



FORENSICS LAB SERIES

Lab 9: Web Browser Forensics

| |
|---|
| Material in this Lab Aligns to the Following Certification Domains/Objectives |
| GIAC Certified Forensics Examiner (GCFE) Domains |
| 1: Browser Forensics |

Document Version: 2016-08-17

Contents

| | |
|--|----|
| Introduction | 3 |
| Objective | 3 |
| Pod Topology | 4 |
| Lab Settings | 5 |
| 1 Mozilla Firefox Browser Forensics | 6 |
| 2 Google Chrome Browser Forensics..... | 14 |

Introduction

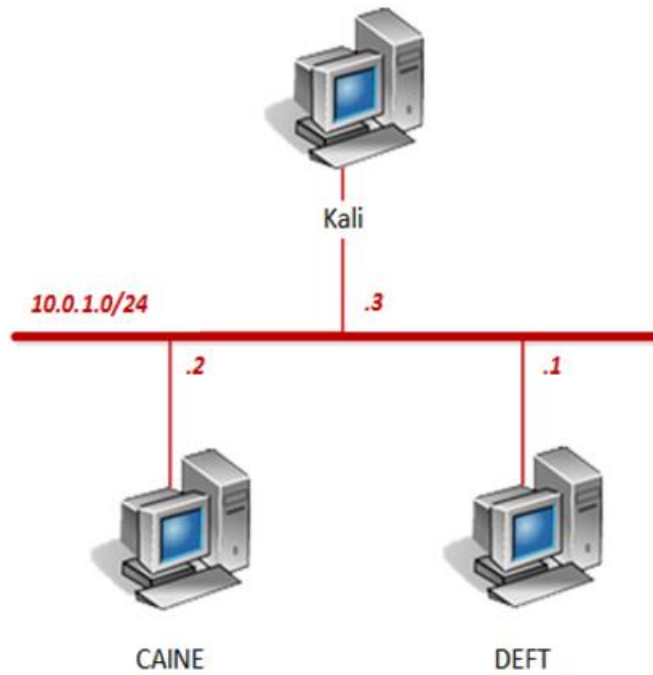
This lab will introduce the basics of Internet browser forensics. Web browsers such as Mozilla Firefox and Google Chrome store their data in SQLite databases that can be examined with a SQL browser.

Objective

In this lab, you will be conducting forensic practices using various tools. You will be performing the following tasks:

1. Mozilla Firefox Browser Forensics
2. Google Chrome Browser Forensics

Pod 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 | Account (if needed) | Password (if needed) |
|-----------------|------------|------------------------|-------------------------|
| DEFT | 10.0.1.1 | deft | password |
| CAINE | 10.0.1.2 | caine | |
| Kali | 10.0.1.3 | root | toor |

1 Mozilla Firefox Browser Forensics

1. Click on the **CAINE** graphic on the *topology page* to open the VM.
2. Open a new terminal by clicking on the **MATE Terminal** icon located in the bottom tool pane.



3. Identify the hidden files and directories from the *Home* directory. Enter the command below followed by pressing the **Enter** key.

```
ls -a
```

```
caine@Caine01:~$ ls -a
.                  .gconf             .profile           Videos
..                 .gimp-2.8          Public            .wine
.bash_history      .gksu.lock         .pureadminrc      .wireshark
.bash_logout       .gnupg            .putty            .wxHexEditor
.bashrc            .gvfs              .python_history   .x11vnc.log.caine:5900
.cache             .ICEauthority      qphotorec.log     .x11vnc.log.caine:5980
.compiz            .icons             .remmina          .Xauthority
.config            .java              .save_dir         .Xdefaults
.cpan              .kde               .ssh              .xinputrc
.dbus              .local             Templates         .xsession-errors
Desktop            .mobiusft          .themes           .xsession-errors.old
.dmrc              .mozilla           .thumbnails       .zenmap
.Documents         Music              .tkcvs            .zuluCrypt
.Downloads         Pictures           .tkcvs-picklists  .zuluCrypt-socket
.dvdisaster        .pip               .TrueCrypt
.fred              .PlayOnLinux      Ubuntu
```

Notice the *“.mozilla”* directory. This is where *Mozilla Firefox* keeps all of its data.

4. Enter the command below to change to the *.mozilla* directory.

```
cd .mozilla
```

```
caine@Caine01:~$ cd .mozilla
caine@Caine01:~/.mozilla$
```

5. List the current files and directors by entering the command below.

```
ls -a
```

```
caine@Caine01:~/.mozilla$ ls -a
.  ..  extensions  firefox
caine@Caine01:~/.mozilla$
```

6. Move further down the directory tree by entering the command below.

```
cd firefox
```

```
caine@Caine01:~/.mozilla$ cd firefox
caine@Caine01:~/.mozilla/firefox$
```

7. Again, identify the files and directories in the current directory. Enter the command below.

```
ls -a
```

```
caine@Caine01:~/.mozilla/firefox$ ls -a
.  ..  Crash Reports  e50tmmfs.default  profiles.ini
caine@Caine01:~/.mozilla/firefox$
```

Notice the randomly generated directory by Firefox, “*e50tmmfs.default*”.

