# FORENSICS V2 LAB SERIES

# Lab 13: Internet Browser Forensics

**Document Version: 2021-01-14**

# Contents

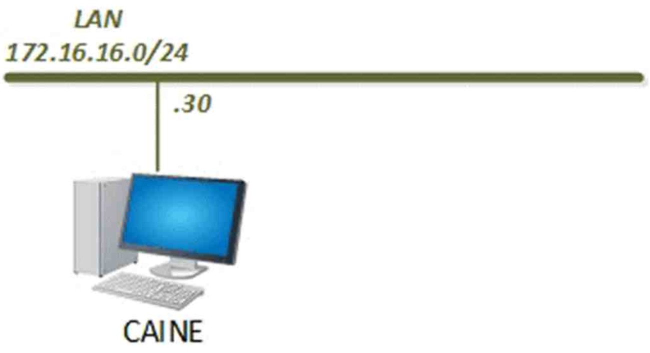
## Introduction

The internet is one of the main reasons why computers and smartphones have become so popular. This module will teach you how to access web history from Windows computers and utilize it in an investigation.

## Objectives

- Learn what files (and folders) are associated with web history
- Learn how to read the data within the web history files
- Learn how to view cached data

## Lab Topology



## Lab Settings

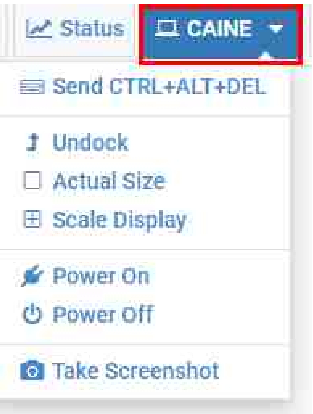
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

| **Virtual Machine** | **IP Address / Subnet Mask** | **Account** (if needed) | **Password** (if needed) |
|---|---|---|---|
| Caine | 172.16.16.30 | caine | Train1ng$ |
| CSI-Linux | 172.16.16.40 | csi | csi |
| DEFT | 172.16.16.20 | deft | Train1ng$ |
| WinOS | 172.16.16.10 | Administrator | Train1ng$ |

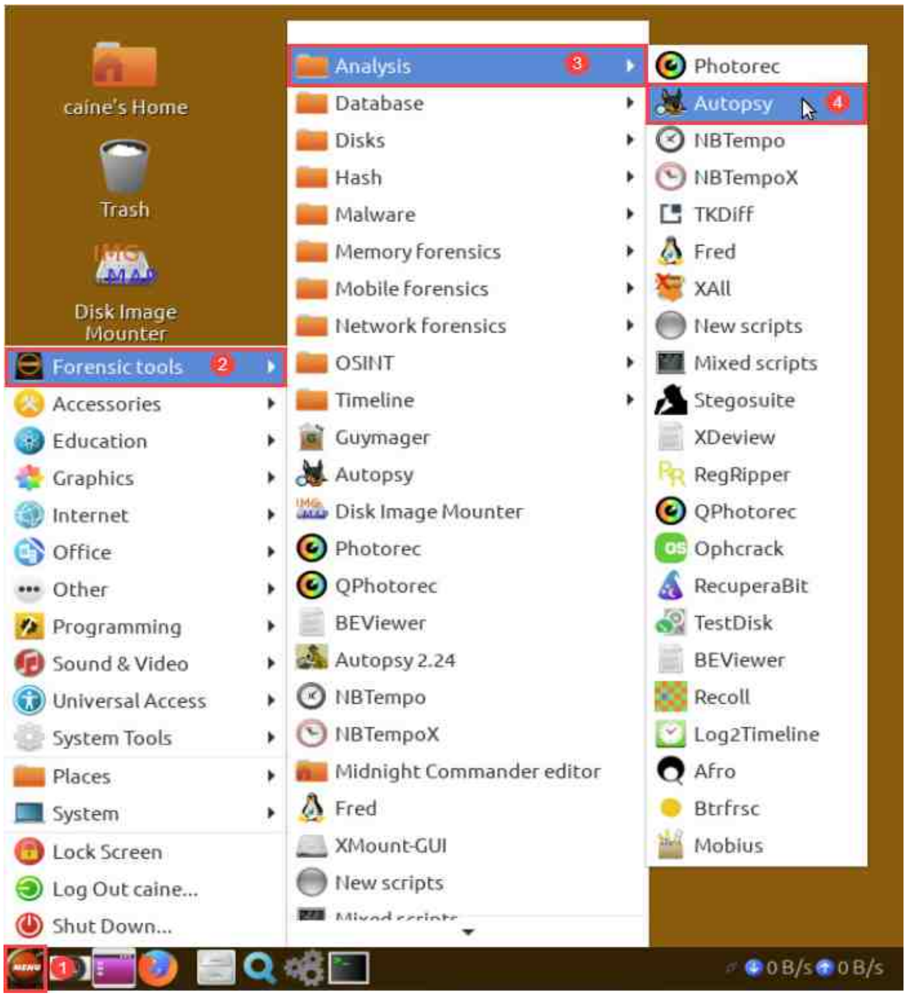
# 1 Learn What Files (and Folders) are Associated with Google Chrome Web History

Browsing the internet has become a pastime for many people. At the same time, web browsers are collecting more and more information about the people that use them. This is mainly to help the browsers work better and provide the information you need quickly without being overwhelmed. Another good purpose for this information is investigation. Web browsers tell great stories, but you need to know how to find where these browsers store their data.

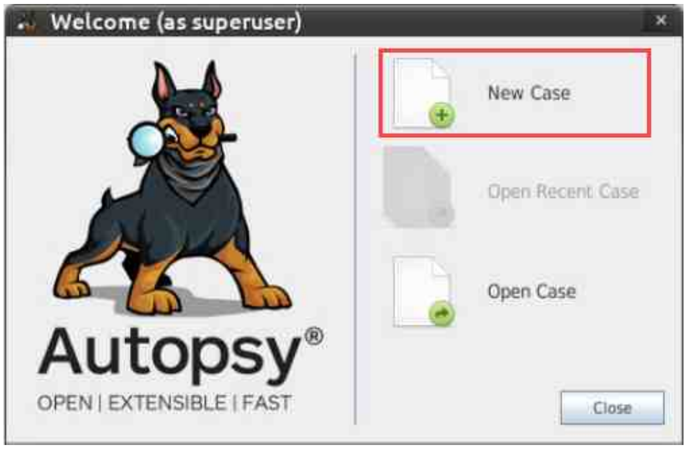
1. To begin, launch the CAINE virtual machine to access the graphical login screen.



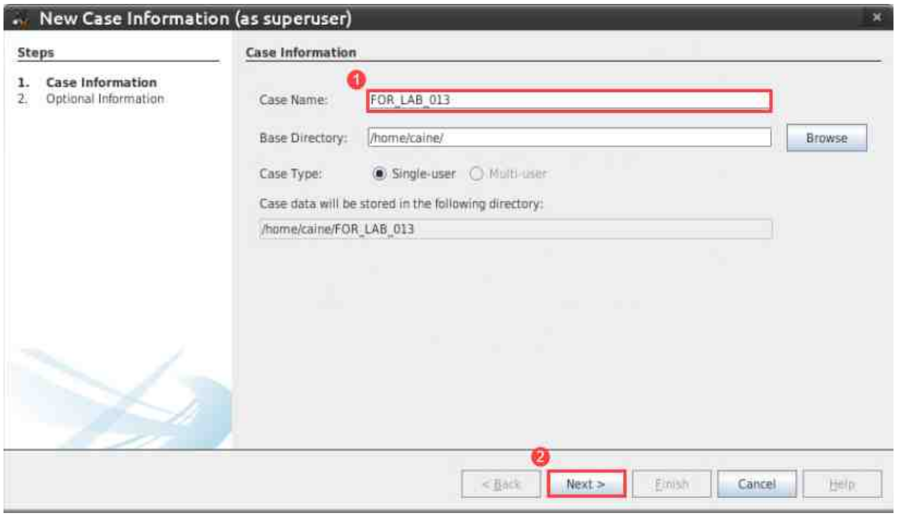
2. Once you are logged into the VM, launch the Autopsy program from the Start menu by navigating to Application Menu (top left corner) > Forensic tools > Analysis > Autopsy. Alternatively, you can open Autopsy from the taskbar by clicking the Autopsy icon as in item 1 below.



3. Since you're already familiar with Autopsy, let's jump right in by creating a new case. In Autopsy, click the New Case option from the Welcome window highlighted below; this will open the New Case Information window.



4. In the New Case Information window, enter `FOR_LAB_013` in the Case Name field. The Base Directory field is used to choose the location of the case folder. Let's leave the default selection and click Next as highlighted below.



Case Name: FOR_LAB_013

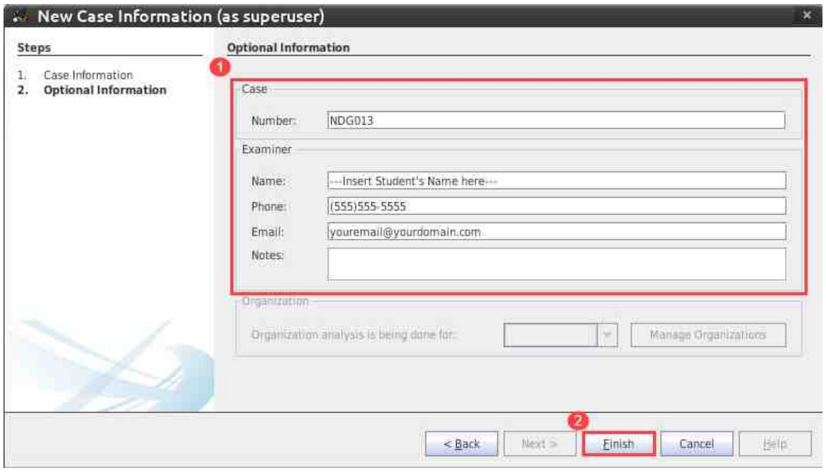
Base Directory: /home/caine/

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

/home/caine/FOR_LAB_013

5. The next window in the New Case wizard is the Optional Information window. Here you can type more information about the case and examiner. Fill in the information as seen in the fields below, and then click Finish when you are done. Remember, the Name field highlighted within the examiner section should contain your name.



Number: NDG013

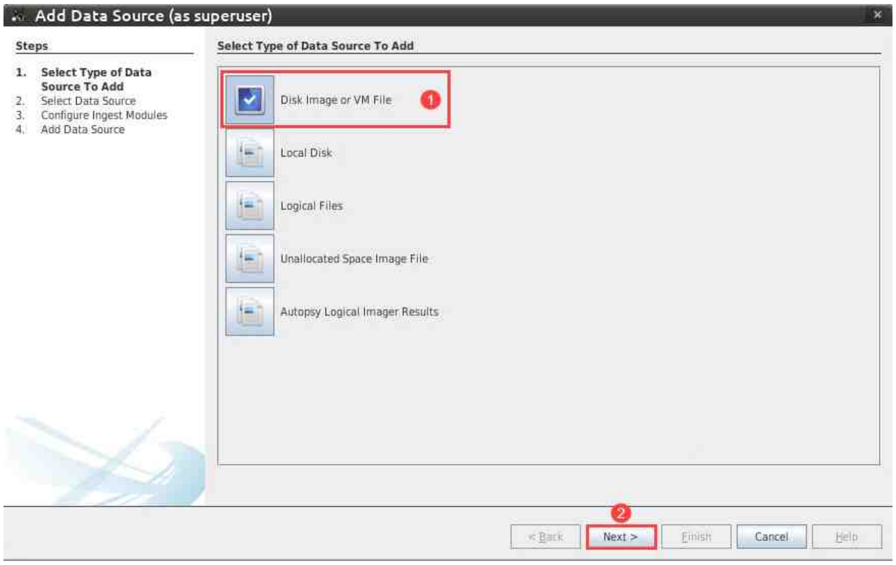
Name: ---Insert Student's Name here---

Phone: (555)555-5555

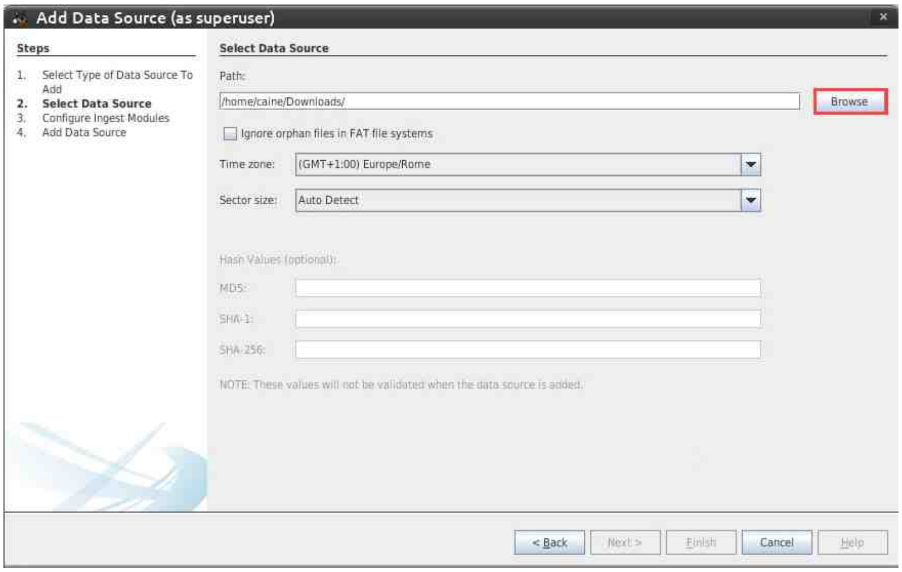
Email: youremail@yourdomain.com

Notes:

6. You will now be taken to the Add Data Source window. Here you can choose between different evidence sources. In this exercise, we will be using a Forensic Evidence File (FEF) so let's select Disk Image or VM file and click Next as highlighted below.


Add Data Source (as superuser)
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Type of Data Source To Add
Disk Image or VM File
1
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
2
< Back
Next >
Finish
Cancel
Help

7. The next window will allow you to choose the image you want to add to the case. Click the Browse button highlighted below to open the Open window that allows you to browse for the FEF.


Add Data Source (as superuser)

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path: /home/caine/Downloads/

□ Ignore orphan files in FAT file systems

Time zone: (GMT+1:00) Europe/Rome

Sector size: Auto Detect

Hash Values (optional):

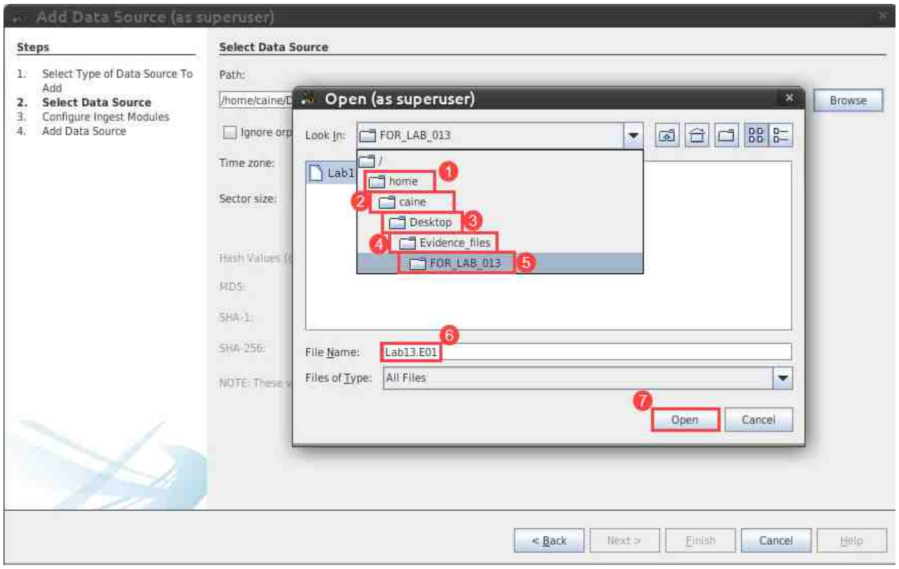
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

8. In the Open window, browse to home > caine > Desktop > Evidence_files > FOR_LAB_013, then click the file called Lab13.E01, and click Open, as highlighted in steps 1 – 7 below.

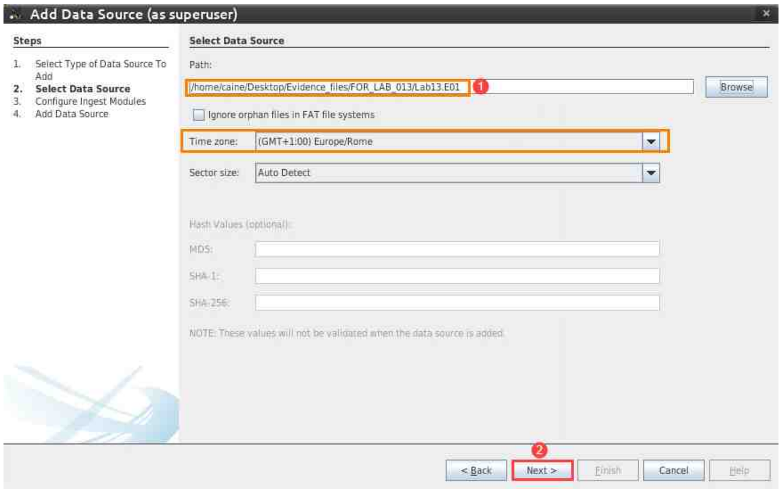

Open (as superuser)

Look In: FOR_LAB_013

File Name: Lab13.E01

Files of Type: All Files

9. The image path will now appear in the Path field, highlighted as item 1 below. We will leave the other options as-is for now and click Next highlighted as item 2 below.



