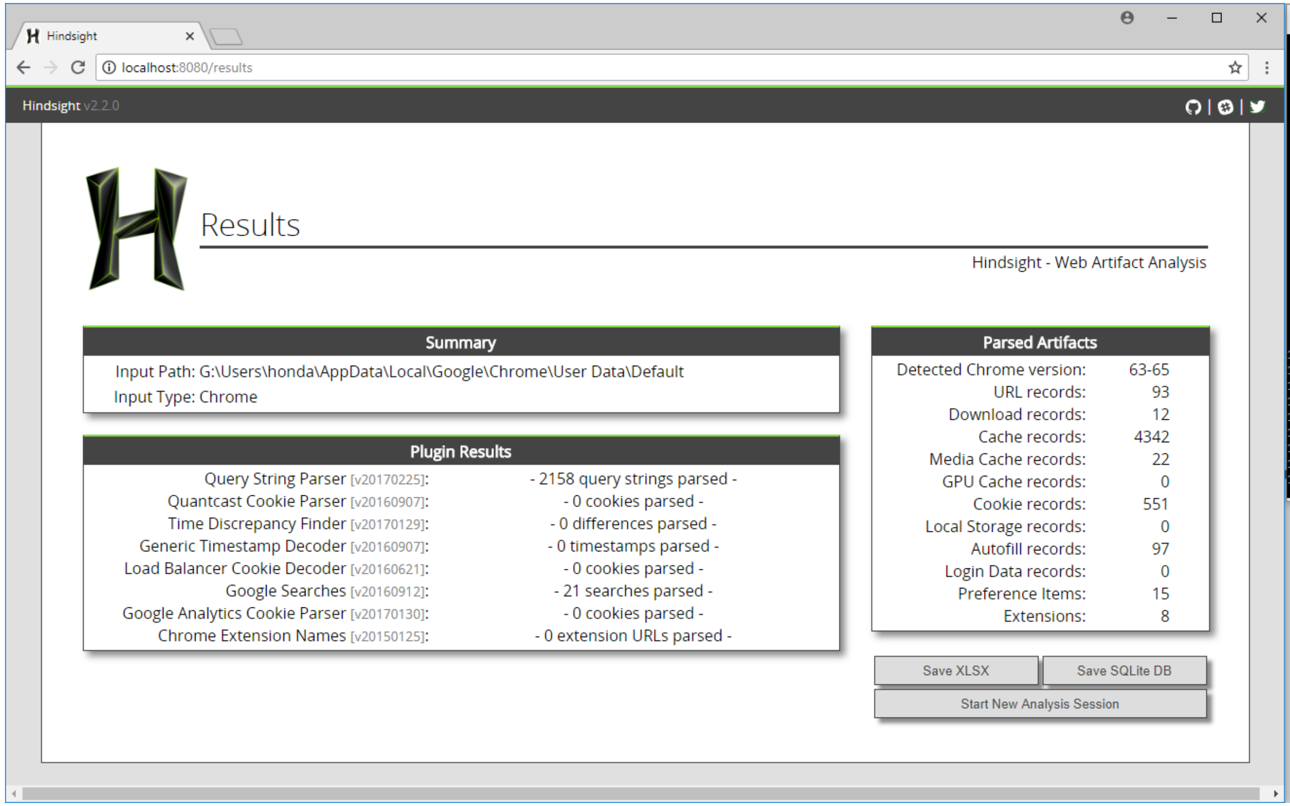
Timezone: Pacific [-8/-7] ▾



```
              |_| |_|_|_| |_|\__,_|___/_|\__, |_| |_|\__|
                                          __/ |
                   by @_RyanBenson       |___/   v2.2.0

################################################################################

Bottle v0.12.9 server starting up (using WSGIRefServer())...
Listening on http://localhost:8080/
Hit Ctrl-C to quit.

127.0.0.1 - - [08/Jul/2018 22:09:56] "GET / HTTP/1.1" 200 18711
127.0.0.1 - - [08/Jul/2018 22:09:57] "GET /static/styles.css HTTP/1.1" 200 5533
127.0.0.1 - - [08/Jul/2018 22:09:57] "GET /static/github.png HTTP/1.1" 200 1571
127.0.0.1 - - [08/Jul/2018 22:09:57] "GET /static/slack.png HTTP/1.1" 200 7645
127.0.0.1 - - [08/Jul/2018 22:09:57] "GET /static/twitter.png HTTP/1.1" 200 6650
127.0.0.1 - - [08/Jul/2018 22:09:57] "GET /static/h.png HTTP/1.1" 200 500313
127.0.0.1 - - [08/Jul/2018 22:09:57] "GET /static/chrome_logo.svg HTTP/1.1" 200 6245
127.0.0.1 - - [08/Jul/2018 22:09:57] "GET /static/fonts/OpenSans-Regular.woff2 HTTP/1.1" 200 47016
127.0.0.1 - - [08/Jul/2018 22:09:57] "GET /static/fonts/OpenSans-Light.woff2 HTTP/1.1" 200 45900
127.0.0.1 - - [08/Jul/2018 22:09:57] "GET /static/error.png HTTP/1.1" 200 322
127.0.0.1 - - [08/Jul/2018 22:09:57] "GET /static/brave_logo.png HTTP/1.1" 200 29951
127.0.0.1 - - [08/Jul/2018 22:09:58] "GET /static/icons/favicon-32x32.png HTTP/1.1" 200 2490
127.0.0.1 - - [08/Jul/2018 22:09:58] "GET /static/icons/favicon-16x16.png HTTP/1.1" 200 1402
127.0.0.1 - - [08/Jul/2018 22:09:58] "GET /static/icons/favicon-96x96.png HTTP/1.1" 200 10832
127.0.0.1 - - [08/Jul/2018 22:09:58] "GET /static/icons/android-icon-192x192.png HTTP/1.1" 200 32106
                     Detected Chrome version:            [  63-65 ]
                                 URL records:            [     93 ]
                            Download records:            [     12 ]
```