8. Navigate to the directory with the randomly generated number. Enter the command below.

```
cd e50tmmfs.default
```

```
caine@Caine01:~/.mozilla/firefox$ cd e50tmmfs.default
caine@Caine01:~/.mozilla/firefox/e50tmmfs.default$
```

9. Identify all files and directories by entering the command below.

```
ls -a
```

```
caine@Caine01:~/.mozilla/firefox/e50tmmfs.default$ ls -a
.          features          revocations.txt
..         formhistory.sqlite  saved-telemetry-pings
addons.json gmp                       search.json
blocklist.xml gmp-gmpopenh264         search.json.mozlz4
bookmarkbackups healthreport             search-metadata.json
cert8.db     Invalidprefs.js         secmod.db
compatibility.ini key3.db                 sessioncheckpoints.json
content-prefs.sqlite localstore.rdf          sessionstore-backups
cookies.sqlite logins.json             sessionstore.js
cookies.sqlite.bak mimeTypees.rdf          SiteSecurityServiceState.txt
crashes      minidumps              storage
datareporting .parentlock            times.json
enumerate_devices.txt permissions.sqlite      webapps
extensions    places.sqlite          webappsstore.sqlite
extensions.ini pluginreg.dat          xulstore.json
extensions.json prefs.js
caine@Caine01:~/.mozilla/firefox/e50tmmfs.default$
```

Notice several *SQLite* databases in the directory with the “.sqlite” extension. This is where the *userdata*, among other items are stored.

10. Copy the files with the .sqlite extension in the current directory to the *home* directory for examination purposes. Enter the command below.

```
cp *.sqlite /home/caine
```

```
caine@Caine01:~/.mozilla/firefox/e50tmmfs.default$ cp *.sqlite /home/caine
caine@Caine01:~/.mozilla/firefox/e50tmmfs.default$
```

11. Enter the command below to change to the *home* directory for *caine*.

```
cd
```

```
caine@Caine01:~/.mozilla/firefox/e50tmmfs.default$ cd
caine@Caine01:~$
```