Add Data Source (as superuser)

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path: /home/caine/Desktop/Evidence_files/FOR_LAB_013/Lab13.E01

□ Ignore orphan files in FAT file systems

Time zone: (GMT+1:00) Europe/Rome

Sector size: Auto Detect

Hash Values (optional):

MD5:

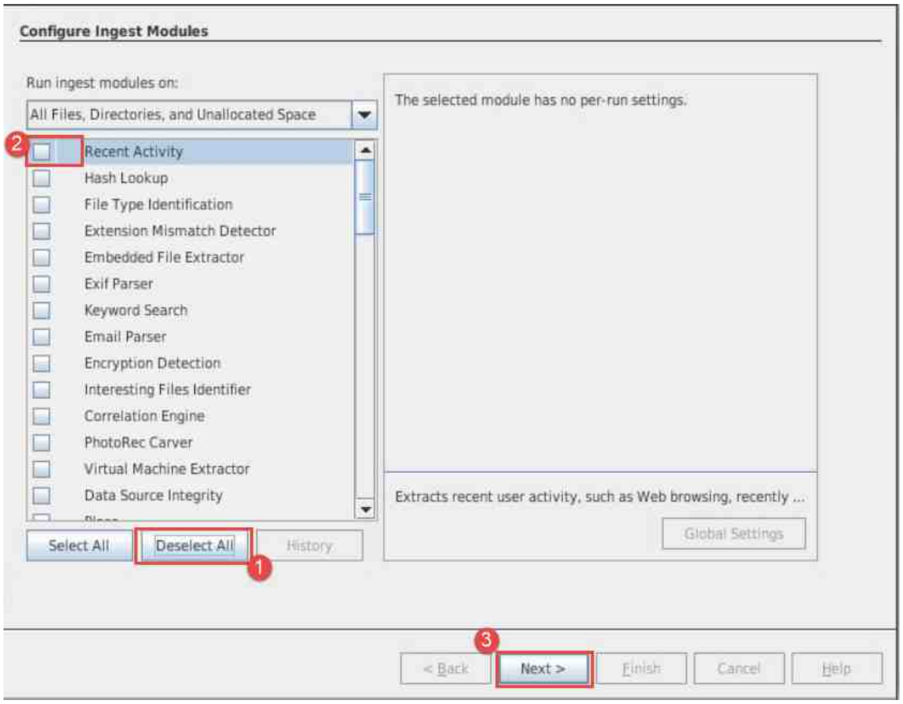
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Time zone is an important aspect of any forensic investigation. Feel free to adjust the time zone to match your respective time zone.

10. You will be taken to the Configure Ingest Modules step of the case creation process. We will be using the Recent Activity Ingest Module in this exercise, so uncheck any other selected Ingest Module by clicking the Deselect All button and then click the checkbox beside Recent Activity, as highlighted in items 1 and 2 below. Then, click Next, as seen in item 3 below.



Configure Ingest Modules

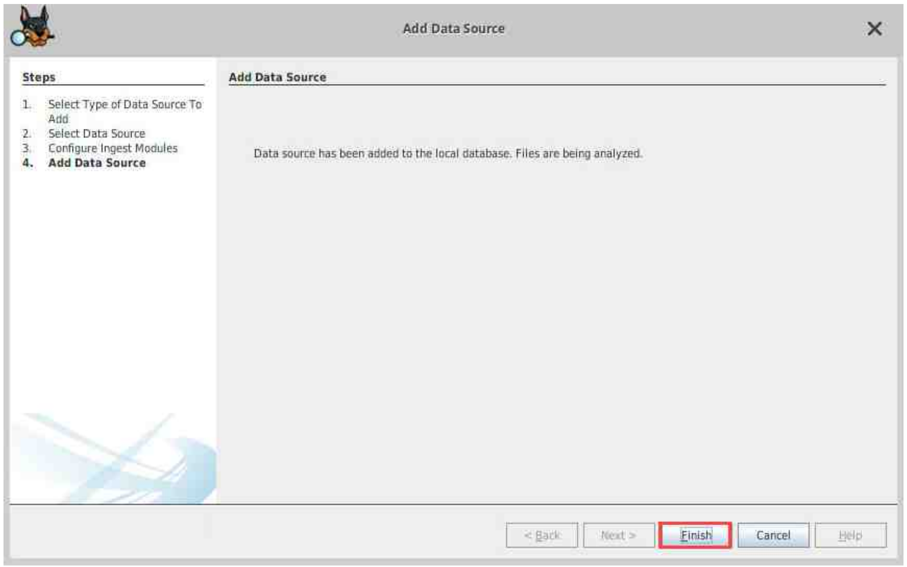
Run ingest modules on: All Files, Directories, and Unallocated Space

□ Recent Activity
□ Hash Lookup
□ File Type Identification
□ Extension Mismatch Detector
□ Embedded File Extractor
□ Exif Parser
□ Keyword Search
□ Email Parser
□ Encryption Detection
□ Interesting Files Identifier
□ Correlation Engine
□ PhotoRec Carver
□ Virtual Machine Extractor
□ Data Source Integrity
□ Plaso

The selected module has no per-run settings.

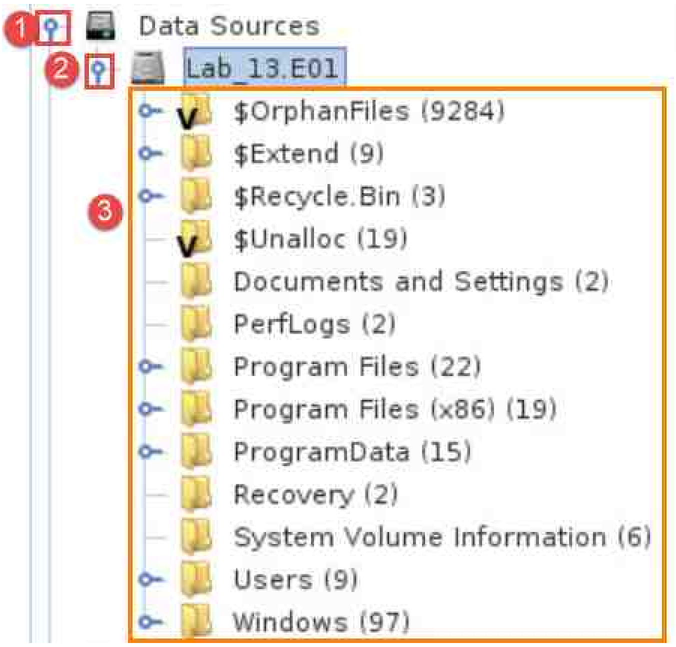
Extracts recent user activity, such as Web browsing, recently ...

11. In the final window in the Add Data Source process, click Finish as highlighted below.



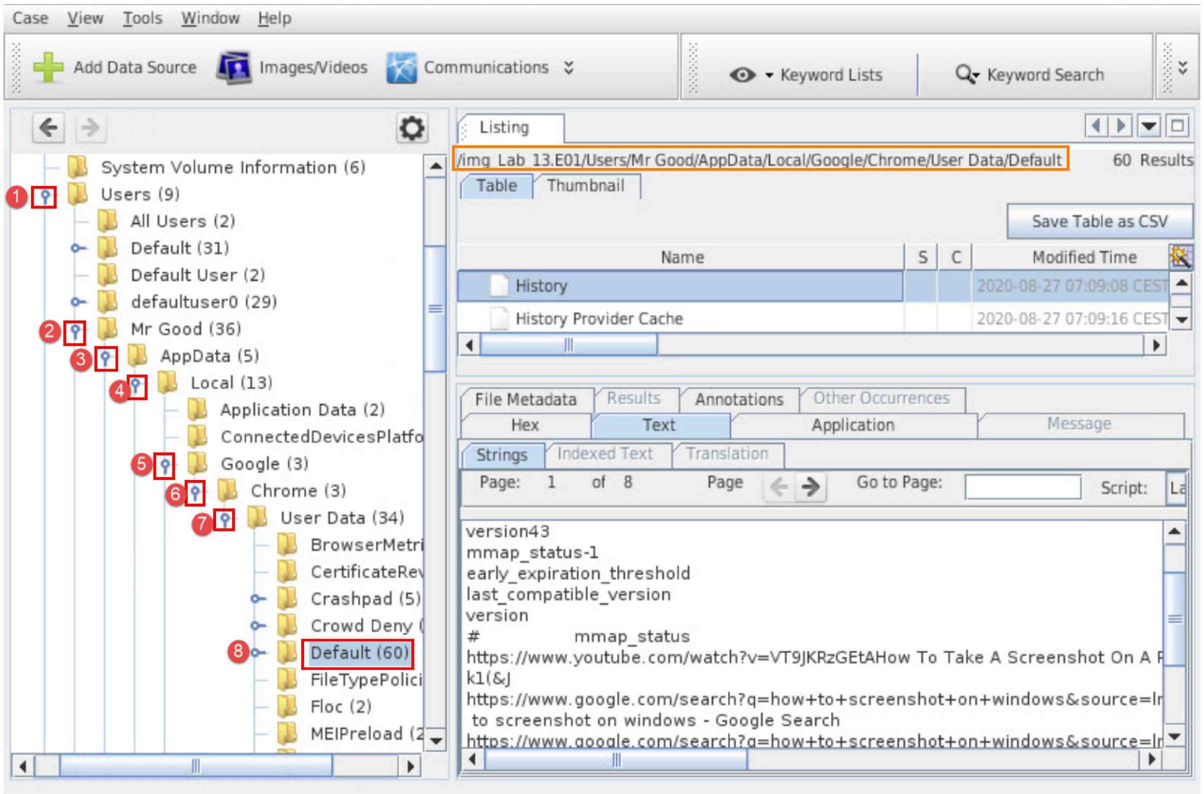
Data source has been added to the local database. Files are being analyzed.

12. You will now be taken to the Autopsy main window. Now we can begin learning the locations of the web history, web cache, and cookies directories for three popular web browsers. These are Google Chrome, Microsoft Edge, and Mozilla Firefox. Let's start with the Google Chrome web browser. This web browser uses a database file to store web history artifacts such as web visits, downloads, bookmarks, etc. Let's begin by clicking the blue pin beside Data Sources, as seen in item 1 below, which will expand and reveal the FEF. Next, click the blue pin beside Lab_13.E01 to view the file structure on the drive, as seen in item 2 below. The file system structure is the folders highlighted below in item 3.



Although each browser operates differently, they all have common features. One such feature is internet history. When this is examined, some might say it is often the key to understanding the user(s) of the computer.

13. Based on the folder structure, it is safe to say that this operating system is post-Windows Vista. We determine this by paying attention to the Users folder that contains the user profiles. The web history file for Google Chrome is located at the path: <User profile>\AppData\Local\Google\Chrome\User Data\Default\. To get there, click the blue pin beside the Users folder, as seen in item 1 below, to expand it and view the users' folders. In this exercise, we are interested in the account called Mr Good. So, click the blue pins beside the following folders to expand them and navigate to the Default folder: Mr Good > AppData > Local > Google > Chrome > User Data > Default, as seen in items 2 - 8.



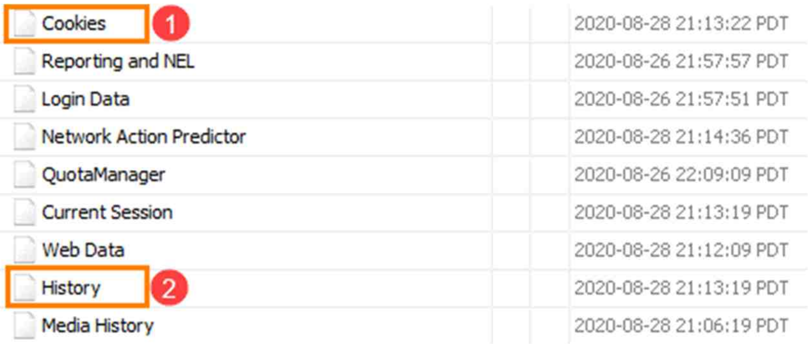
/img_Lab 13.E01/Users/Mr Good/AppData/Local/Google/Chrome/User Data/Default 60 Results

| Name | S | C | Modified Time |
|---|---|---|---|
| History | | | 2020-08-27 07:09:08 CEST |
| History Provider Cache | | | 2020-08-27 07:09:16 CEST |

```
version43
mmap_status-1
early_expiration_threshold
last_compatible_version
version
#            mmap_status
https://www.youtube.com/watch?v=VT9JKRzGEtAHow To Take A Screenshot On A F
k1(&J
https://www.google.com/search?q=how+to+screenshot+on+windows&source=lr
 to screenshot on windows - Google Search
https://www.google.com/search?q=how+to+screenshot+on+windows&source=lr
```

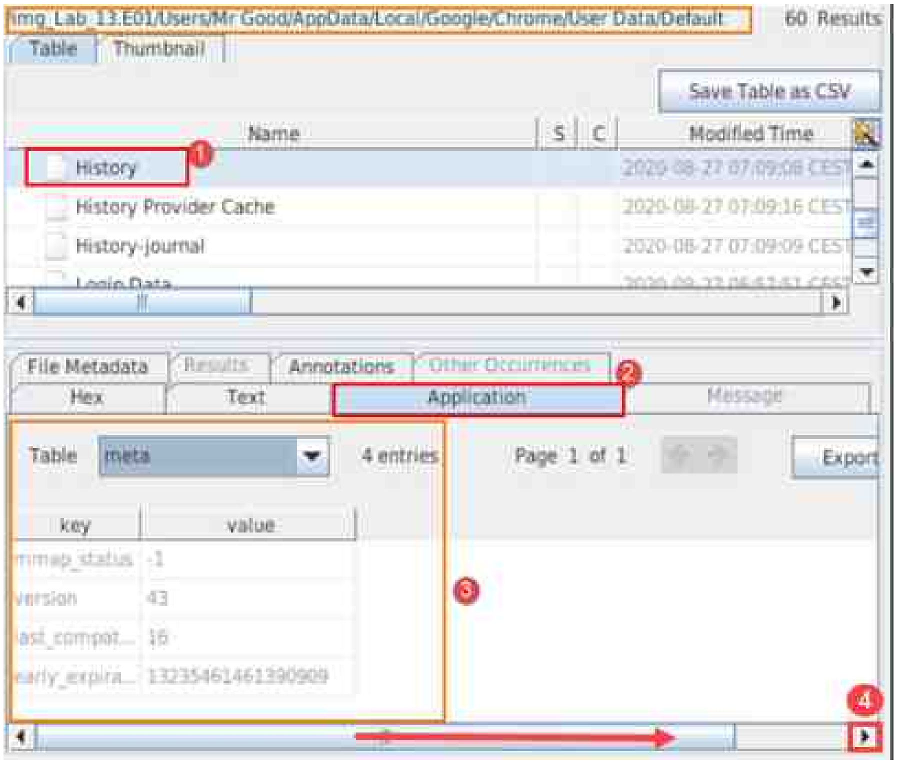
Autopsy creates references to the current folder and parent folder within the File List pane.