Hindsight (2/2)

- Outputs and details are shown after the analysis is done.



Results

Hindsight - Web Artifact Analysis

Summary

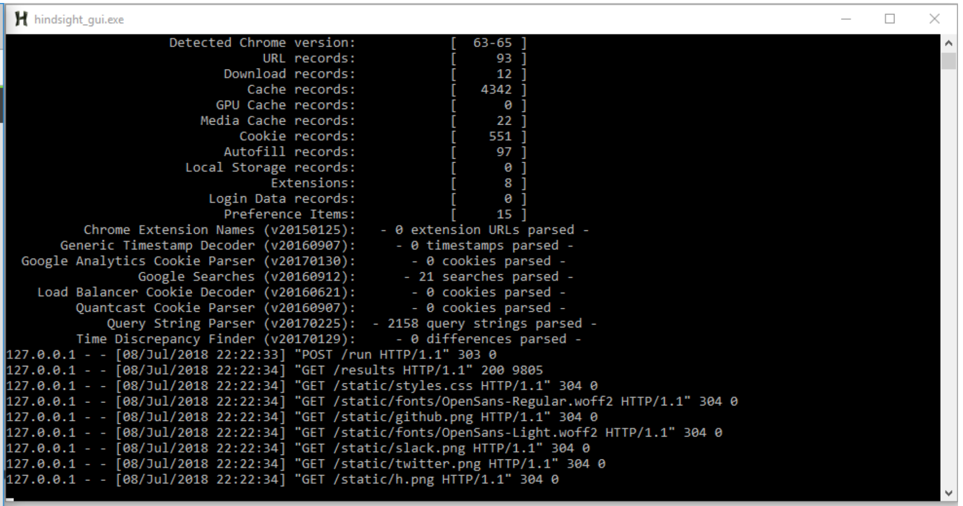
Input Path: G:\Users\honda\AppData\Local\Google\Chrome\User Data\Default
Input Type: Chrome