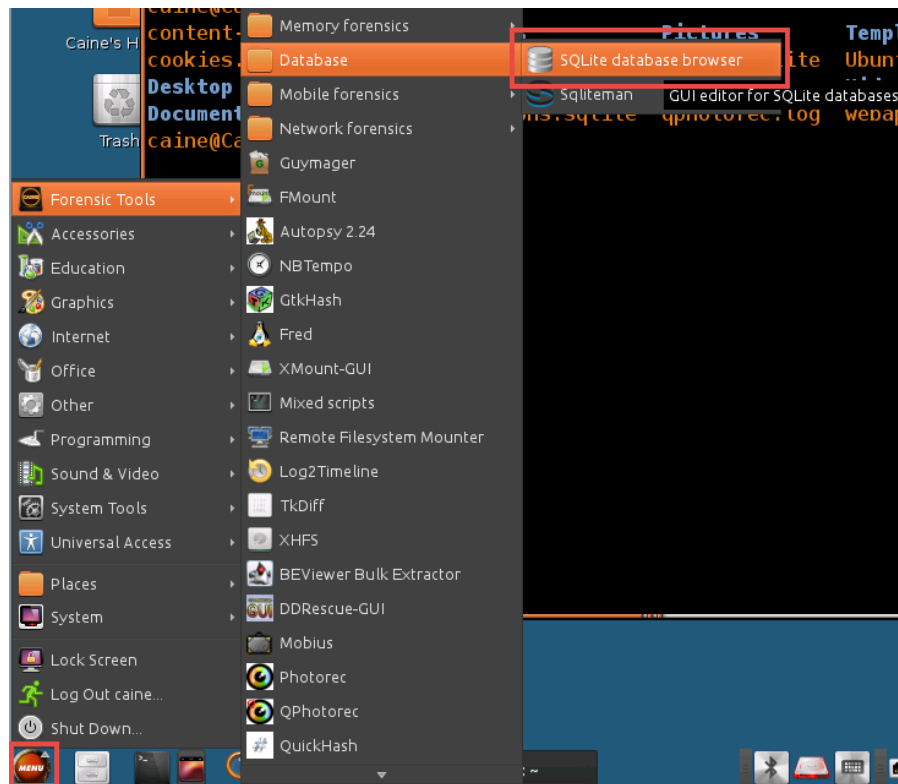

12. List the files in the current directory. Enter the command below.

```
ls
```

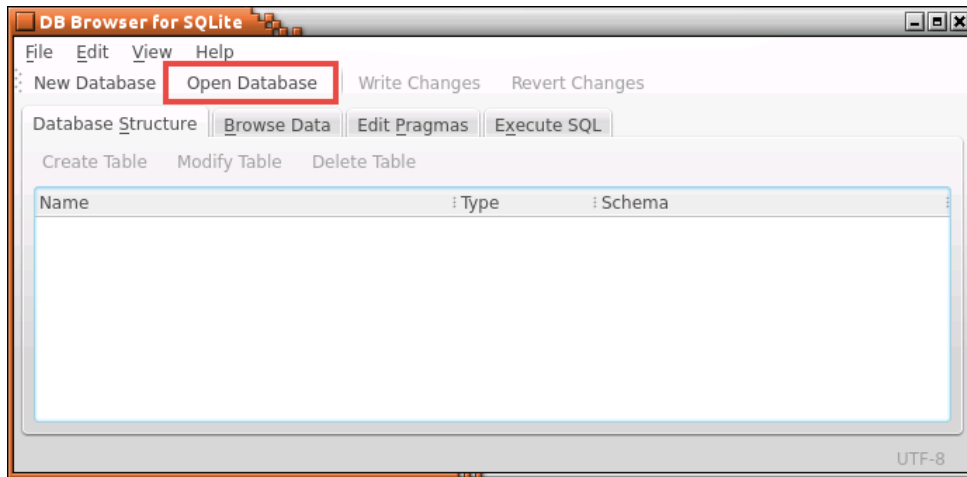
```
caine@Caine01:~$ ls
content-prefs.sqlite  Downloads  Pictures  Templates
cookies.sqlite        formhistory.sqlite  places.sqlite  Ubuntu
Desktop              Music      Public    Videos
Documents             permissions.sqlite  qphotorec.log  webappsstore.sqlite
caine@Caine01:~$
```

Notice all files with the *.sqlite* extension have been copied over.

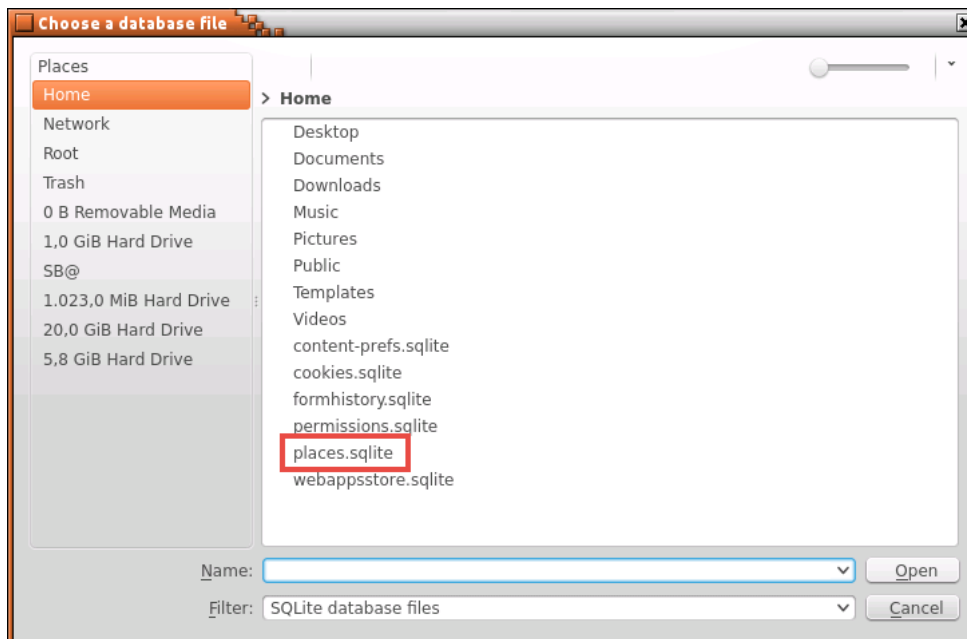
13. Navigate to **Menu > Forensic Tools > Database > SQLite database browser** to open the *SQLite* database reader.



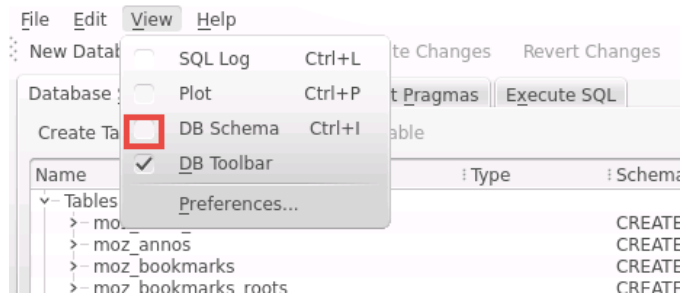
14. In the *SQLite* window, click on **Open Database**.



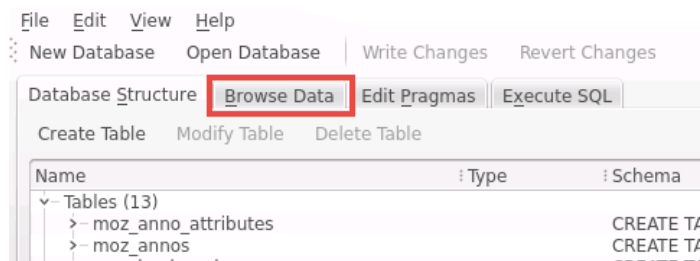
15. In the *Choose a database file* window, select **places.sqlite** from the *Home* directory.