14. In the Default folder, there are several files that are used to assist the Google Chrome browser to function optimally. The files we are mainly interested in are the ones called Cookies and History, as seen in items 1 and 2 below.



| | | | |
|---|---|---|---|
| Cookies | 1 | | 2020-08-28 21:13:22 PDT |
| Reporting and NEL | | | 2020-08-26 21:57:57 PDT |
| Login Data | | | 2020-08-26 21:57:51 PDT |
| Network Action Predictor | | | 2020-08-28 21:14:36 PDT |
| QuotaManager | | | 2020-08-26 22:09:09 PDT |
| Current Session | | | 2020-08-28 21:13:19 PDT |
| Web Data | | | 2020-08-28 21:12:09 PDT |
| History | 2 | | 2020-08-28 21:13:19 PDT |
| Media History | | | 2020-08-28 21:06:19 PDT |

15. Let us look at the History file first. To begin, click the file as seen in item 1 below. Ensure that the Application tab is selected, as seen in item 2. Autopsy will display the contents of the selected file using the related application. In this case, the History file is a database file, so it will be displayed in a database format in rows and columns, as highlighted in item 3 below. If you do not see all the columns, you can scroll to the right using the horizontal scroll bar or by clicking the horizontal arrow seen in item 4 below.



img_Lab_13.E01/Users/Mr Good/AppData/Local/Google/Chrome/User Data/Default 60 Results

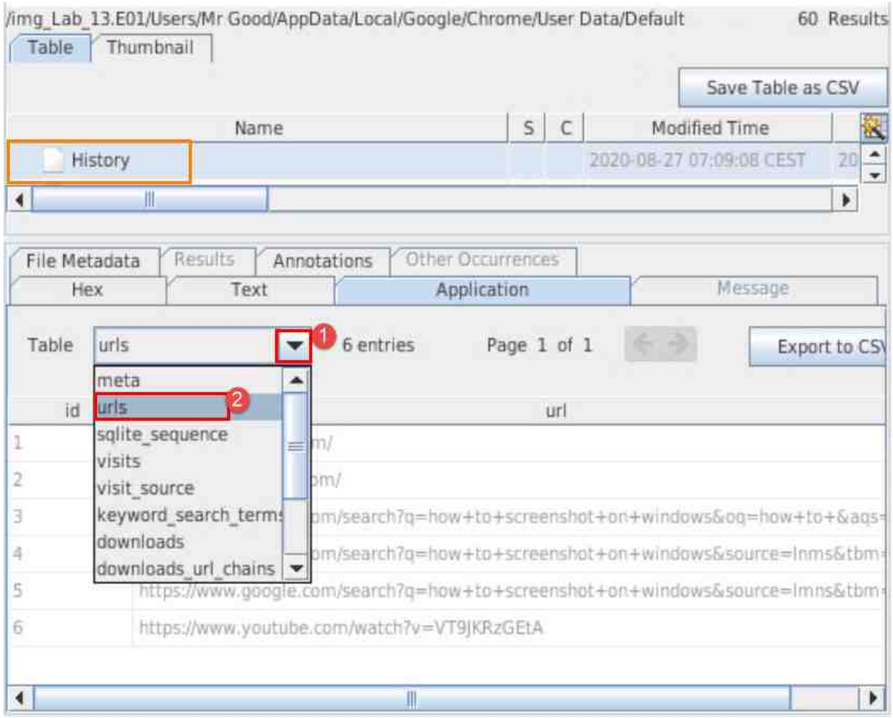
| Name | S | C | Modified Time |
|---|---|---|---|
| History | | | 2020-08-27 07:09:08 CEST |
| History Provider Cache | | | 2020-08-27 07:09:16 CEST |
| History-journal | | | 2020-08-27 07:09:09 CEST |
| Login Data | | | 2020-09-23 06:53:51 CEST |

Table meta 4 entries Page 1 of 1

| key | value |
|---|---|
| mmap_status | -1 |
| version | 43 |
| last_compat... | 16 |
| early_expira... | 13235461461390909 |

The history file is an SQLite database and can be exported from Autopsy and viewed by using other tools such as DB Browser for SQLite.

16. Since databases have different tables, let’s change to the web history table by clicking urls from the Table dropdown menu, as seen in items 1 and 2 below.

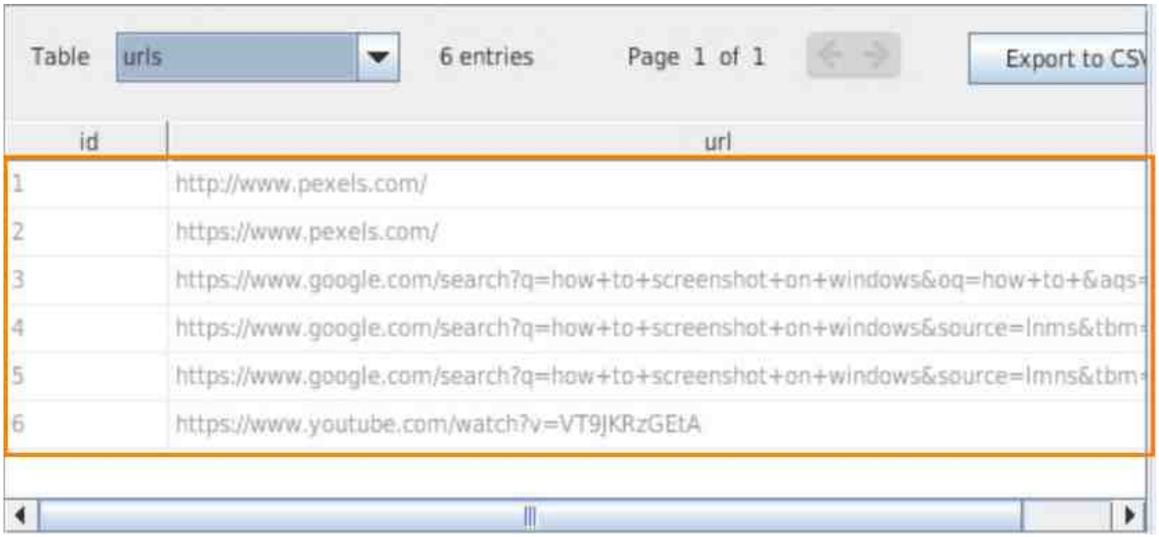

/img_Lab_13.E01/Users/Mr Good/AppData/Local/Google/Chrome/User Data/Default 60 Results

| Name | S | C | Modified Time | |
|---|---|---|---|---|
| History | | | 2020-08-27 07:09:08 CEST | 20 |

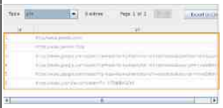
Table: urls — 6 entries — Page 1 of 1

| id | url |
|---|---|
| 1 | m/ |
| 2 | om/ |
| 3 | om/search?q=how+to+screenshot+on+windows&oq=how+to+&aqs= |
| 4 | om/search?q=how+to+screenshot+on+windows&source=lnms&tbm= |
| 5 | https://www.google.com/search?q=how+to+screenshot+on+windows&source=lmns&tbm= |
| 6 | https://www.youtube.com/watch?v=VT9JKRzGEtA |

17. As you can see in the table that appears, each URL that was accessed is listed. The table below the following screenshot outlines the purpose of each column.



| id | url |
|---|---|
| 1 | http://www.pexels.com/ |
| 2 | https://www.pexels.com/ |
| 3 | https://www.google.com/search?q=how+to+screenshot+on+windows&oq=how+to+&aqs |
| 4 | https://www.google.com/search?q=how+to+screenshot+on+windows&source=lnms&tbm |
| 5 | https://www.google.com/search?q=how+to+screenshot+on+windows&source=lmns&tbm |
| 6 | https://www.youtube.com/watch?v=VT9JKRzGEtA |

| | |
|---|---|
| id |  This column is the sequential order that each unique URL was visited |
| url | This column is the specific URL that was visited |
| title | This column is the title of the webpage |
| Visit_count | This column displays the number of times each URL was visited |
| Typed_count | This column displays each time the specific URL was typed |
| Last_visit_time | This column displays, in Unix time, the date and time the website was last visited |

18. Next, let’s look at another table. Click the visits table from the Table dropdown menu as seen in items 1 and 2.

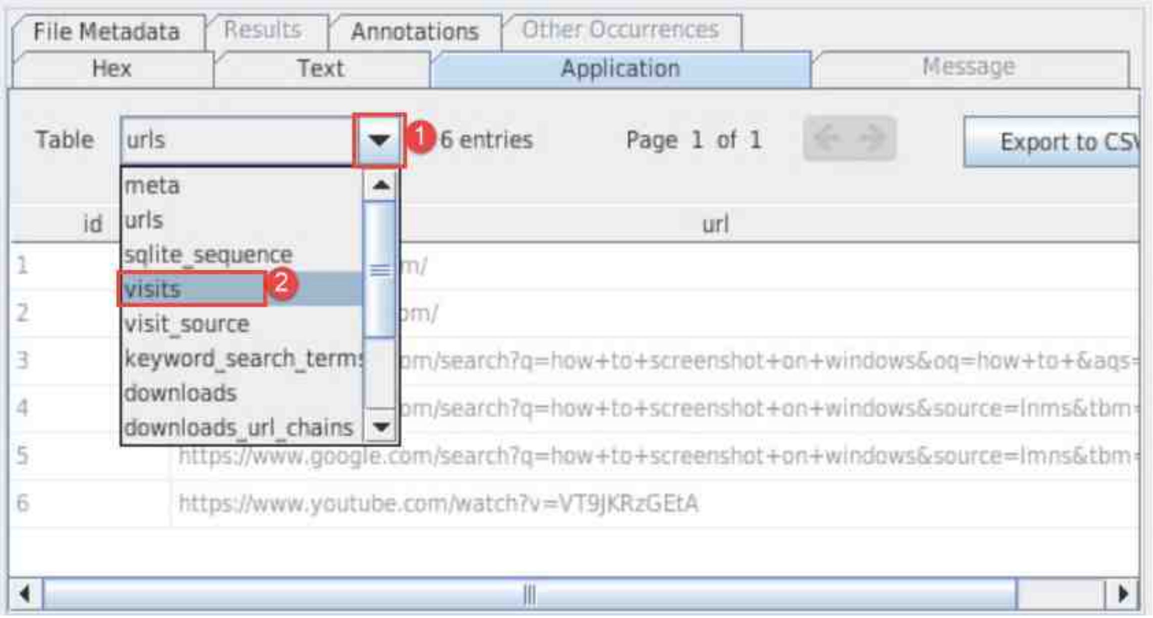
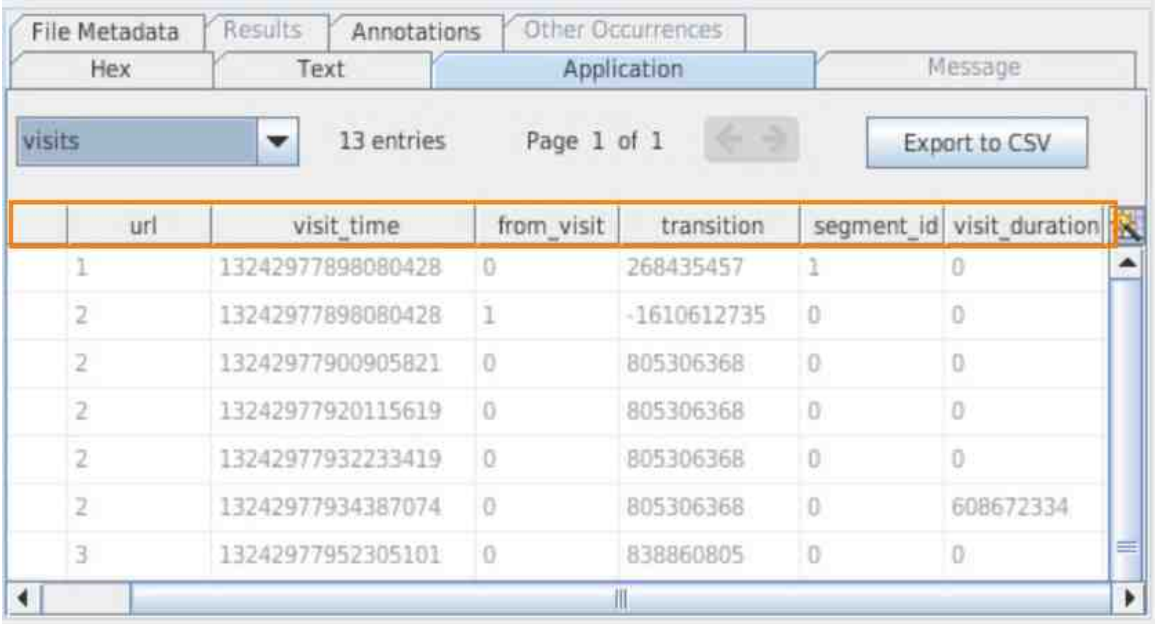


Table urls 6 entries Page 1 of 1

| id | url |
|---|---|
| 1 | m/ |
| 2 | om/ |
| 3 | om/search?q=how+to+screenshot+on+windows&oq=how+to+&aqs= |
| 4 | om/search?q=how+to+screenshot+on+windows&source=lnms&tbm |
| 5 | https://www.google.com/search?q=how+to+screenshot+on+windows&source=lnms&tbm |
| 6 | https://www.youtube.com/watch?v=VT9JKRzGEtA |

19. This table seems a lot more cryptic. There is no plain text data in it. The table below the following screenshot outlines the purpose of some of the more important columns.

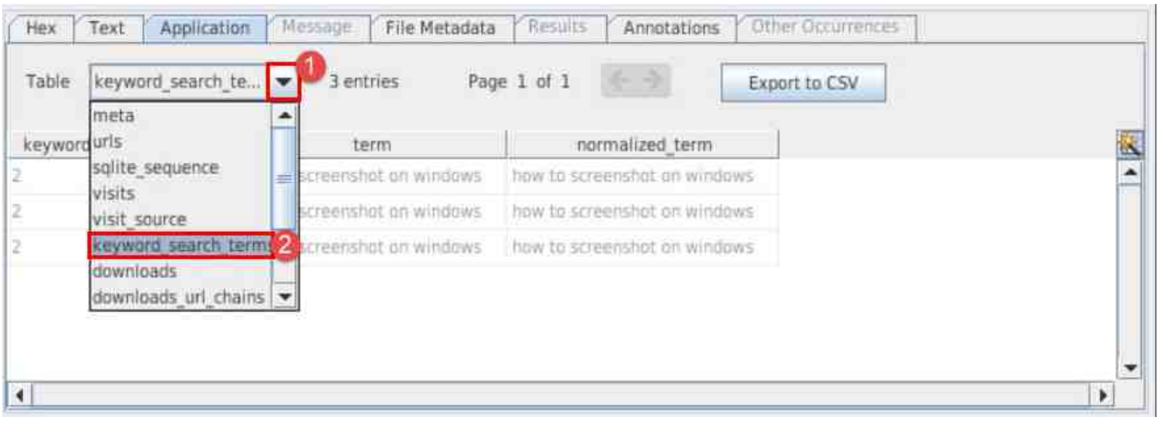


| | url | visit_time | from_visit | transition | segment_id | visit_duration |
|---|---|---|---|---|---|---|
| | 1 | 13242977898080428 | 0 | 268435457 | 1 | 0 |
| | 2 | 13242977898080428 | 1 | -1610612735 | 0 | 0 |
| | 2 | 13242977900905821 | 0 | 805306368 | 0 | 0 |
| | 2 | 13242977920115619 | 0 | 805306368 | 0 | 0 |
| | 2 | 13242977932233419 | 0 | 805306368 | 0 | 0 |
| | 2 | 13242977934387074 | 0 | 805306368 | 0 | 608672334 |
| | 3 | 13242977952305101 | 0 | 838860805 | 0 | 0 |

| | |
|---|---|
| id | This column is the sequential order that each entry was placed in the database. |
| url | The *url* column contains the ID number of the URL that we saw in the *urls* table above. For example, **2** in the url column, refers to the website https://www.pexels.com which is item **2** in the *urls* table. |
| Visit_time | The *visit_time* column contains the date and time that the referenced url was accessed by the browser. This is stored in Google Chrome Time and can be converted to human-readable format using a tool like Digital Detective's *DCode*[1] software. |
| From_visit | The *from_visit* column references the ID number of the URL that this visit was redirected from. |
| Visit_duration | The *visit_duration* column provides the length of time the user spent on the website. This data is stored in microseconds. |

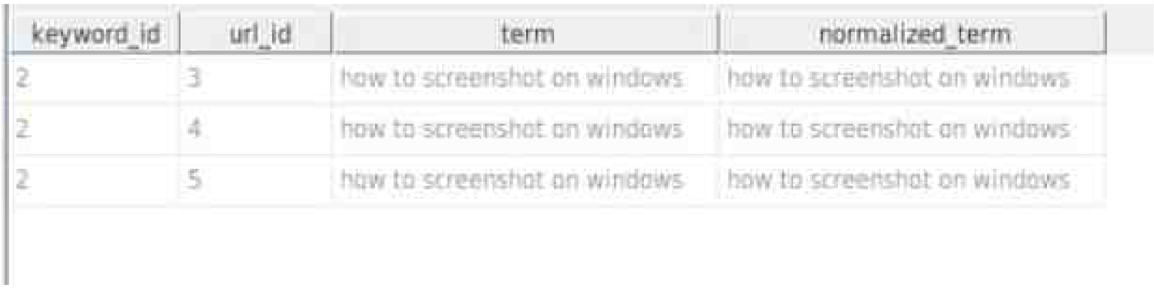
[1] https://www.digital-detective.net/dcode/

20. Next, let's look at another table. Click the keyword_search_terms table from the Table dropdown menu as seen in items 1 and 2.



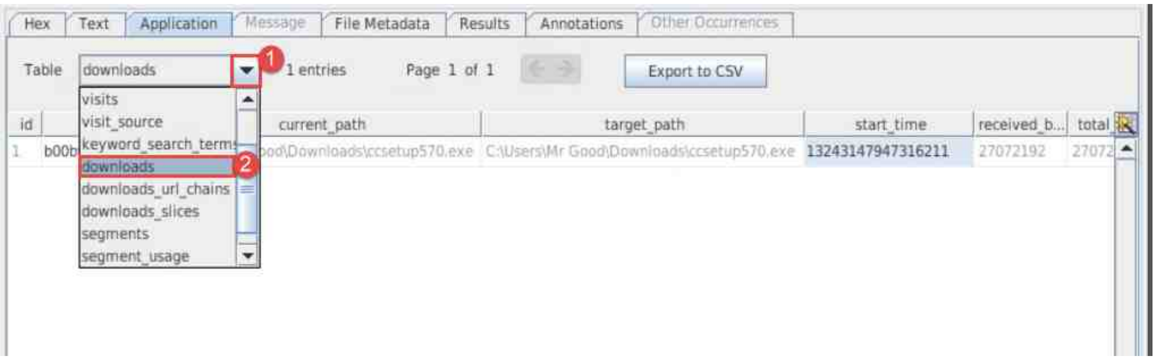
| keyword | term | normalized_term |
|---|---|---|
| 2 | creenshot on windows | how to screenshot on windows |
| 2 | creenshot on windows | how to screenshot on windows |
| 2 | creenshot on windows | how to screenshot on windows |

21. As seen in the screenshot below, this is a pretty straight-forward table. It lists the search terms entered in the browser and also references the url_id from the urls table.