Plugin Results

Query String Parser [v20170225]:	- 2158 query strings parsed -
Quantcast Cookie Parser [v20160907]:	- 0 cookies parsed -
Time Discrepancy Finder [v20170129]:	- 0 differences parsed -
Generic Timestamp Decoder [v20160907]:	- 0 timestamps parsed -
Load Balancer Cookie Decoder [v20160621]:	- 0 cookies parsed -
Google Searches [v20160912]:	- 21 searches parsed -
Google Analytics Cookie Parser [v20170130]:	- 0 cookies parsed -
Chrome Extension Names [v20150125]:	- 0 extension URLs parsed -

Parsed Artifacts

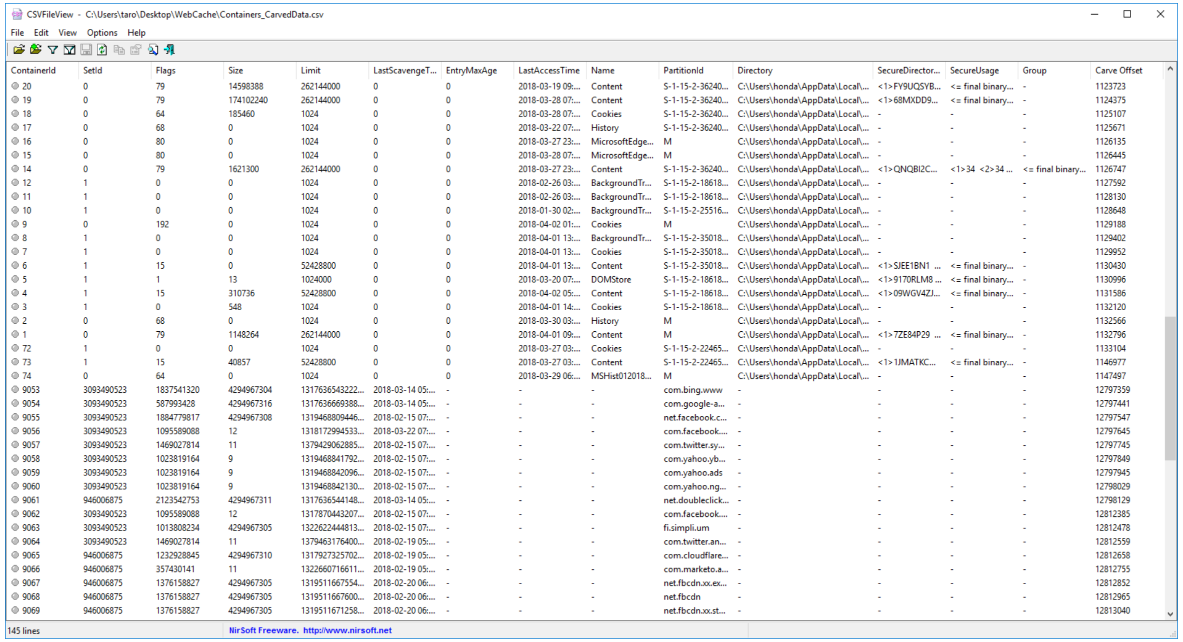
Detected Chrome version:	63-65
URL records:	93
Download records:	12
Cache records:	4342
Media Cache records:	22
GPU Cache records:	0
Cookie records:	551
Local Storage records:	0
Autofill records:	97
Login Data records:	0
Preference Items:	15
Extensions:	8



```
                 Detected Chrome version:            [  63-65 ]
                             URL records:            [     93 ]
                        Download records:            [     12 ]
                           Cache records:            [   4342 ]
                       GPU Cache records:            [      0 ]
                     Media Cache records:            [     22 ]
                          Cookie records:            [    551 ]
                        Autofill records:            [     97 ]
                   Local Storage records:            [      0 ]
                              Extensions:            [      8 ]
                      Login Data records:            [      0 ]
                        Preference Items:            [     15 ]
       Chrome Extension Names (v20150125):   - 0 extension URLs parsed -
    Generic Timestamp Decoder (v20160907):     - 0 timestamps parsed -
 Google Analytics Cookie Parser (v20170130):      - 0 cookies parsed -
              Google Searches (v20160912):     - 21 searches parsed -
  Load Balancer Cookie Decoder (v20160621):      - 0 cookies parsed -
       Quantcast Cookie Parser (v20160907):      - 0 cookies parsed -
          Query String Parser (v20170225):  - 2158 query strings parsed -
       Time Discrepancy Finder (v20170129):     - 0 differences parsed -
127.0.0.1 - - [08/Jul/2018 22:22:33] "POST /run HTTP/1.1" 303 0
127.0.0.1 - - [08/Jul/2018 22:22:34] "GET /results HTTP/1.1" 200 9805
127.0.0.1 - - [08/Jul/2018 22:22:34] "GET /static/styles.css HTTP/1.1" 304 0
127.0.0.1 - - [08/Jul/2018 22:22:34] "GET /static/fonts/OpenSans-Regular.woff2 HTTP/1.1" 304 0
127.0.0.1 - - [08/Jul/2018 22:22:34] "GET /static/github.png HTTP/1.1" 304 0
127.0.0.1 - - [08/Jul/2018 22:22:34] "GET /static/fonts/OpenSans-Light.woff2 HTTP/1.1" 304 0
127.0.0.1 - - [08/Jul/2018 22:22:34] "GET /static/slack.png HTTP/1.1" 304 0
127.0.0.1 - - [08/Jul/2018 22:22:34] "GET /static/twitter.png HTTP/1.1" 304 0
127.0.0.1 - - [08/Jul/2018 22:22:34] "GET /static/h.png HTTP/1.1" 304 0
```