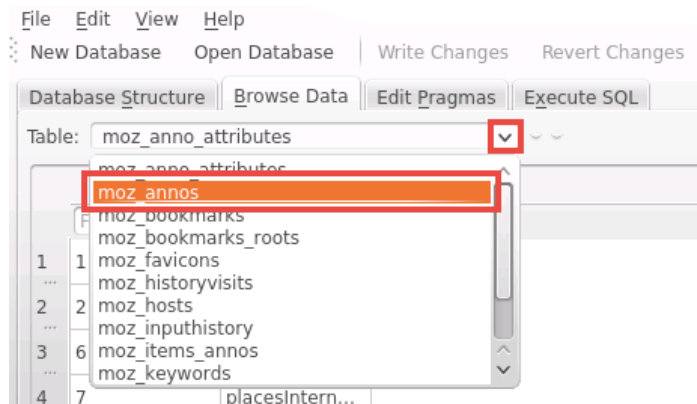
16. Verify that the *DB Schema* is disabled from the view by clicking on **View** and unchecking the **DB Schema** checkbox.



17. Click on the **Browse Data** tab.



18. In this view, various tables in the database can be explored. Begin exploring metadata in the *moz_annos* table. Click on the **drop-down menu** next to *Table:* and select **moz_annos**.





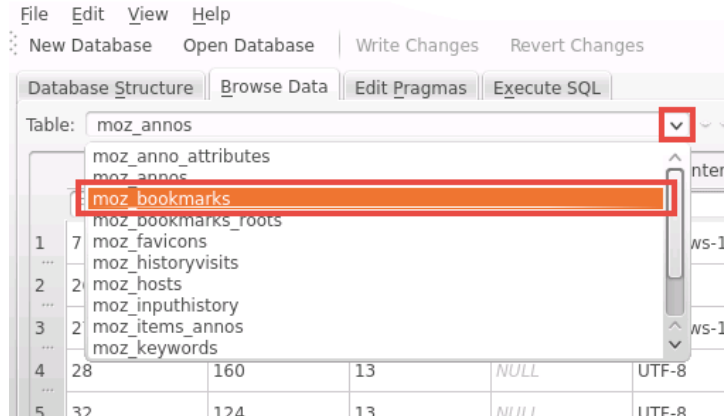
19. In this table, there is metadata available for various downloads and files that were executed by the web browser. The *content* column contains some of the information. Notice the dates are stored in *WebKit* time (number of microseconds since *01/01/1601 00:00:00 UTC* represents in 64-bit integers).

Table: moz_annos New Record Delete Record

| | id | place_id | ino_attribute_id | mime_type | content | flags | expiration | type | dateAdded | lastM |
|---|----|----------|------------------|-----------|-------------------|-------|------------|------|---------------|-------|
| 1 | 7 | 78 | 13 | NULL | windows-1252 | 0 | 4 | 3 | 1420025841... | 14200 |
| 2 | 26 | 102 | 13 | NULL | UTF-8 | 0 | 4 | 3 | 1420108629... | 14201 |
| 3 | 27 | 96 | 13 | NULL | windows-1252 | 0 | 4 | 3 | 1420108632... | 14201 |
| 4 | 28 | 160 | 13 | NULL | UTF-8 | 0 | 4 | 3 | 1420112930... | 14201 |
| 5 | 32 | 124 | 13 | NULL | UTF-8 | 0 | 4 | 3 | 1420201517... | 14202 |
| 6 | 33 | 170 | 14 | NULL | file:///home/c... | 0 | 5 | 3 | 1462133119... | 14621 |
| 7 | 34 | 170 | 15 | NULL | vol3-D..Syste... | 0 | 5 | 3 | 1462133119... | 14621 |
| 8 | 35 | 170 | 16 | NULL | {"state":1,"e... | 0 | 5 | 3 | 1462133119... | 14621 |

To convert *WebKit* time, use conversion websites such as, <http://www.epochconverter.com/webkit>.

20. Using the *SQLite* application, change to another table. Click on the **drop-down menu** located next to *Table:* and select **moz_bookmarks**.

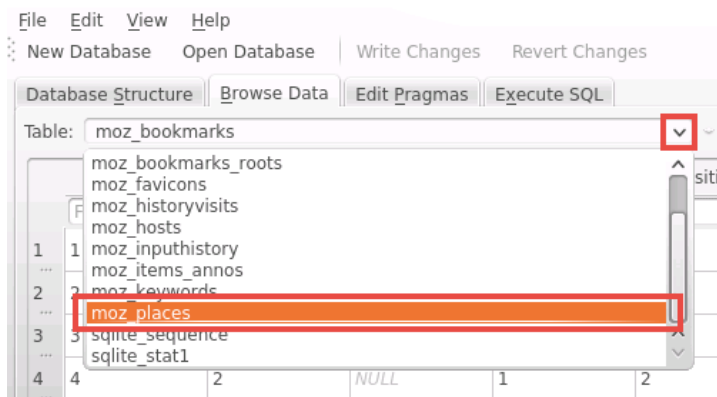




21. Briefly analyze through the titles of the bookmarks underneath the *title* column. Notice the bookmarks from *Mozilla* that are present.