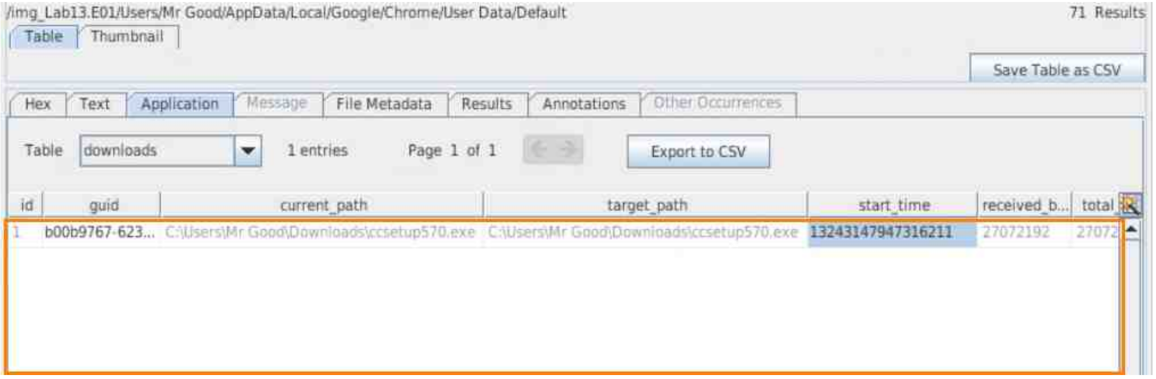
| keyword_id | url_id | term | normalized_term |
|---|---|---|---|
| 2 | 3 | how to screenshot on windows | how to screenshot on windows |
| 2 | 4 | how to screenshot on windows | how to screenshot on windows |
| 2 | 5 | how to screenshot on windows | how to screenshot on windows |

22. The last table we will look at is the downloads table. Click the downloads table from the Table dropdown menu, as seen in items 1 and 2.



| id | | current_path | target_path | start_time | received_b... | total |
|---|---|---|---|---|---|---|
| 1 | b00b | ood\Downloads\ccsetup570.exe | C:\Users\Mr Good\Downloads\ccsetup570.exe | 13243147947316211 | 27072192 | 27072 |

23. The downloads table contains the list of files that were downloaded. The table below the following screenshot outlines the purpose of some of the more important columns.



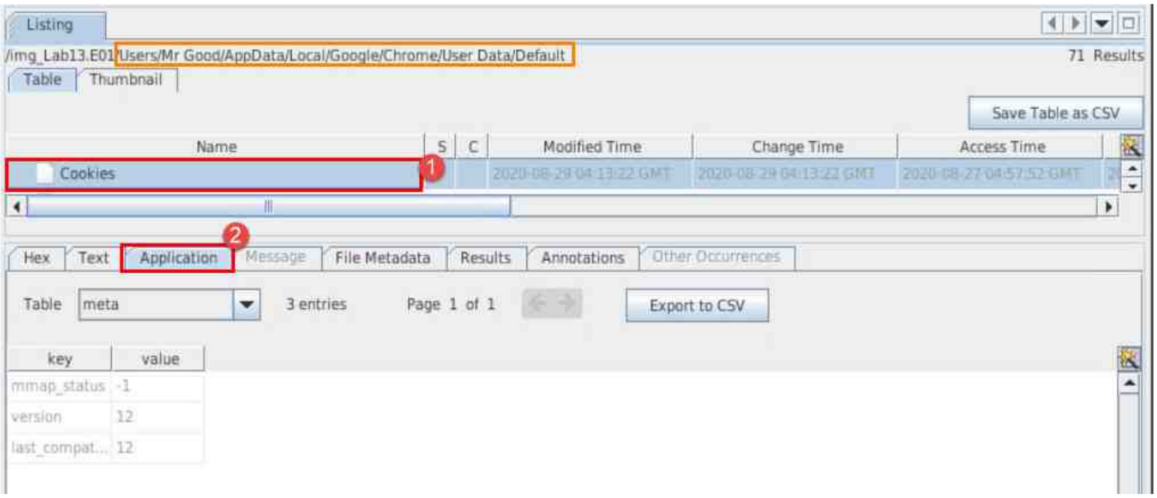
/img_Lab13.E01/Users/Mr Good/AppData/Local/Google/Chrome/User Data/Default 71 Results

Table downloads 1 entries Page 1 of 1

| id | guid | current_path | target_path | start_time | received_b... | total |
|---|---|---|---|---|---|---|
| 1 | b00b9767-623... | C:\Users\Mr Good\Downloads\ccsetup570.exe | C:\Users\Mr Good\Downloads\ccsetup570.exe | 13243147947316211 | 27072192 | 27072 |

| | |
|---|---|
| current_path | The location where the file is currently located |
| start_time | The date and time the file was downloaded |
| total_bytes | The size of the downloaded file |
| tab_url | The URL of the visited page |
| last_modified | The date and time the webpage was last visited |

24. Earlier, we mentioned the Cookies database file. This is the other file in the Default folder that is of interest to us. Let’s take a look at its contents. To do this, click the Cookies file and then click the Application tab, as seen in items 1 and 2 below.



| Name | S | C | Modified Time | Change Time | Access Time |
|---|---|---|---|---|---|
| Cookies | | | 2020-08-29 04:13:22 GMT | 2020-08-29 04:13:22 GMT | 2020-08-27 04:57:52 GMT |

Table meta 3 entries Page 1 of 1

| key | value |
|---|---|
| mmap_status | -1 |
| version | 12 |
| last_compat... | 12 |

25. The Cookies database file has only 2 tables, the meta and the cookies table. Browse to the cookies table by clicking it from the Table dropdown menu as seen in items 1 and 2 below.

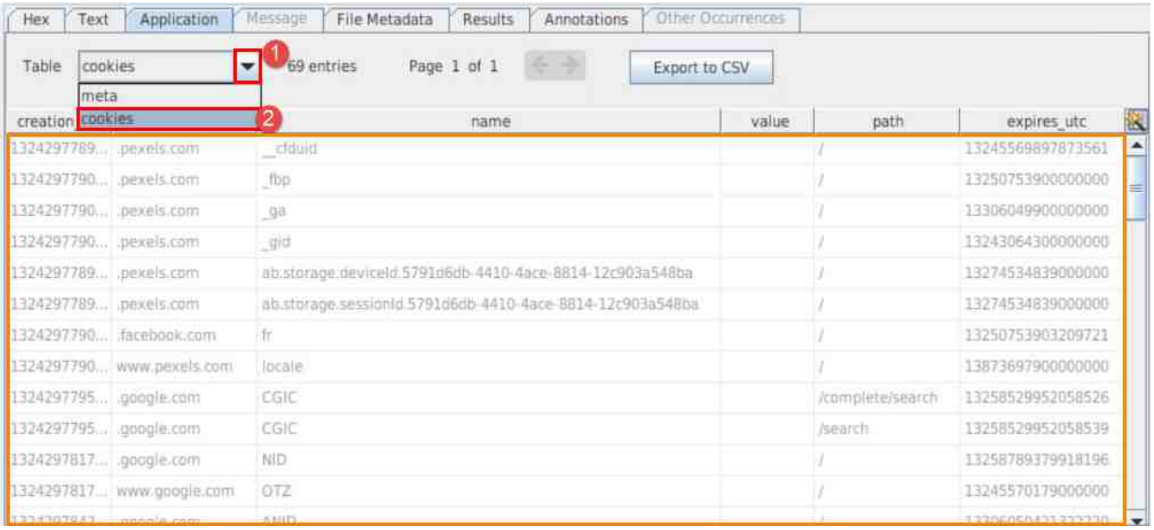


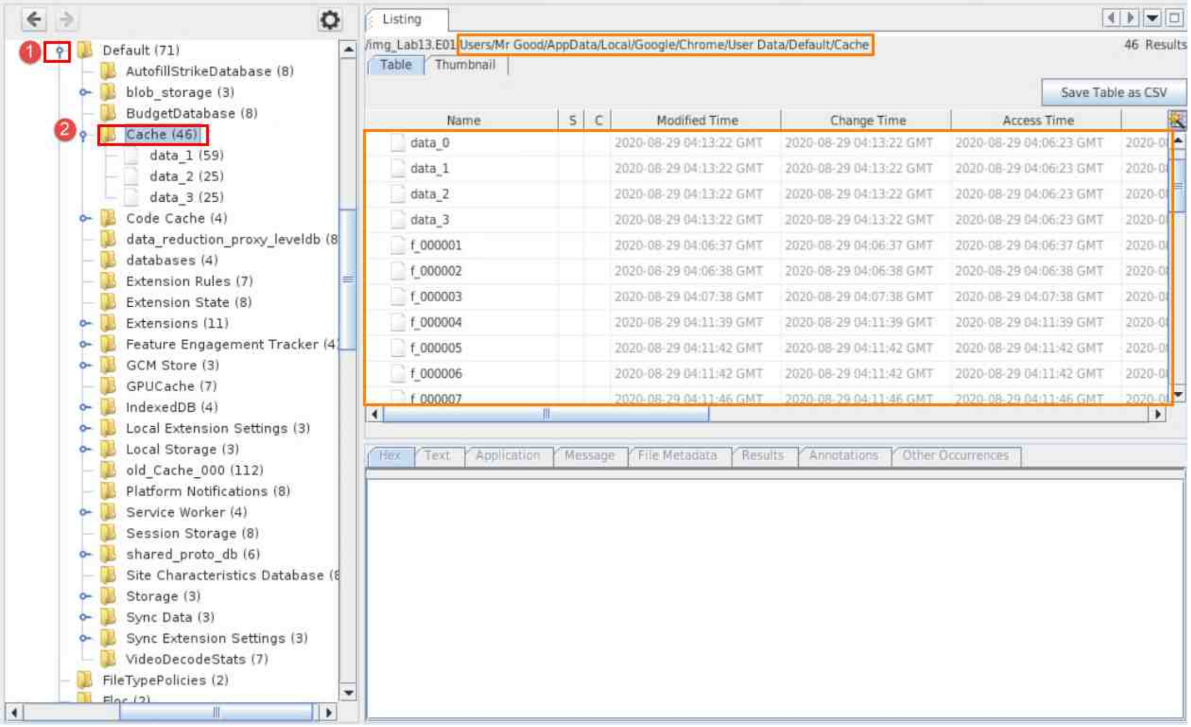
Table cookies 69 entries Page 1 of 1

| creation | | name | value | path | expires_utc |
|---|---|---|---|---|---|
| 1324297789... | .pexels.com | __cfduid | | / | 13245569897873561 |
| 1324297790... | .pexels.com | _fbp | | / | 13250753900000000 |
| 1324297790... | .pexels.com | _ga | | / | 13306049900000000 |
| 1324297790... | .pexels.com | _gid | | / | 13243064300000000 |
| 1324297789... | .pexels.com | ab.storage.deviceId.5791d6db-4410-4ace-8814-12c903a548ba | | / | 13274534839000000 |
| 1324297789... | .pexels.com | ab.storage.sessionId.5791d6db-4410-4ace-8814-12c903a548ba | | / | 13274534839000000 |
| 1324297790... | .facebook.com | fr | | / | 13250753903209721 |
| 1324297790... | www.pexels.com | locale | | / | 13873697900000000 |
| 1324297795... | .google.com | CGIC | | /complete/search | 13258529952058526 |
| 1324297795... | .google.com | CGIC | | /search | 13258529952058539 |
| 1324297817... | .google.com | NID | | / | 13258789379918196 |
| 1324297817... | www.google.com | OTZ | | / | 13245570179000000 |

26. Cookies are small files placed on the computer by websites. These files contain different types of data that record and store information, and settings about the user. The cookies can be of great value in proving that a user actually visited a website, and possibly store some things they did while there. The table below outlines the purpose of some of the more important columns of the Cookies database file, shown in the previous step.

| | |
|---|---|
| Creation_utc | The *creation_utc* is the data and time that the cookie was created on the computer. This data is stored in Google Chrome time. |
| Host_key | The *host_key* is the top-level domain name of the website that created the cookie. |
| Name | This is the name of the cookie. |
| Expires_utc | The *expires_utc* is the date and time that the cookie will expire and be deleted from the computer. |
| Last_access_utc | The *last_access_utc* is the date and time the cookie was last accessed by the website. |

27. The files we have accessed so far contained tons of metadata about the user's browsing activity. Now let's see if we can actually see what they were looking at. Web browsers use caching to make browsing faster. This means they download data to the computer so that it can be accessed quicker the next time you visit the webpage. This is great news for forensic examiners. Let's take a look at the cache data for the Google Chrome browser. The folder is located within a subdirectory of the current folder called Default. Expand the Default folder to access it by clicking the blue pin beside Default and then click the Cache folder, as seen in items 1 and 2 below.



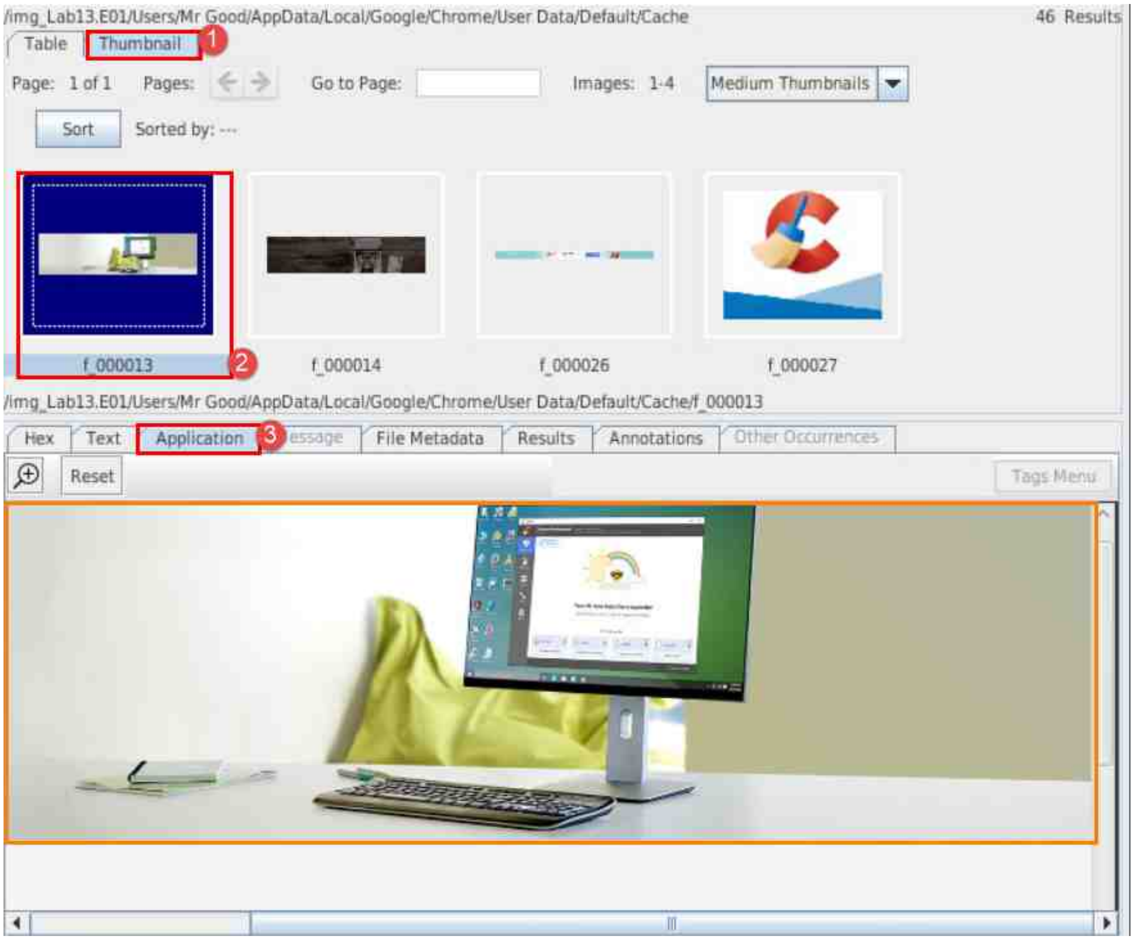
```
Default (71)
    AutofillStrikeDatabase (8)
    blob_storage (3)
    BudgetDatabase (8)
    Cache (46)
        data_1 (59)
        data_2 (25)
        data_3 (25)
    Code Cache (4)
    data_reduction_proxy_leveldb (8
    databases (4)
    Extension Rules (7)
    Extension State (8)
    Extensions (11)
    Feature Engagement Tracker (4
    GCM Store (3)
    GPUCache (7)
    IndexedDB (4)
    Local Extension Settings (3)
    Local Storage (3)
    old_Cache_000 (112)
    Platform Notifications (8)
    Service Worker (4)
    Session Storage (8)
    shared_proto_db (6)
    Site Characteristics Database (8
    Storage (3)
    Sync Data (3)
    Sync Extension Settings (3)
    VideoDecodeStats (7)
FileTypePolicies (2)
Floc (2)
```

/img_Lab13.E01/Users/Mr Good/AppData/Local/Google/Chrome/User Data/Default/Cache

46 Results

| Name | S | C | Modified Time | Change Time | Access Time |
|---|---|---|---|---|---|
| data_0 | | | 2020-08-29 04:13:22 GMT | 2020-08-29 04:13:22 GMT | 2020-08-29 04:06:23 GMT |
| data_1 | | | 2020-08-29 04:13:22 GMT | 2020-08-29 04:13:22 GMT | 2020-08-29 04:06:23 GMT |
| data_2 | | | 2020-08-29 04:13:22 GMT | 2020-08-29 04:13:22 GMT | 2020-08-29 04:06:23 GMT |
| data_3 | | | 2020-08-29 04:13:22 GMT | 2020-08-29 04:13:22 GMT | 2020-08-29 04:06:23 GMT |
| f_000001 | | | 2020-08-29 04:06:37 GMT | 2020-08-29 04:06:37 GMT | 2020-08-29 04:06:37 GMT |
| f_000002 | | | 2020-08-29 04:06:38 GMT | 2020-08-29 04:06:38 GMT | 2020-08-29 04:06:38 GMT |
| f_000003 | | | 2020-08-29 04:07:38 GMT | 2020-08-29 04:07:38 GMT | 2020-08-29 04:07:38 GMT |
| f_000004 | | | 2020-08-29 04:11:39 GMT | 2020-08-29 04:11:39 GMT | 2020-08-29 04:11:39 GMT |
| f_000005 | | | 2020-08-29 04:11:42 GMT | 2020-08-29 04:11:42 GMT | 2020-08-29 04:11:42 GMT |
| f_000006 | | | 2020-08-29 04:11:42 GMT | 2020-08-29 04:11:42 GMT | 2020-08-29 04:11:42 GMT |
| f_000007 | | | 2020-08-29 04:11:46 GMT | 2020-08-29 04:11:46 GMT | 2020-08-29 04:11:46 GMT |

28. As you can see in the Cache folder, there are lots of files that have standard naming and no extension. There are many different types of files inside this folder. The ones we will look at are the picture files. Let us click the Thumbnail tab, highlighted below at item 1, to switch the view to thumbnail view. As you can now see, many of the files we saw in the list view are actually picture files. They can provide you with a glimpse of the webpages that were viewed by the user. Select the first file as highlighted in item 2. To see an enlarged view, click the Application tab as seen below at item 3.