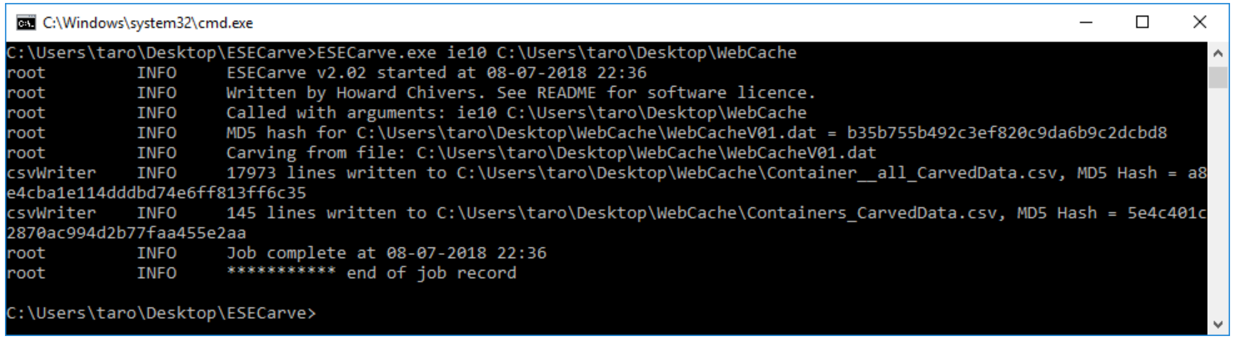
ESECarve

- ESE is a database format used to store histories.
  - It is also used in Windows Search.
  - Copy the artifacts to other work folder; the tool will output the results to the same path as the inputs.
- Contents of the ESE database may be carved in some cases.
- The tool is **not** publicly available.
  - We are introducing this for your information.


CSVFileView - C:\Users\taro\Desktop\WebCache\Containers_CarvedData.csv
File Edit View Options Help