| | id | type | fk | parent | position | title | keyword_id | folder_type | |
|---|--------|--------|--------|--------|----------|-------------------------|------------|-------------|----|
| | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | |
| 1 | 1 | 2 | NULL | 0 | 0 | | NULL | NULL | 14 |
| 2 | 2 | 2 | NULL | 1 | 0 | Bookmarks Menu | NULL | NULL | 14 |
| 3 | 3 | 2 | NULL | 1 | 1 | Bookmarks Toolbar | NULL | NULL | 14 |
| 4 | 4 | 2 | NULL | 1 | 2 | Tags | NULL | NULL | 14 |
| 5 | 5 | 2 | NULL | 1 | 3 | Unsorted Bookmarks | NULL | NULL | 14 |
| 6 | 6 | 1 | 1 | 3 | 1 | Getting Started | NULL | NULL | 14 |
| 7 | 7 | 2 | NULL | 2 | 3 | Ubuntu and Free Soft... | NULL | NULL | 14 |
| 8 | 8 | 1 | 2 | 7 | 0 | Ubuntu | NULL | NULL | 14 |
| 9 | 9 | 1 | 3 | 7 | 1 | Ubuntu Wiki (commu... | NULL | NULL | 14 |

22. Identify the user history left on the system. Change the database table by clicking on the **drop-down menu** next to *Table:* and select **moz_places**.

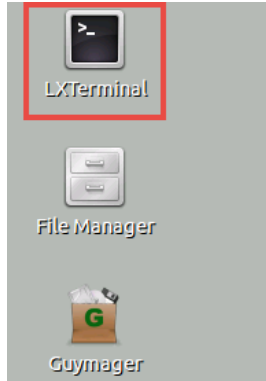


23. Briefly analyze through the web history underneath the *url* column. Notice the various URLs in *Mozilla's* history.

| | id | url | title | rev_host | visit_count | hidden | typ |
|---|--------|--|-----------------|------------------|-------------|--------|--------|
| | Filter | Filter | Filter | Filter | Filter | Filter | Filter |
| 1 | 1 | https://www.mozilla.org/en-US/firefox/central/ | NULL | gro.allizom.w... | 0 | 0 | 0 |
| 2 | 2 | http://www.ubuntu.com/ | The leading ... | moc.utnubu... | 0 | 0 | 0 |
| 3 | 3 | http://wiki.ubuntu.com/ | NULL | moc.utnubu.i... | 0 | 0 | 0 |
| 4 | 4 | https://answers.launchpad.net/ubuntu/+addqu... | NULL | ten.daphcnu... | 0 | 0 | 0 |
| 5 | 5 | http://www.debian.org/ | NULL | gro.naibed.w... | 0 | 0 | 0 |
| 6 | 6 | https://one.ubuntu.com/ | NULL | moc.utnubu... | 0 | 0 | 0 |
| 7 | 7 | https://www.mozilla.org/en-US/firefox/help/ | NULL | gro.allizom.w... | 0 | 0 | 0 |
| 8 | 8 | https://www.mozilla.org/en-US/firefox/customize/ | NULL | gro.allizom.w... | 0 | 0 | 0 |
| 9 | 9 | https://www.mozilla.org/en-US/contribute/ | NULL | gro.allizom.w... | 0 | 0 | 0 |

2 Google Chrome Browser Forensics

1. Click on the **DEFT** graphic on the *topology page* to open the VM.
2. Open a new terminal by clicking on the **LXTerminal** icon located on the *Desktop*.



3. Using the terminal, list all the files and directories in the `/home/deft/` directory. Enter the command below.

```
ls -a
```

```
deft-virtual-machine ~ % ls -a
.          Documents      .local        .pulse
..         Downloads     .macromedia  .pulse-cookie
.adobe     evidence          .mountmanager .ssh
.android   .gconf            .mozilla     Templates
.ant       .gksu.lock        .mtpaint     .thumbnails
.bash_history .gnome           Music        Videos
.bashrc    .gstreamer-0.10  NewFolder    .vim
.cache     .gtk-bookmarks   pdfcrack-01.5 .viminfo
.config    .icons           .pip         .Xauthority
.dbus      .java            .pki         .xscreensaver
.Desktop   .lessht         .profile     .xsession-errors
.dmrc      .libnet-openssh-perl Public        .xsession-errors.old
deft-virtual-machine ~ %
```

4. Notice the hidden files and directories. Navigate to the **.config/** directory by entering the command below.

```
cd .config
```

```
deft-virtual-machine ~ % cd .config/
deft-virtual-machine ~/.config %
```

- Enter the command below to list files and directories in a list view in the current directory.

```
ls -l
```

```
deft-virtual-machine ~/.config % ls -l
total 100
drwx----- 2 deft deft 4096 Jul 11 17:21 dconf
drwx----- 10 deft deft 4096 Apr 25 07:27 google-chrome
drwxrw-r-- 2 deft deft 4096 Apr 20 11:56 gpview
drwx----- 2 deft deft 4096 Apr 25 09:04 gtk-2.0
drwx----- 2 deft deft 4096 Nov 19 2015 gtk-3.0
drwx----- 2 deft deft 4096 Nov 19 2015 htop
drwx----- 2 deft deft 4096 Nov 19 2015 leafpad
drwx----- 2 deft deft 4096 Nov 19 2015 libfm
drwxrwxr-x 3 deft deft 4096 Apr 20 11:13 libreoffice
drwxrwxr-x 4 deft deft 4096 May 10 18:40 lsc
-rw-r--r-- 1 deft deft 58 Nov 19 2015 lxkeymap.cfg
drwx----- 3 deft deft 4096 Nov 19 2015 lxpanel
drwx----- 3 deft deft 4096 Nov 19 2015 lxsession
drwx----- 2 deft deft 4096 Nov 19 2015 lxterminal
drwx----- 3 deft deft 4096 Apr 19 13:49 menus
drwx----- 2 deft deft 4096 Nov 19 2015 openbox
drwx----- 3 deft deft 4096 Nov 19 2015 pcmanfm
-rw-r--r-- 1 deft deft 8119 Apr 6 12:46 Trolltech.conf
drwx----- 2 deft deft 4096 Nov 19 2015 update-notifier
-rw----- 1 deft deft 624 Nov 19 2015 user-dirs.dirs
-rw-r--r-- 1 deft deft 5 Nov 19 2015 user-dirs.locale
drwxr-xr-x 2 deft deft 4096 Nov 19 2015 Vialinx
drwxr-xr-x 2 deft deft 4096 Nov 19 2015 vlc
drwx----- 3 deft deft 4096 Nov 19 2015 xfce4
deft-virtual-machine ~/.config %
```