/img_Lab13.E01/Users/Mr Good/AppData/Local/Google/Chrome/User Data/Default/Cache 46 Results

Page: 1 of 1 Pages: Go to Page: Images: 1-4 Medium Thumbnails

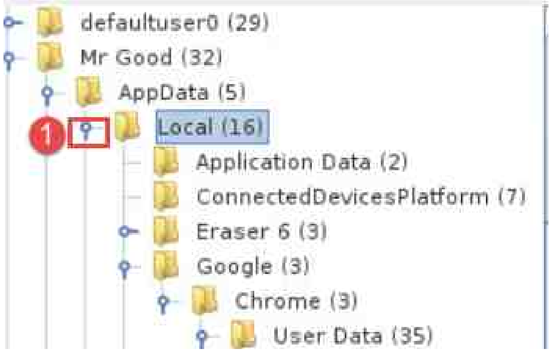
Sorted by: ---

/img_Lab13.E01/Users/Mr Good/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000013

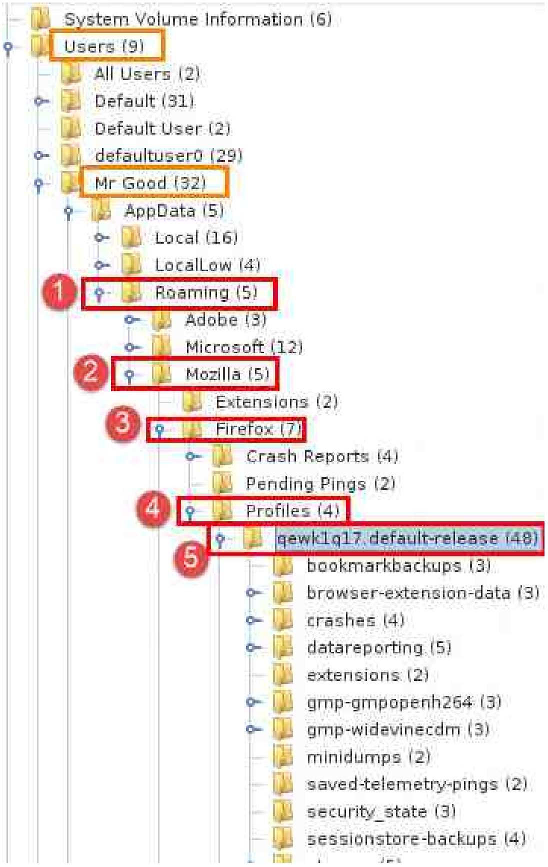
29. Now let’s look at the Firefox web browser.

## 2 Learn What Files (and Folders) are Associated with Firefox Web History

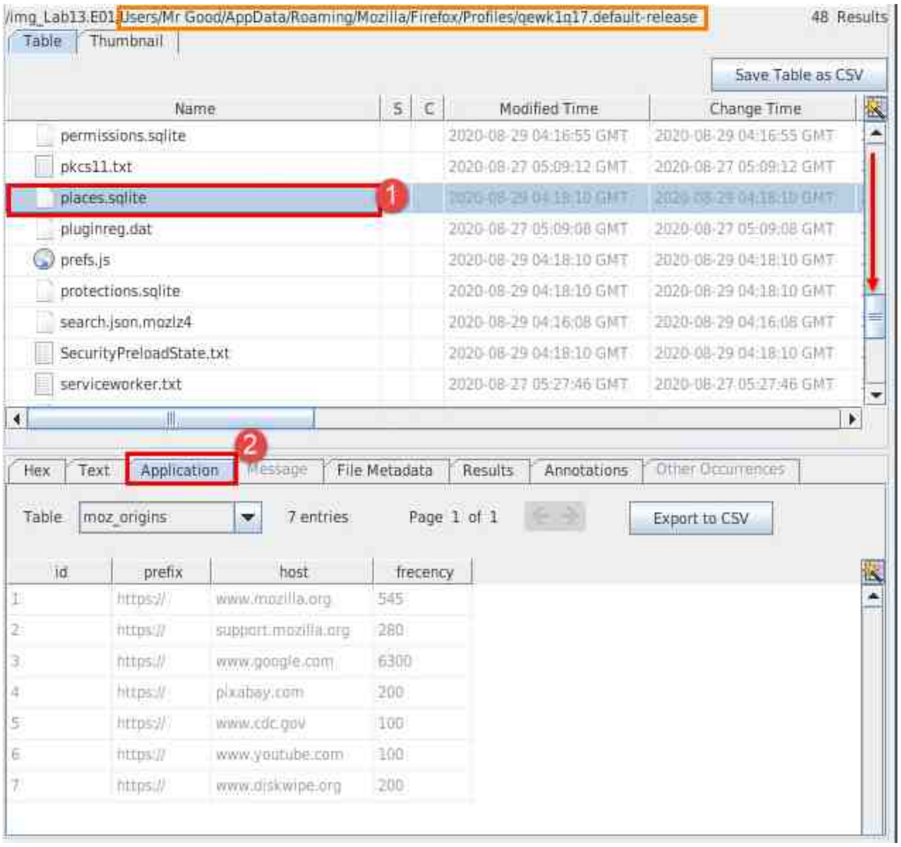
1. The Firefox web browser is one of the common web browsers, and it stores tons of data as well. The data is located in a different path, however. Let's begin by contracting the previously expanded folders. Do this by clicking the blue pin beside the folder called Local as seen in item 1 below.



2. The history and cookies files are stored in the path C > Users > Mr Good > AppData > Roaming > Mozilla > Firefox > Profiles > *.default-release, while the cache is stored in C > Users > Mr Good > AppData > local > Mozilla > Firefox > Profiles > *.default-release. Let's go to the history and cookies files first. To do this, click the blue pins beside the following folders to expand them and navigate to the *.default-release folder: Roaming > Mozilla > Firefox > Profiles > qewk1q17.default-release, as seen in items 1 - 5 below.



3. Once there, scroll down until you locate the file called places.sqlite and click the Application tab as seen in items 1 and 2 below. The table below the following screenshot outlines the purpose of some of the more important columns.



| Name | S | C | Modified Time | Change Time |
|---|---|---|---|---|
| permissions.sqlite | | | 2020-08-29 04:16:55 GMT | 2020-08-29 04:16:55 GMT |
| pkcs11.txt | | | 2020-08-27 05:09:12 GMT | 2020-08-27 05:09:12 GMT |
| places.sqlite | | | 2020-08-29 04:18:10 GMT | 2020-08-29 04:18:10 GMT |
| pluginreg.dat | | | 2020-08-27 05:09:08 GMT | 2020-08-27 05:09:08 GMT |
| prefs.js | | | 2020-08-29 04:18:10 GMT | 2020-08-29 04:18:10 GMT |
| protections.sqlite | | | 2020-08-29 04:18:10 GMT | 2020-08-29 04:18:10 GMT |
| search.json.mozlz4 | | | 2020-08-29 04:16:08 GMT | 2020-08-29 04:16:08 GMT |
| SecurityPreloadState.txt | | | 2020-08-29 04:18:10 GMT | 2020-08-29 04:18:10 GMT |
| serviceworker.txt | | | 2020-08-27 05:27:46 GMT | 2020-08-27 05:27:46 GMT |

Table moz_origins 7 entries Page 1 of 1

| id | prefix | host | frecency |
|---|---|---|---|
| 1 | https:// | www.mozilla.org | 545 |
| 2 | https:// | support.mozilla.org | 280 |
| 3 | https:// | www.google.com | 6300 |
| 4 | https:// | pixabay.com | 200 |
| 5 | https:// | www.cdc.gov | 100 |
| 6 | https:// | www.youtube.com | 100 |
| 7 | https:// | www.diskwipe.org | 200 |

| | |
|---|---|
| id | This column is the sequential order that each entry was placed in the table. |
| Prefix | This column provides the prefix of the web address. |
| Host | This is the top-level domain for the URL. |
| Frequency | This is a score given to each URL to track the frequency and recency of visits. It is used to provide better suggestions for the user. |

4. The first table you will see is the moz_origins table. It stores data about the top-level domains from visited web pages.

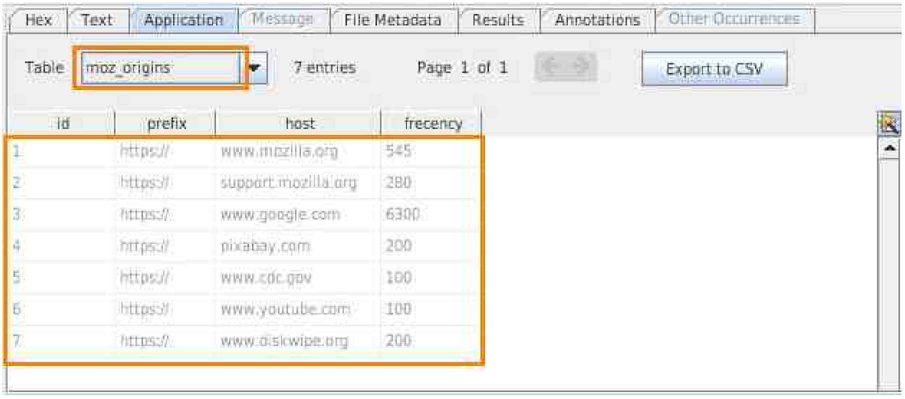


Table moz_origins 7 entries Page 1 of 1

| id | prefix | host | frecency |
|---|---|---|---|
| 1 | https:// | www.mozilla.org | 545 |
| 2 | https:// | support.mozilla.org | 280 |
| 3 | https:// | www.google.com | 6300 |
| 4 | https:// | pixabay.com | 200 |
| 5 | https:// | www.cdc.gov | 100 |
| 6 | https:// | www.youtube.com | 100 |
| 7 | https:// | www.diskwipe.org | 200 |

5. Let's change to the web history table by clicking moz_places from the Table dropdown menu, as seen in items 1 and 2 below.

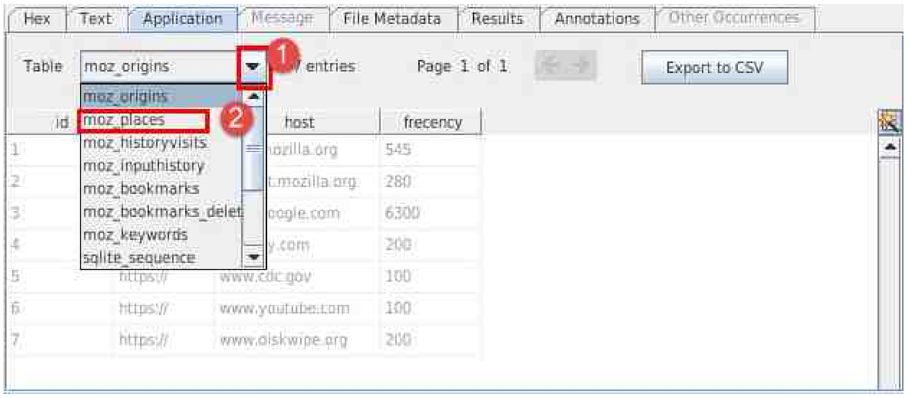


Table moz_origins 7 entries Page 1 of 1

| id | prefix | host | frecency |
|---|---|---|---|
| 1 | | ozilla.org | 545 |
| 2 | | t.mozilla.org | 280 |
| 3 | | oogle.com | 6300 |
| 4 | | y.com | 200 |
| 5 | https:// | www.cdc.gov | 100 |
| 6 | https:// | www.youtube.com | 100 |
| 7 | https:// | www.diskwipe.org | 200 |

6. As you can see in the table that appears, each URL that was accessed is listed. The table below the following screenshot outlines the purpose of some of the more important columns.

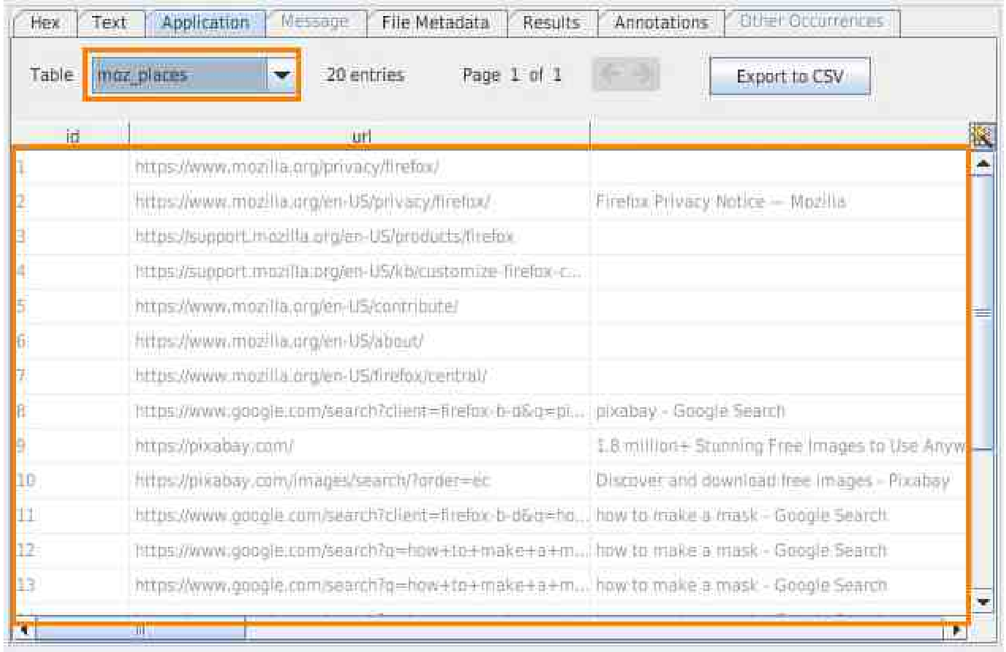
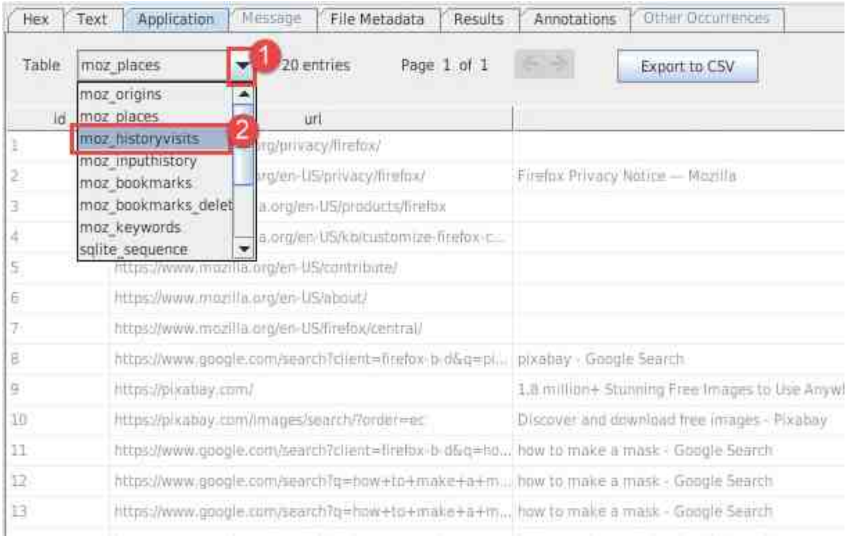