ContainerId	SetId	Flags	Size	Limit	LastScavengeT...	EntryMaxAge	LastAccessTime	Name	PartitionId	Directory	SecureDirector...	SecureUsage	Group	Carve Offset
20	0	79	14598388	262144000	0	0	2018-03-19 09:...	Content	S-1-15-2-36240...	C:\Users\honda\AppData\Local\...	<1>FY9UQSYB...	<= final binary...	-	1123723
19	0	79	174102240	262144000	0	0	2018-03-28 07:...	Content	S-1-15-2-36240...	C:\Users\honda\AppData\Local\...	<1>68MXDD9...	<= final binary...	-	1124375
18	0	64	185460	1024	0	0	2018-03-28 07:...	Cookies	S-1-15-2-36240...	C:\Users\honda\AppData\Local\...	-	-	-	1125107
17	0	68	0	1024	0	0	2018-03-22 07:...	History	S-1-15-2-36240...	C:\Users\honda\AppData\Local\...	-	-	-	1125671
16	0	80	0	1024	0	0	2018-03-27 23:...	MicrosoftEdge...	M	C:\Users\honda\AppData\Local\...	-	-	-	1126135
15	0	80	0	1024	0	0	2018-03-28 07:...	MicrosoftEdge...	M	C:\Users\honda\AppData\Local\...	-	-	-	1126445
14	0	79	1621300	262144000	0	0	2018-03-27 23:...	Content	S-1-15-2-36240...	C:\Users\honda\AppData\Local\...	<1>QNQBI2C...	<1>34 <2>34 ...	<= final binary...	1126747
12	1	0	0	1024	0	0	2018-02-26 03:...	BackgroundTr...	S-1-15-2-18618...	C:\Users\honda\AppData\Local\...	-	-	-	1127592
11	1	0	0	1024	0	0	2018-02-26 03:...	BackgroundTr...	S-1-15-2-18618...	C:\Users\honda\AppData\Local\...	-	-	-	1128130
10	1	0	0	1024	0	0	2018-01-30 02:...	BackgroundTr...	S-1-15-2-25516...	C:\Users\honda\AppData\Local\...	-	-	-	1128648
9	0	192	0	1024	0	0	2018-04-02 01:...	Cookies	M	C:\Users\honda\AppData\Local\...	-	-	-	1129188
8	1	0	0	1024	0	0	2018-04-01 13:...	BackgroundTr...	S-1-15-2-35018...	C:\Users\honda\AppData\Local\...	-	-	-	1129402
7	1	0	0	1024	0	0	2018-04-01 13:...	Cookies	S-1-15-2-35018...	C:\Users\honda\AppData\Local\...	-	-	-	1129952
6	1	15	0	52428800	0	0	2018-04-01 13:...	Content	S-1-15-2-35018...	C:\Users\honda\AppData\Local\...	<1>SJEE1BN1 ...	<= final binary...	-	1130430
5	1	1	13	1024000	0	0	2018-03-20 07:...	DOMStore	S-1-15-2-18618...	C:\Users\honda\AppData\Local\...	<1>9170RLM8 ...	<= final binary...	-	1130996
4	1	15	310736	52428800	0	0	2018-04-02 05:...	Content	S-1-15-2-18618...	C:\Users\honda\AppData\Local\...	<1>09WGV4ZJ...	<= final binary...	-	1131586
3	1	0	548	1024	0	0	2018-04-01 14:...	Cookies	S-1-15-2-18618...	C:\Users\honda\AppData\Local\...	-	-	-	1132120
2	0	68	0	1024	0	0	2018-03-30 03:...	History	M	C:\Users\honda\AppData\Local\...	-	-	-	1132566
1	0	79	1148264	262144000	0	0	2018-04-01 09:...	Content	M	C:\Users\honda\AppData\Local\...	<1>7ZE84P29 ...	<= final binary...	-	1132796
72	1	0	0	1024	0	0	2018-03-27 03:...	Cookies	S-1-15-2-22465...	C:\Users\honda\AppData\Local\...	-	-	-	1133104
73	1	15	40857	52428800	0	0	2018-03-27 03:...	Content	S-1-15-2-22465...	C:\Users\honda\AppData\Local\...	<1>1JMATKC...	<= final binary...	-	1146977
74	0	64	0	1024	0	0	2018-03-29 06:...	MSHist012018...	M	C:\Users\honda\AppData\Local\...	-	-	-	1147497
9053	3093490523	1837541320	4294967304	1317636543222...	2018-03-14 05:...	-	-	-	com.bing.www	-	-	-	-	12797359
9054	3093490523	587993428	4294967316	1317636669388...	2018-03-14 05:...	-	-	-	com.google-a...	-	-	-	-	12797441
9055	3093490523	1884779817	4294967308	1319468809446...	2018-02-15 07:...	-	-	-	net.facebook.c...	-	-	-	-	12797547
9056	3093490523	1095589088	12	1318172994533...	2018-03-22 07:...	-	-	-	com.facebook....	-	-	-	-	12797645
9057	3093490523	1469027814	11	1379429062885...	2018-02-15 07:...	-	-	-	com.twitter.sy...	-	-	-	-	12797745
9058	3093490523	1023819164	9	1319468841792...	2018-02-15 07:...	-	-	-	com.yahoo.yb...	-	-	-	-	12797849
9059	3093490523	1023819164	9	1319468842096...	2018-02-15 07:...	-	-	-	com.yahoo.ads	-	-	-	-	12797945
9060	3093490523	1023819164	9	1319468842130...	2018-02-15 07:...	-	-	-	com.yahoo.ng...	-	-	-	-	12798029
9061	946006875	2123542753	4294967311	1317636544148...	2018-03-14 05:...	-	-	-	net.doubleclick...	-	-	-	-	12798129
9062	3093490523	1095589088	12	1317870443207...	2018-02-15 07:...	-	-	-	com.facebook....	-	-	-	-	12812385
9063	3093490523	1013808234	4294967305	1322622444813...	2018-02-15 07:...	-	-	-	fi.simpli.um	-	-	-	-	12812478
9064	3093490523	1469027814	11	1379463176400...	2018-02-19 05:...	-	-	-	com.twitter.an...	-	-	-	-	12812559
9065	946006875	1232928845	4294967310	1317927325702...	2018-02-19 05:...	-	-	-	com.cloudflare...	-	-	-	-	12812658
9066	946006875	357430141	11	1322660716611...	2018-02-19 05:...	-	-	-	com.marketo.a...	-	-	-	-	12812755
9067	946006875	1376158827	4294967305	1319511667554...	2018-02-20 06:...	-	-	-	net.fbcdn.xx.ex...	-	-	-	-	12812852
9068	946006875	1376158827	4294967305	1319511667600...	2018-02-20 06:...	-	-	-	net.fbcdn	-	-	-	-	12812965
9069	946006875	1376158827	4294967305	1319511671258...	2018-02-20 06:...	-	-	-	net.fbcdn.xx.st...	-	-	-	-	12813040