- Enter the command below to navigate into the google-chrome directory.

```
cd google-chrome
```

```
deft-virtual-machine ~/.config % cd google-chrome
deft-virtual-machine ~/.config/google-chrome %
```

- List the files and directories by entering the command below.

```
ls
```

```
deft-virtual-machine ~/.config/google-chrome % ls
Avatars Safe Browsing Bloom Prefix Set
Certificate Revocation Lists Safe Browsing Cookies
Channels Safe Browsing Cookies-journal
chrome_shutdown_ms.txt Safe Browsing Csd Whitelist
Crash Reports Safe Browsing Download
Default Safe Browsing Download Whitelist
Dictionaries Safe Browsing Extension Blacklist
EVWhitelist Safe Browsing Inclusion Whitelist
First Run Safe Browsing IP Blacklist
Local State Safe Browsing UwS List
PepperFlash Safe Browsing UwS List Prefix Set
pnacl ShaderCache
Safe Browsing Bloom
deft-virtual-machine ~/.config/google-chrome %
```

8. Navigate to the Default directory to access the databases.

```
cd Default
```

```
deft-virtual-machine ~/.config/google-chrome % cd Default
deft-virtual-machine ../google-chrome/Default %
```

9. List the files and directories in the current directory.

```
ls
```

```
deft-virtual-machine ../google-chrome/Default % ls
Application Cache      GPUCache              Pepper Data
Bookmarks              History               Preferences
Bookmarks.bak          History-journal        QuotaManager
Cookies                History Provider Cache QuotaManager-journal
Cookies-journal        IndexedDB              README
Current Session        Last Session           Secure Preferences
Current Tabs            Last Tabs              Service Worker
databases               Local Extension Settings Session Storage
data_reduction_proxy_leveldb Local Storage           Shortcuts
Extension Cookies       Login Data             Shortcuts-journal
Extension Cookies-journal Login Data-journal      Top Sites
Extensions              Network Action Predictor Top Sites-journal
Extension State          Network Action Predictor-journal TransportSecurity
Favicons                Network Persistent State Visited Links
Favicons-journal        Origin Bound Certs     Web Data
File System              Origin Bound Certs-journal Web Data-journal
deft-virtual-machine ../google-chrome/Default %
```

10. Copy the *SQLite* databases to the Home directory. Start with the **History** database by entering the command below.

```
sudo cp History /home/deft/
```

```
deft-virtual-machine ../google-chrome/Default % sudo cp History /home/deft/
[sudo] password for deft:
deft-virtual-machine ../google-chrome/Default %
```

If prompted for a password, type **password** followed by pressing the **Enter** key.

11. Enter the command below to copy the **Cookies** database to the *Home* directory.

```
sudo cp Cookies /home/deft/
```

```
deft-virtual-machine ../google-chrome/Default % sudo cp Cookies /home/deft/
deft-virtual-machine ../google-chrome/Default %
```

If prompted for a password, type **password** followed by pressing the **Enter** key.

12. Copy the **Top Sites** database to the *home* directory.

```
sudo cp Top\ Sites /home/deft/
```

```
deft-virtual-machine ../google-chrome/Default % sudo cp Top\ Sites /home/deft/
deft-virtual-machine ../google-chrome/Default %
```

If prompted for a password, type **password** followed by pressing the **Enter** key.