Table moz_places 20 entries Page 1 of 1

| id | url | |
|---|---|---|
| 1 | https://www.mozilla.org/privacy/firefox/ | |
| 2 | https://www.mozilla.org/en-US/privacy/firefox/ | Firefox Privacy Notice — Mozilla |
| 3 | https://support.mozilla.org/en-US/products/firefox | |
| 4 | https://support.mozilla.org/en-US/kb/customize-firefox-c... | |
| 5 | https://www.mozilla.org/en-US/contribute/ | |
| 6 | https://www.mozilla.org/en-US/about/ | |
| 7 | https://www.mozilla.org/en-US/firefox/central/ | |
| 8 | https://www.google.com/search?client=firefox-b-d&q=pi... | pixabay - Google Search |
| 9 | https://pixabay.com/ | 1.8 million+ Stunning Free Images to Use Anyw |
| 10 | https://pixabay.com/images/search/?order=ec | Discover and download free images - Pixabay |
| 11 | https://www.google.com/search?client=firefox-b-d&q=ho... | how to make a mask - Google Search |
| 12 | https://www.google.com/search?q=how+to+make+a+m... | how to make a mask - Google Search |
| 13 | https://www.google.com/search?q=how+to+make+a+m... | how to make a mask - Google Search |

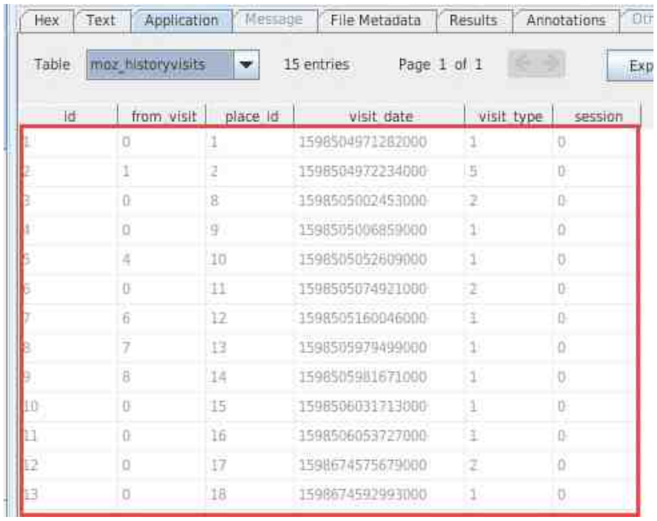
| | |
|---|---|
| id | This column is the sequential order in which each unique URL was visited |
| url | This column is the specific URL that was visited |
| Title | This column is the title of the webpage |
| Visit_count | This column displays the number of times each URL was visited |
| Last_visit_date | This column displays, in Unix time, the date and time the website was last visited |
| Preview_image_url | This column will list the name of the preview image on a webpage |
| Origin_id | References the URL that matches ID number from the *moz_origins* table |

7. Let's change to another table. Click moz_historyvisits from the Table dropdown menu as seen in items 1 and 2 below.



| id | url | |
|---|---|---|
| 1 | rg/privacy/firefox/ | |
| 2 | rg/en-US/privacy/firefox/ | Firefox Privacy Notice — Mozilla |
| 3 | a.org/en-US/products/firefox | |
| 4 | a.org/en-US/kb/customize-firefox-c... | |
| 5 | https://www.mozilla.org/en-US/contribute/ | |
| 6 | https://www.mozilla.org/en-US/about/ | |
| 7 | https://www.mozilla.org/en-US/firefox/central/ | |
| 8 | https://www.google.com/search?client=firefox-b-d&q=pi... | pixabay - Google Search |
| 9 | https://pixabay.com/ | 1.8 million+ Stunning Free Images to Use Anywh |
| 10 | https://pixabay.com/images/search/?order=ec | Discover and download free images - Pixabay |
| 11 | https://www.google.com/search?client=firefox-b-d&q=ho... | how to make a mask - Google Search |
| 12 | https://www.google.com/search?q=how+to+make+a+m... | how to make a mask - Google Search |
| 13 | https://www.google.com/search?q=how+to+make+a+m... | how to make a mask - Google Search |

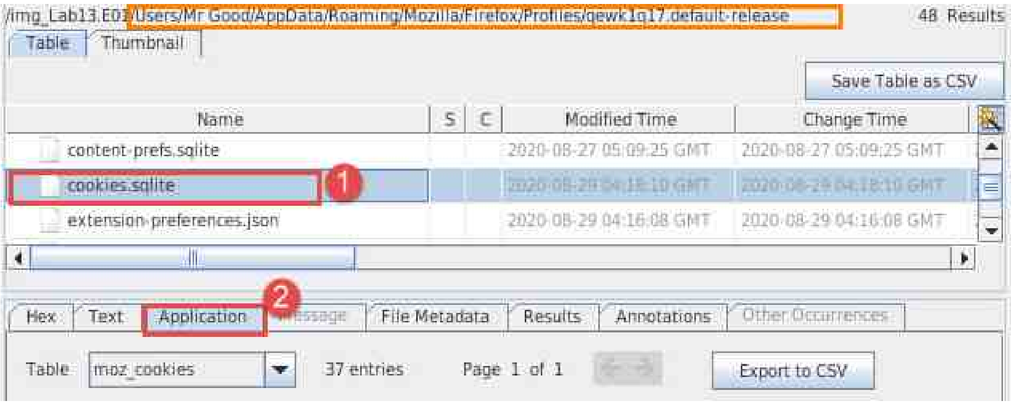
8. An entry is created in moz_historyvisits each time you visit a webpage. It stores information about the date and time of the visit, the referrer, and the method used to access the page. The table below the following screenshot outlines the purpose of some of the more important columns.



| id | from visit | place id | visit date | visit type | session |
|---|---|---|---|---|---|
| 1 | 0 | 1 | 1598504971282000 | 1 | 0 |
| 2 | 1 | 2 | 1598504972234000 | 5 | 0 |
| 3 | 0 | 8 | 1598505002453000 | 2 | 0 |
| 4 | 0 | 9 | 1598505006859000 | 1 | 0 |
| 5 | 4 | 10 | 1598505052609000 | 1 | 0 |
| 6 | 0 | 11 | 1598505074921000 | 2 | 0 |
| 7 | 6 | 12 | 1598505160046000 | 1 | 0 |
| 8 | 7 | 13 | 1598505979499000 | 1 | 0 |
| 9 | 8 | 14 | 1598505981671000 | 1 | 0 |
| 10 | 0 | 15 | 1598506031713000 | 1 | 0 |
| 11 | 0 | 16 | 1598506053727000 | 1 | 0 |
| 12 | 0 | 17 | 1598674575679000 | 2 | 0 |
| 13 | 0 | 18 | 1598674592993000 | 1 | 0 |

| | |
|---|---|
| id | This column is the sequential order in which each unique URL was visited. |
| From_visit | This column is the ID of the URL that the web page was visited from. |
| Place_id | This column is the ID of the URL that was visited. |
| Visit_date | This column displays the date and time each URL was visited. |
| Visit_type | This is an index that *Firefox* uses to tell how the webpage was visited. It has 9 different IDs, including 3 for access from a bookmark, 7 for a download, 9 for a page reload, etc. For more information, visit https://developer.mozilla.org/en-US/docs/Mozilla/Tech/Places/Database |

9. The history file is structured a little different than the one from Google Chrome but still provides similarly valuable information. Now let's move on to the cookies file. This is located in the same directory as the places.sqlite file. To access it, click the file called cookies.sqlite and then click the Application tab as seen in items 1 and 2 below.

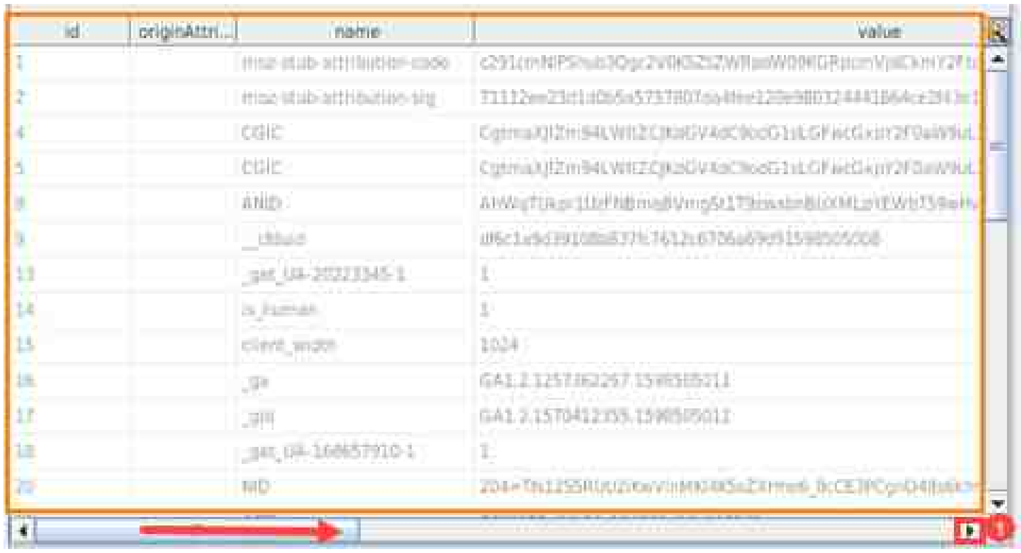


/img_Lab13.E01/Users/Mr Good/AppData/Roaming/Mozilla/Firefox/Profiles/qewk1q17.default-release    48 Results

| Name | S | C | Modified Time | Change Time |
|---|---|---|---|---|
| content-prefs.sqlite | | | 2020-08-27 05:09:25 GMT | 2020-08-27 05:09:25 GMT |
| cookies.sqlite | | | 2020-08-29 04:18:10 GMT | 2020-08-29 04:18:10 GMT |
| extension-preferences.json | | | 2020-08-29 04:16:08 GMT | 2020-08-29 04:16:08 GMT |

Table moz_cookies    37 entries    Page 1 of 1

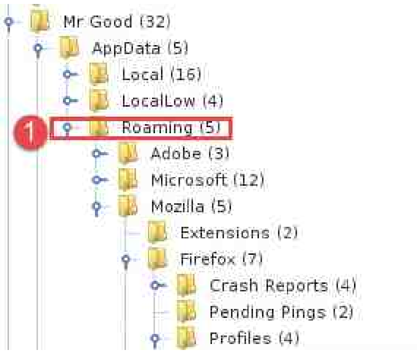
10. This cookies database has only one table called moz_cookies. The table below the following screenshot outlines the purpose of some of the more important columns. To view additional columns, scroll to the right using the horizontal scroll bar or the horizontal arrow seen in item 1 below.



| id | originAttri... | name | value |
|---|---|---|---|
| 1 | | moz-stub-attribution-code | [illegible] |
| 2 | | moz-stub-attribution-sig | [illegible] |
| 4 | | CGIC | [illegible] |
| 5 | | CGIC | [illegible] |
| 8 | | ANID | [illegible] |
| 9 | | __cfduid | [illegible] |
| 13 | | _gat_UA-20223345-1 | 1 |
| 14 | | is_human | 1 |
| 15 | | client_width | 1024 |
| 16 | | _ga | GA1.2.1257362257.1598505211 |
| 17 | | _gid | GA1.2.1570412355.1598505011 |
| 18 | | _gat_UA-168657910-1 | 1 |
| 20 | | NID | [illegible] |

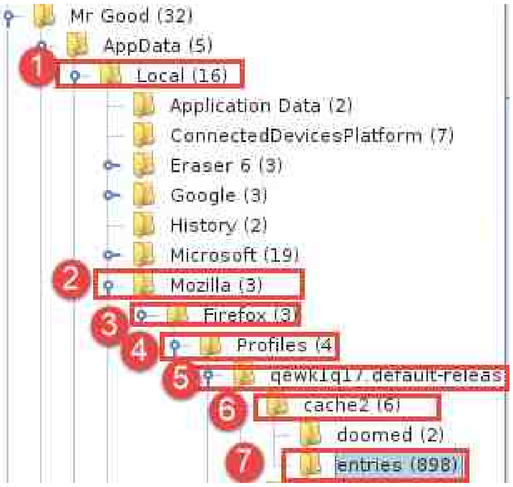
| | |
|---|---|
| id | This column is the sequential order in which  each cookie was added. |
| Name | This is the name of the cookie. |
| Value | This is the data stored inside the cookie and can vary based on the website and the type of cookie it is. |
| Host | The *host* is the top-level domain of the website that created the cookie. |
| Expiry | The *expiry* is the date and time that the cookie will expire and be deleted from the computer. |
| lastAccessed | The *lastAccessed* column is the date and time the cookie was last accessed by the website. |
| creationTime | The *creationTime* column is the date and time that the cookie was created on the computer. This data is stored in Google Chrome time. |

11. Now let’s check out the Cache folder for Firefox. We mentioned the path above, so let us begin by clicking the blue pin beside Roaming to contract the folders as seen below.



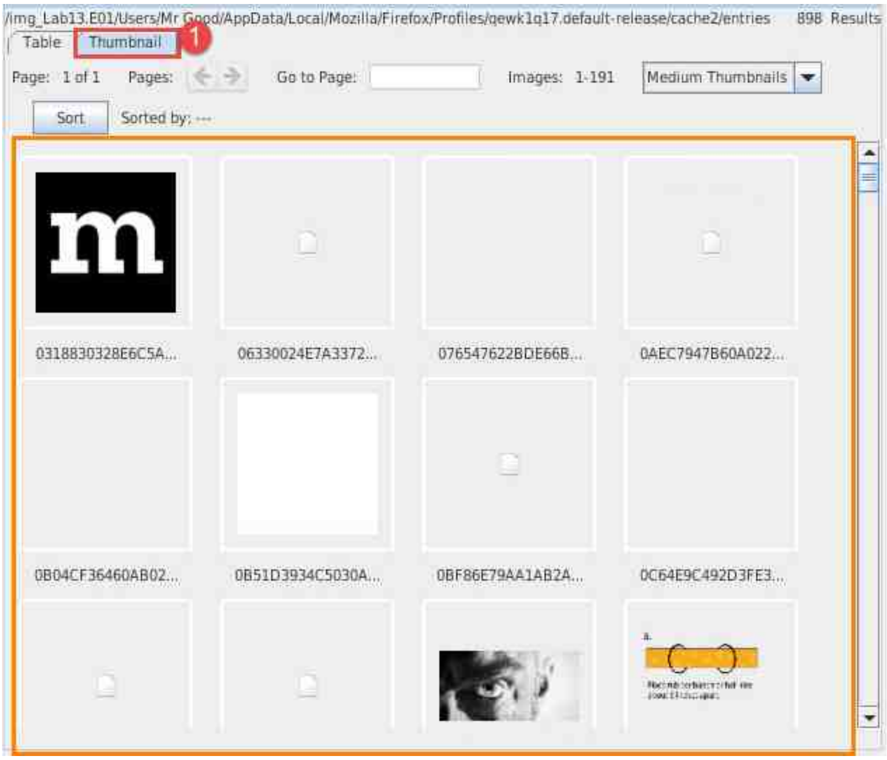
Mr Good (32)
AppData (5)
Local (16)
LocalLow (4)
Roaming (5)
Adobe (3)
Microsoft (12)
Mozilla (5)
Extensions (2)
Firefox (7)
Crash Reports (4)
Pending Pings (2)
Profiles (4)

12. Next, click the blue pins beside the following folders to navigate to the Cache folder: Local > Mozilla > Firefox > Profiles > qewk1q17.default-release > cache2 > entries as seen in items 1 - 7 below.



Mr Good (32)
AppData (5)
Local (16)
Application Data (2)
ConnectedDevicesPlatform (7)
Eraser 6 (3)
Google (3)
History (2)
Microsoft (19)
Mozilla (3)
Firefox (3)
Profiles (4
qewk1q17.default-releas
cache2 (6)
doomed (2)
entries (898)

13. As you can see in the entries folder, there are many cached files. Click the Thumbnail tab highlighted in item 1 below to switch to thumbnail view. This way, you can review pictures that were cached.