145 lines NirSoft Freeware. http://www.nirsoft.net



```
C:\Users\taro\Desktop\ESECarve>ESECarve.exe ie10 C:\Users\taro\Desktop\WebCache
root         INFO     ESECarve v2.02 started at 08-07-2018 22:36
root         INFO     Written by Howard Chivers. See README for software licence.
root         INFO     Called with arguments: ie10 C:\Users\taro\Desktop\WebCache
root         INFO     MD5 hash for C:\Users\taro\Desktop\WebCache\WebCacheV01.dat = b35b755b492c3ef820c9da6b9c2dcbd8
root         INFO     Carving from file: C:\Users\taro\Desktop\WebCache\WebCacheV01.dat
csvWriter    INFO     17973 lines written to C:\Users\taro\Desktop\WebCache\Container__all_CarvedData.csv, MD5 Hash = a8
e4cba1e114dddbd74e6ff813ff6c35
csvWriter    INFO     145 lines written to C:\Users\taro\Desktop\WebCache\Containers_CarvedData.csv, MD5 Hash = 5e4c401c
2870ac994d2b77faa455e2aa
root         INFO     Job complete at 08-07-2018 22:36
root         INFO     ************ end of job record

C:\Users\taro\Desktop\ESECarve>
```

Summary

Summary

- Histories might provide idea about what the attacker has watched during the attack.
- Since many applications use Web Browser as their frameworks, some web browser histories that are not a part of web browsing could be found.
  - For example, sometimes histories from the Windows Explorer could be found in the Internet Explorer histories.
- Don’t forget that the histories could be cleared.
  - Sometimes carving may become necessary.