13. Change to the *deft* user home directory by entering the command below.

```
cd
```

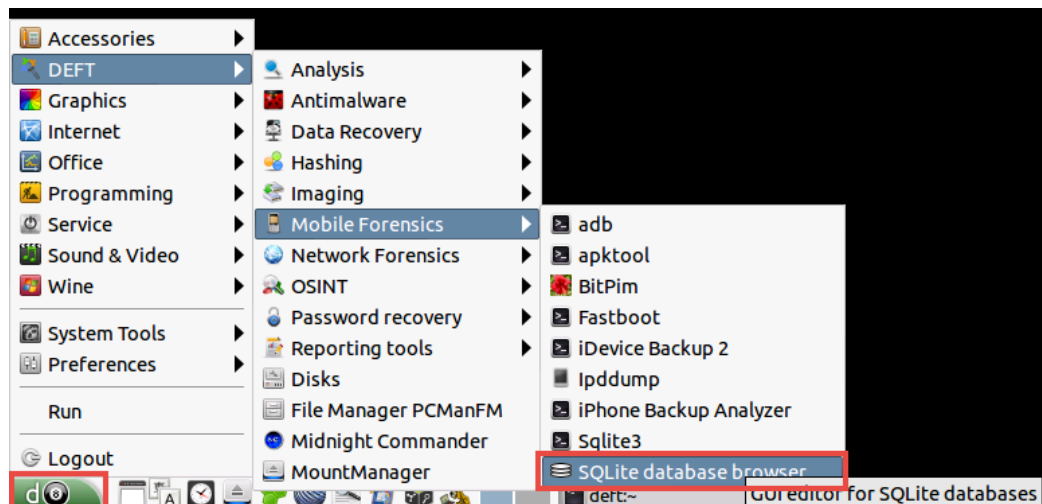
```
deft-virtual-machine ../google-chrome/Default % cd
deft-virtual-machine ~ %
```

14. List the files and directories in the current *home* directory and verify that the files have been copied over.

```
ls
```

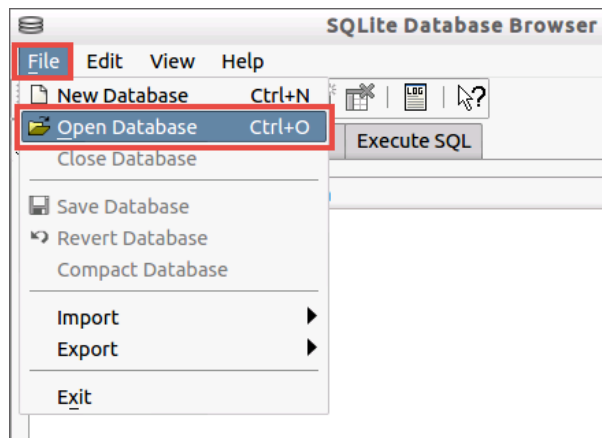
```
deft-virtual-machine ~ % ls
Cookies  Documents  evidence  Music      pdfcrack-01.5  Templates  Videos
Desktop  Downloads  History   NewFolder  Public          Top Sites
```

15. Open the *SQLite* application by navigating to **Menu > DEFT > Mobile Forensics > SQLite data browser**.

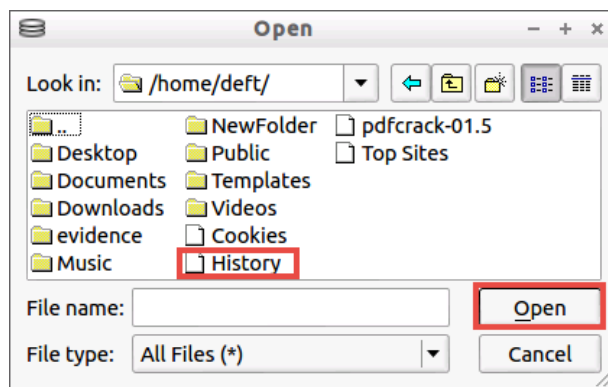


If prompted for a password, type **password** and click **OK**.

16. Using the *SQLite* application, navigate to **File > Open Database**.




17. In the *Open* dialog window, change the location to **/home/deft/** and select the **History** file. Click **Open**.



18. Once opened, click on the **Browse Data** tab.

| Database Structure Browse Data Execute SQL | | | |
|--|--------|------|--------------|
| Name | Object | Type | Schema |
| meta | table | | CREATE T... |
| downloads | table | | CREATE T... |
| downloads_url_chains | table | | CREATE T... |
| urls | table | | CREATE T... |
| visits | table | | CREATE T... |
| visit_source | table | | CREATE T... |
| keyword_search_terms | table | | CREATE T... |
| segments | table | | CREATE T... |
| segment_usage | table | | CREATE T... |
| sqlite_autoindex_meta_1 | index | | |
| sqlite_autoindex_downloads_url_chains_1 | index | | |
| keyword_search_terms_index1 | index | | CREATE IN... |
| keyword_search_terms_index2 | index | | CREATE IN... |
| keyword_search_terms_index3 | index | | CREATE IN... |
| urls_url_index | index | | CREATE IN... |
| visits_url_index | index | | CREATE IN... |
| visits_from_index | index | | CREATE IN... |
| visits_time_index | index | | CREATE IN... |
| segments_name | index | | CREATE IN... |
| segments_url_id | index | | CREATE IN... |

19. Click on the **drop-down menu** next to *Table:* and select **urls**.

| Database Structure Browse Data Execute SQL | | |
|--|----------------------|---|
| Table: | meta |  |
| | downloads | |
| | downloads url chains | |
| 1 | urls | |
| 2 | visits | |
| 3 | visit_source | |
| | keyword_search_terms | |
| | segments | |
| | segment_usage | |