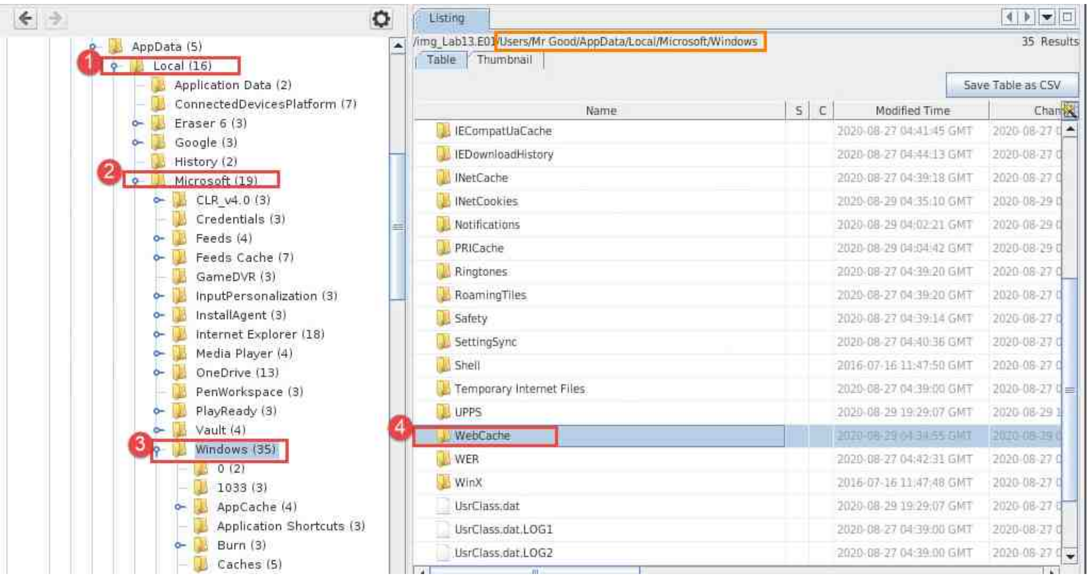


/img_Lab13.E01/Users/Mr Good/AppData/Local/Mozilla/Firefox/Profiles/qewk1q17.default-release/cache2/entries 898 Results

14. Now let's look at the artifacts for the Internet Explorer (IE) browser.

## 3 Learn What Files (and Folders) are Associated with Internet Explorer Web History

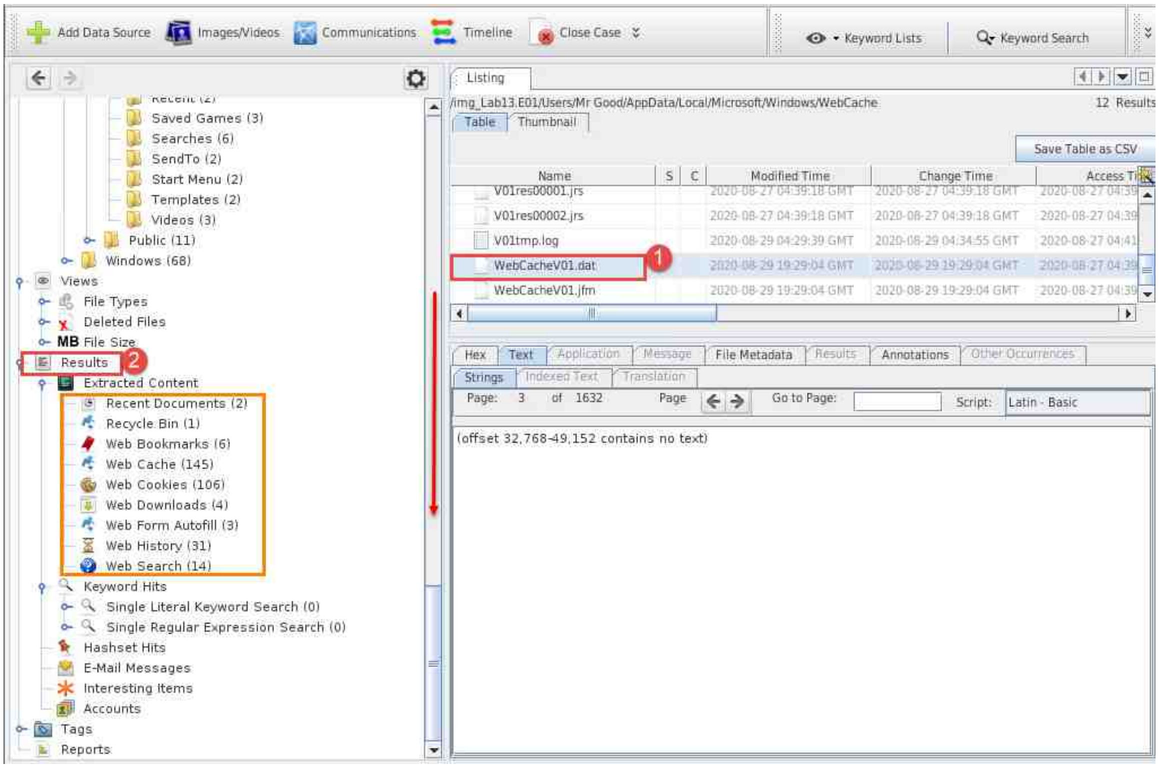
1. The Internet Explorer web browser is another very common web browser and stores just as much data as the other web browsers. Also, like the other browsers, the data for Internet Explorer is located in a different path. Let’s begin by contracting the previously expanded folders.
2. Unlike the other browsers, the history, cookies, and cache are stored in different folders. We will navigate to each by starting with the history file. To do this, click the blue pins beside the following folders to expand them and navigate to the WebCache folder, Local > Microsoft > Windows > WebCache, as seen in items 1 - 4 below.



/img_Lab13.E01/Users/Mr Good/AppData/Local/Microsoft/Windows 35 Results

| Name | S | C | Modified Time | Chan |
|---|---|---|---|---|
| IECompatUaCache | | | 2020-08-27 04:41:45 GMT | 2020-08-27 0 |
| IEDownloadHistory | | | 2020-08-27 04:44:13 GMT | 2020-08-27 0 |
| INetCache | | | 2020-08-27 04:39:18 GMT | 2020-08-27 0 |
| INetCookies | | | 2020-08-29 04:35:10 GMT | 2020-08-29 0 |
| Notifications | | | 2020-08-29 04:02:21 GMT | 2020-08-29 0 |
| PRICache | | | 2020-08-29 04:04:42 GMT | 2020-08-29 0 |
| Ringtones | | | 2020-08-27 04:39:20 GMT | 2020-08-27 0 |
| RoamingTiles | | | 2020-08-27 04:39:20 GMT | 2020-08-27 0 |
| Safety | | | 2020-08-27 04:39:14 GMT | 2020-08-27 0 |
| SettingSync | | | 2020-08-27 04:40:36 GMT | 2020-08-27 0 |
| Shell | | | 2016-07-16 11:47:50 GMT | 2020-08-27 0 |
| Temporary Internet Files | | | 2020-08-27 04:39:00 GMT | 2020-08-27 0 |
| UPPS | | | 2020-08-29 19:29:07 GMT | 2020-08-29 1 |
| WebCache | | | 2020-08-29 04:34:55 GMT | 2020-08-29 0 |
| WER | | | 2020-08-27 04:42:31 GMT | 2020-08-27 0 |
| WinX | | | 2016-07-16 11:47:48 GMT | 2020-08-27 0 |
| UsrClass.dat | | | 2020-08-29 19:29:07 GMT | 2020-08-27 0 |
| UsrClass.dat.LOG1 | | | 2020-08-27 04:39:00 GMT | 2020-08-27 0 |
| UsrClass.dat.LOG2 | | | 2020-08-27 04:39:00 GMT | 2020-08-27 0 |

3. Once there, click the file called WebCacheV01.dat as seen in item 1 below. This is an ESE database file that is used to store the web history for IE. This file can be exported and parsed using an ESE database viewer. However, the Recent Activity Ingest Module already parsed this file for us. You can browse through the results by clicking the arrows seen in item 2 below. The table below the following screenshot outlines the meanings of the rows.

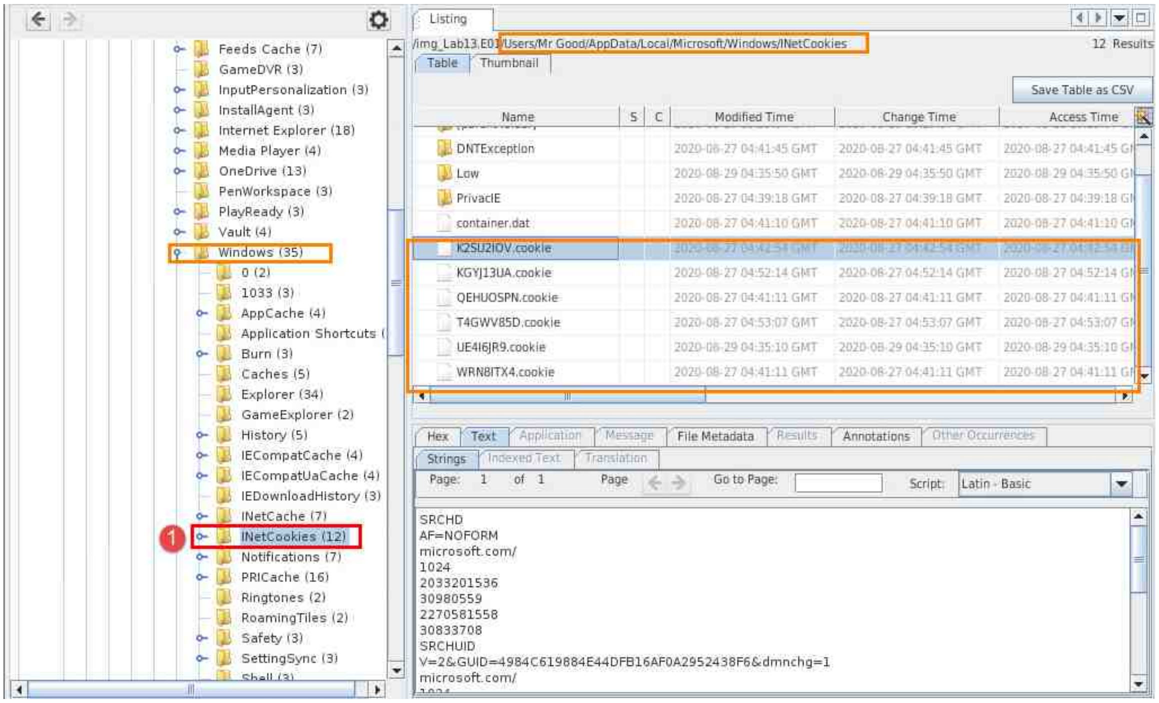


| Name | S | C | Modified Time | Change Time | Access Ti |
|---|---|---|---|---|---|
| V01res00001.jrs | | | 2020-08-27 04:39:18 GMT | 2020-08-27 04:39:18 GMT | 2020-08-27 04:39 |
| V01res00002.jrs | | | 2020-08-27 04:39:18 GMT | 2020-08-27 04:39:18 GMT | 2020-08-27 04:39 |
| V01tmp.log | | | 2020-08-29 04:29:39 GMT | 2020-08-29 04:34:55 GMT | 2020-08-27 04:41 |
| WebCacheV01.dat | | | 2020-08-29 19:29:04 GMT | 2020-08-29 19:29:04 GMT | 2020-08-27 04:39 |
| WebCacheV01.jfm | | | 2020-08-29 19:29:04 GMT | 2020-08-29 19:29:04 GMT | 2020-08-27 04:39 |

(offset 32,768-49,152 contains no text)

| | |
|---|---|
| URL | This is the specific URL that was visited |
| Referrer URL | This is populated if the user accessed this URL from another one |
| Title | This is the name of the webpage |
| Program Name | This is the name of the program that the data is associated with |
| Domain | This is the top-level domain name for the website |
| Username | This is the name of the user that accessed the webpage |
| Source File | The Source File path is the name of the file that the data was parsed from |

4. As you saw, the IE history file is structured differently than the other 2 browsers. Now let’s move on to the cookies file. This is located in the folder called INetCookies located within the same Windows folder that you used in step 2 to find the WebCache folder. To access INetCookies, click the folder called INetCookies, as seen in item 1 below. As you can see, the cookies are stored as separate files. The file system Creation, Access, and Modified times can tell you when they were created and last used. Click each one to learn the associated website and possibly the kind of data stored in them.



/img_Lab13.E01/Users/Mr Good/AppData/Local/Microsoft/Windows/INetCookies

12 Results

| Name | S | C | Modified Time | Change Time | Access Time |
|---|---|---|---|---|---|
| DNTException | | | 2020-08-27 04:41:45 GMT | 2020-08-27 04:41:45 GMT | 2020-08-27 04:41:45 GI |
| Low | | | 2020-08-29 04:35:50 GMT | 2020-08-29 04:35:50 GMT | 2020-08-29 04:35:50 GI |
| PrivacIE | | | 2020-08-27 04:39:18 GMT | 2020-08-27 04:39:18 GMT | 2020-08-27 04:39:18 GI |
| container.dat | | | 2020-08-27 04:41:10 GMT | 2020-08-27 04:41:10 GMT | 2020-08-27 04:41:10 GI |
| K2SU2IOV.cookie | | | 2020-08-27 04:42:54 GMT | 2020-08-27 04:42:54 GMT | 2020-08-27 04:42:54 GI |
| KGYJ13UA.cookie | | | 2020-08-27 04:52:14 GMT | 2020-08-27 04:52:14 GMT | 2020-08-27 04:52:14 GI |
| QEHUOSPN.cookie | | | 2020-08-27 04:41:11 GMT | 2020-08-27 04:41:11 GMT | 2020-08-27 04:41:11 GI |
| T4GWV85D.cookie | | | 2020-08-27 04:53:07 GMT | 2020-08-27 04:53:07 GMT | 2020-08-27 04:53:07 GI |
| UE4I6JR9.cookie | | | 2020-08-29 04:35:10 GMT | 2020-08-29 04:35:10 GMT | 2020-08-29 04:35:10 GI |
| WRN8ITX4.cookie | | | 2020-08-27 04:41:11 GMT | 2020-08-27 04:41:11 GMT | 2020-08-27 04:41:11 GI |

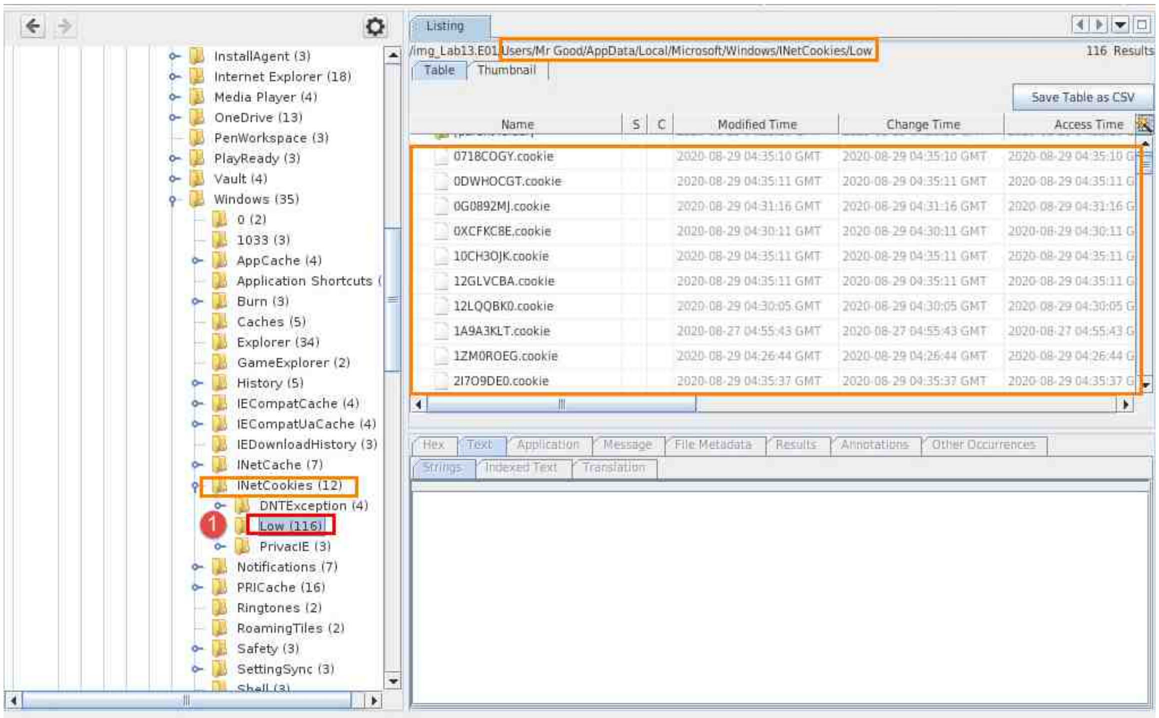
Page: 1 of 1 Page

Go to Page:

Script: Latin - Basic

```
SRCHD
AF=NOFORM
microsoft.com/
1024
2033201536
30980559
2270581558
30833708
SRCHUID
V=2&GUID=4984C619884E44DFB16AF0A2952438F6&dmnchg=1
microsoft.com/
```

5. Click the folder called Low to view the additional cookies, as seen in item 1. They are structured just like the ones from the INetCookies folder.

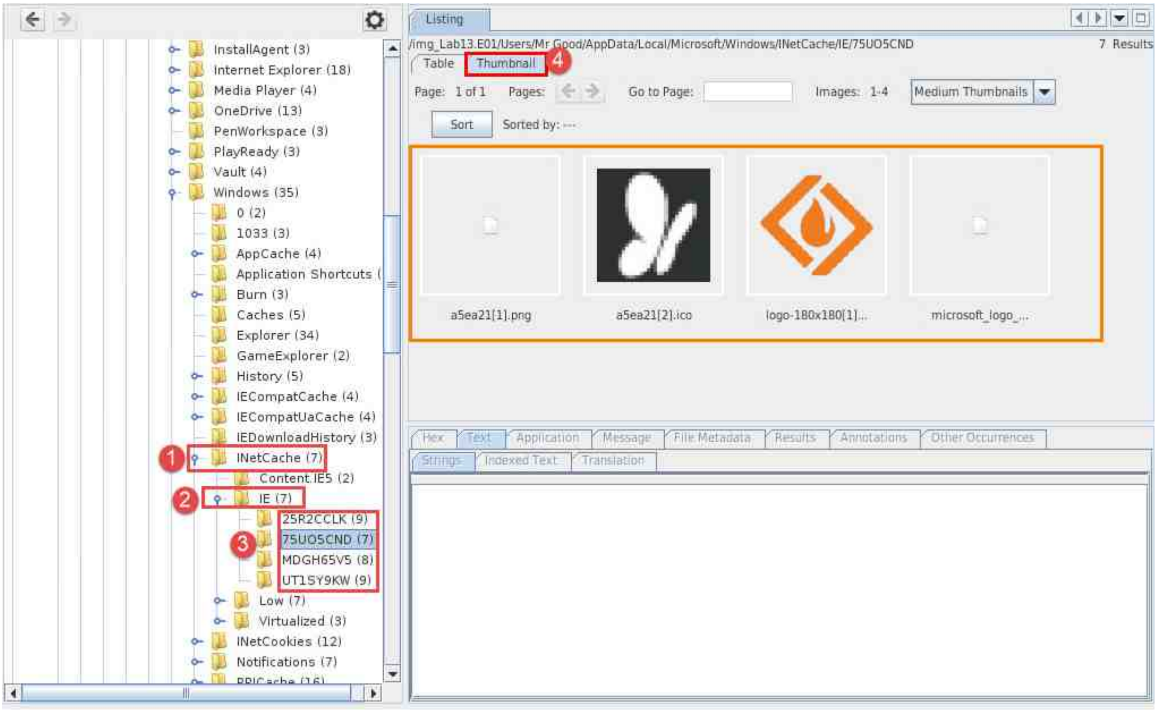


/img_Lab13.E01/Users/Mr Good/AppData/Local/Microsoft/Windows/INetCookies/Low

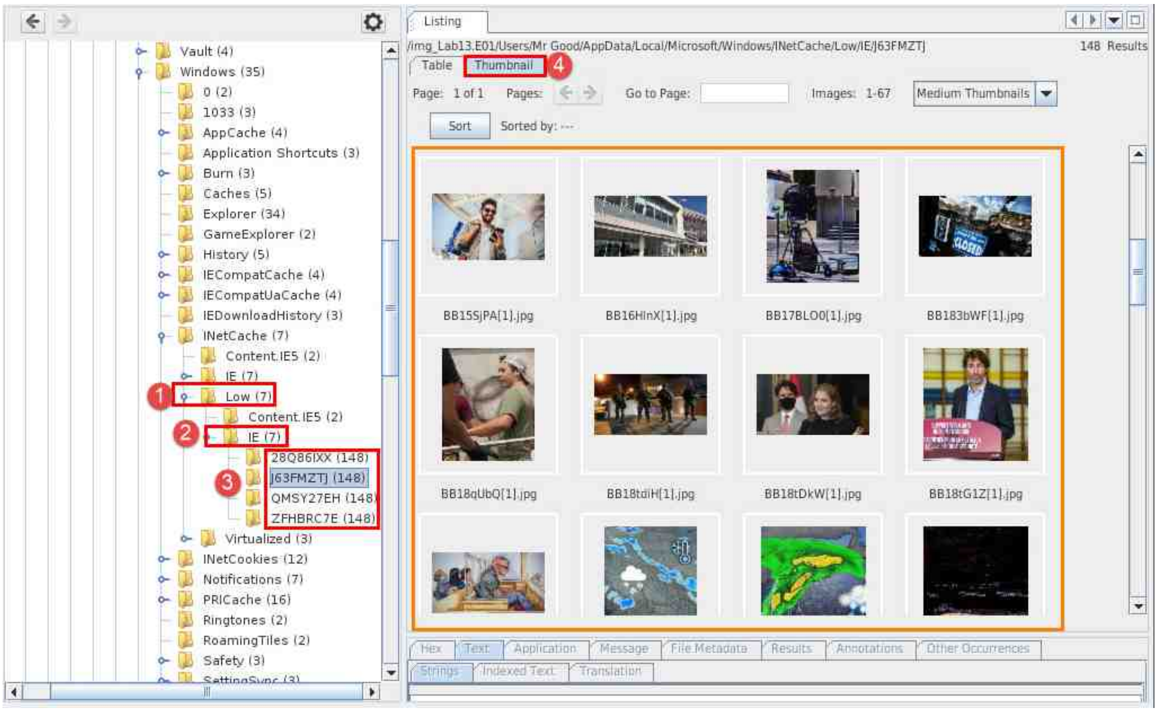
116 Results

| Name | S | C | Modified Time | Change Time | Access Time |
|---|---|---|---|---|---|
| 0718COGY.cookie | | | 2020-08-29 04:35:10 GMT | 2020-08-29 04:35:10 GMT | 2020-08-29 04:35:10 G |
| 0DWHOCGT.cookie | | | 2020-08-29 04:35:11 GMT | 2020-08-29 04:35:11 GMT | 2020-08-29 04:35:11 G |
| 0G0892MJ.cookie | | | 2020-08-29 04:31:16 GMT | 2020-08-29 04:31:16 GMT | 2020-08-29 04:31:16 G |
| 0XCFKC8E.cookie | | | 2020-08-29 04:30:11 GMT | 2020-08-29 04:30:11 GMT | 2020-08-29 04:30:11 G |
| 10CH3OJK.cookie | | | 2020-08-29 04:35:11 GMT | 2020-08-29 04:35:11 GMT | 2020-08-29 04:35:11 G |
| 12GLVCBA.cookie | | | 2020-08-29 04:35:11 GMT | 2020-08-29 04:35:11 GMT | 2020-08-29 04:35:11 G |
| 12LQQBK0.cookie | | | 2020-08-29 04:30:05 GMT | 2020-08-29 04:30:05 GMT | 2020-08-29 04:30:05 G |
| 1A9A3KLT.cookie | | | 2020-08-27 04:55:43 GMT | 2020-08-27 04:55:43 GMT | 2020-08-27 04:55:43 G |
| 1ZM0ROEG.cookie | | | 2020-08-29 04:26:44 GMT | 2020-08-29 04:26:44 GMT | 2020-08-29 04:26:44 G |
| 2I7O9DE0.cookie | | | 2020-08-29 04:35:37 GMT | 2020-08-29 04:35:37 GMT | 2020-08-29 04:35:37 G |

6. Let us look at the web cache for IE. This is located in the folder called INetCache located within the folder called Windows (just as the WebCache and INetCookies folders were). To access it, click the folder called INetCache, as seen in item 1 below. The cached files are stored in 2 main folders. Let's click the blue pin beside the folder called IE, as seen in item 2, and click each of the folders with alphanumeric names to view cached content, as seen in item 3. Unlike the other browsers, this one stores the file extensions for the cached files. You can click the Thumbnail tab to view the pictures, as seen in item 4 below.



7. The second folder is also called IE, but it is found inside the folder called Low. Access the folder by clicking the blue pin beside Low and then clicking  IE, as seen in items 1 and 2 below. As before, the cached files are inside the folders with alphanumeric names. Click each folder and use the Thumbnail tab to review the files.

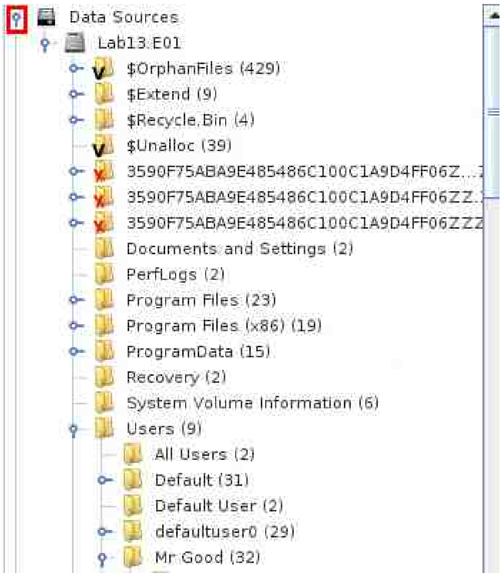


8. As you saw from these 3 exercises, the browser stores tons of data. We reviewed some of the basic ones, but tons more data exist that can help to further investigate and explain. The methods we used are very basic and not often practiced. Most examiners will parse the data and review it automatically. Since we ran the Recent Activity module, Autopsy has the parsed data ready and waiting. Let’s take a look at this data in the final exercise.

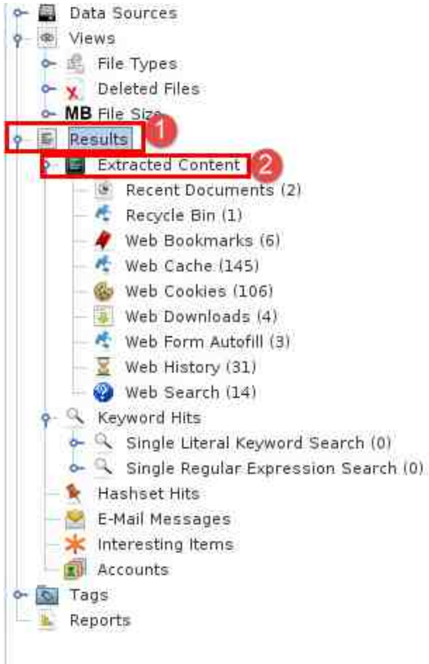
## 4 Reviewing Parsed Browsing Activity in Autopsy

Forensic processing makes examinations quicker and easier to understand. It is important to know where the parsers get their data, which is why we manually visited each location in the previous exercises. This is important as it helps in cross verification. In this exercise, we will quickly look at where Autopsy displays its parsed browsing history, and explain some of the artifacts.

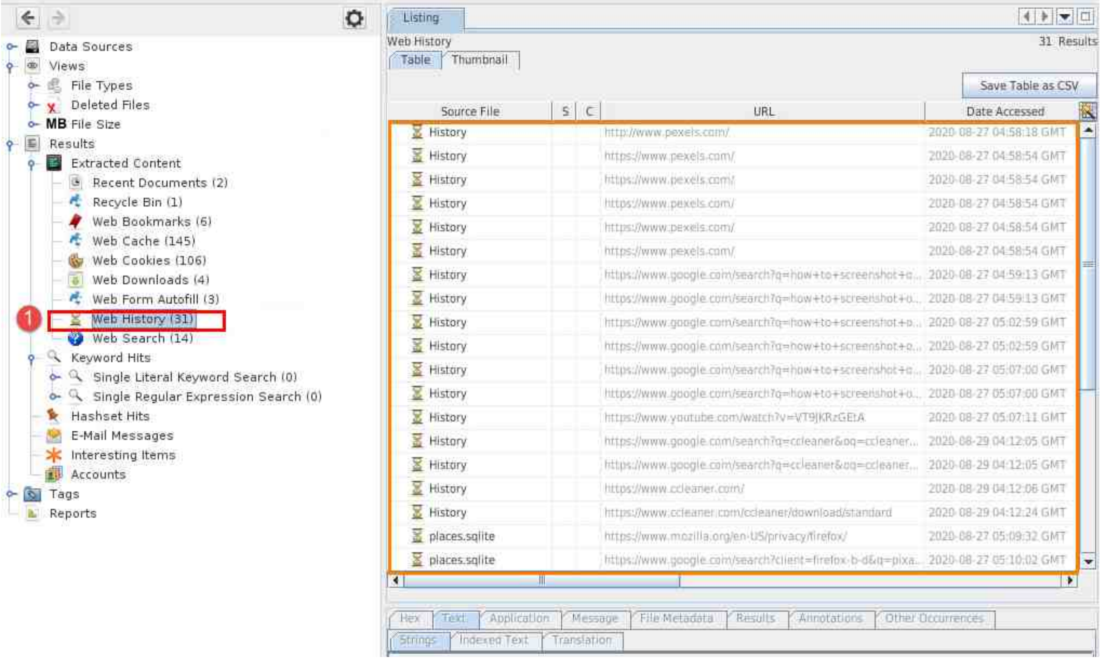
1. Let's begin by clicking the blue pin beside Data Sources, as seen below, to contract the tree and make it more manageable.



2. Now, click the blue pin beside Results and then click Extracted Content, as seen in items 1 and 2 below. As you can see in the list that appears, the parsed data is categorized based on data type.

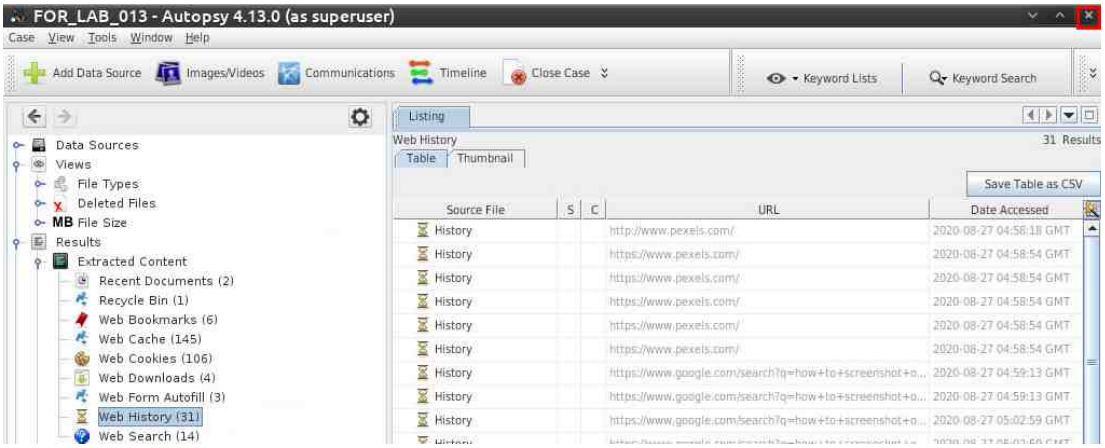


3. Let's click on the Web History option, as seen in item 1, below. This will provide the aggregated list of all the web history found on the drive from the sources we visited earlier. The good thing about this is that the date and time are already parsed, unlike in the database view.



| Source File | S | C | URL | Date Accessed |
|---|---|---|---|---|
| History | | | http://www.pexels.com/ | 2020-08-27 04:58:18 GMT |
| History | | | https://www.pexels.com/ | 2020-08-27 04:58:54 GMT |
| History | | | https://www.pexels.com/ | 2020-08-27 04:58:54 GMT |
| History | | | https://www.pexels.com/ | 2020-08-27 04:58:54 GMT |
| History | | | https://www.pexels.com/ | 2020-08-27 04:58:54 GMT |
| History | | | https://www.pexels.com/ | 2020-08-27 04:58:54 GMT |
| History | | | https://www.google.com/search?q=how+to+screenshot+o... | 2020-08-27 04:59:13 GMT |
| History | | | https://www.google.com/search?q=how+to+screenshot+o... | 2020-08-27 04:59:13 GMT |
| History | | | https://www.google.com/search?q=how+to+screenshot+o... | 2020-08-27 05:02:59 GMT |
| History | | | https://www.google.com/search?q=how+to+screenshot+o... | 2020-08-27 05:02:59 GMT |
| History | | | https://www.google.com/search?q=how+to+screenshot+o... | 2020-08-27 05:07:00 GMT |
| History | | | https://www.google.com/search?q=how+to+screenshot+o... | 2020-08-27 05:07:00 GMT |
| History | | | https://www.youtube.com/watch?v=VT9jKRzGEtA | 2020-08-27 05:07:11 GMT |
| History | | | https://www.google.com/search?q=ccleaner&oq=ccleaner... | 2020-08-29 04:12:05 GMT |
| History | | | https://www.google.com/search?q=ccleaner&oq=ccleaner... | 2020-08-29 04:12:05 GMT |
| History | | | https://www.ccleaner.com/ | 2020-08-29 04:12:06 GMT |
| History | | | https://www.ccleaner.com/ccleaner/download/standard | 2020-08-29 04:12:24 GMT |
| places.sqlite | | | https://www.mozilla.org/en-US/privacy/firefox/ | 2020-08-27 05:09:32 GMT |
| places.sqlite | | | https://www.google.com/search?client=firefox-b-d&q=pixa... | 2020-08-27 05:10:02 GMT |

4. Please feel free to look at the other categories to see how they match up with the data we found in the tables when manually parsing them.
5. You are now at the end of this lab. Close Autopsy by clicking the X at the top-right corner, as seen below.



| Source File | S | C | URL | Date Accessed |
|---|---|---|---|---|
| History | | | http://www.pexels.com/ | 2020-08-27 04:58:18 GMT |
| History | | | https://www.pexels.com/ | 2020-08-27 04:58:54 GMT |
| History | | | https://www.pexels.com/ | 2020-08-27 04:58:54 GMT |
| History | | | https://www.pexels.com/ | 2020-08-27 04:58:54 GMT |
| History | | | https://www.pexels.com/ | 2020-08-27 04:58:54 GMT |
| History | | | https://www.pexels.com/ | 2020-08-27 04:58:54 GMT |
| History | | | https://www.google.com/search?q=how+to+screenshot+o... | 2020-08-27 04:59:13 GMT |
| History | | | https://www.google.com/search?q=how+to+screenshot+o... | 2020-08-27 04:59:13 GMT |
| History | | | https://www.google.com/search?q=how+to+screenshot+o... | 2020-08-27 05:02:59 GMT |