20. Expand the **url** column and briefly analyze the list of URLs shown.

Database Structure Browse Data Execute SQL

Table: urls

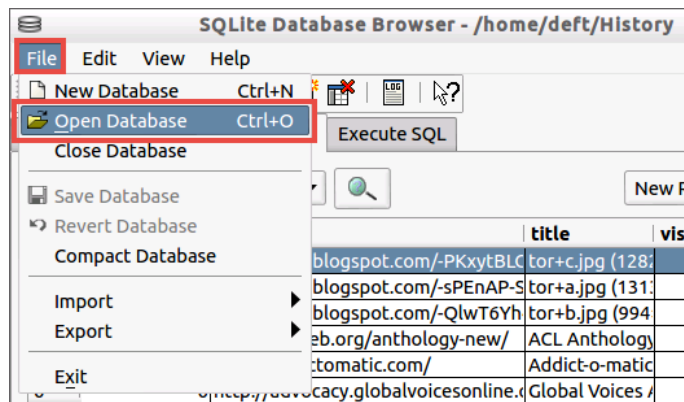
New Record Delete Record

| | id | url | title | visit_count | typed_count |
|----|----|--|------------------|-------------|-------------|
| 1 | 1 | http://2.bp.blogspot.com/-PKxytBLCtor+c.jpg (128 | | 0 | |
| 2 | 2 | http://3.bp.blogspot.com/-sPEnAP-Slor+a.jpg (131 | | 0 | |
| 3 | 3 | http://4.bp.blogspot.com/-QlwT6Yhlor+b.jpg (994 | | 0 | |
| 4 | 4 | http://aclweb.org/anthology-new/ | ACL Anthology | 0 | |
| 5 | 5 | http://addictomatic.com/ | Addict-o-matic | 0 | |
| 6 | 6 | http://advocacy.globalvoicesonline.c | Global Voices / | 0 | |
| 7 | 7 | http://ahmia.fi/ | Search onion s | 0 | |
| 8 | 8 | http://analysisintelligence.com/ | Analysis Intelli | 0 | |
| 9 | 9 | http://anoncentral.tumblr.com/ | Anonymous | 0 | |
| 10 | 10 | http://anuragbhatia.com/programm | anuragbhatia.c | 0 | |
| 11 | 11 | http://armypubs.army.mil/doctrine/ | Active_FM - Ar | 0 | |
| 12 | 12 | http://bgpatterns.com/ | BgPatterns — | 0 | |
| 13 | 13 | http://blekko.com/ | Blekko | 0 | |
| 14 | 14 | http://blog.didierstevens.com/2010 | Free Malicious | 0 | |
| 15 | 15 | http://blog.iqmatrix.com/ | IQ Matrix Blog | 0 | |
| 16 | 16 | http://boardreader.com/ | BoardReader | 0 | |

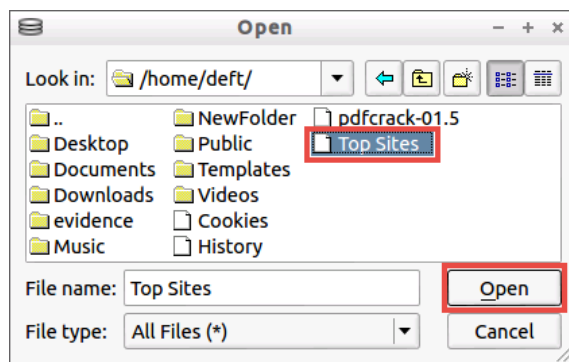
1 - 402 of 402

Go to: 0

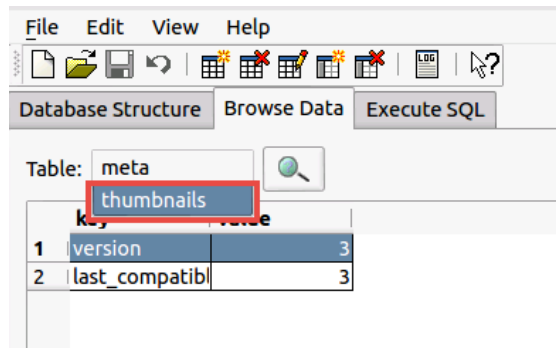
21. Switch to the *Top Sites* database. Click **File** and select **Open Database**.



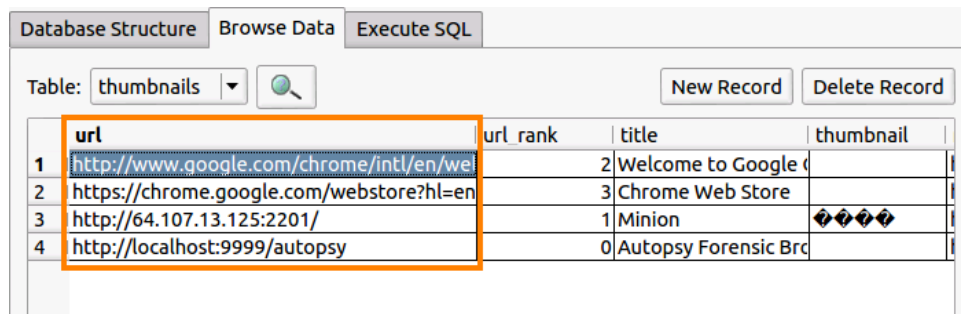
22. In the *Open* dialog window, change the location to **/home/deft/** and select the **Top Sites** file. Click **Open**.



23. Using *SQLite*, make sure that the *Browse Data* tab is selected and click on the **drop-down menu** next to *Table:*. Select **thumbnails**.

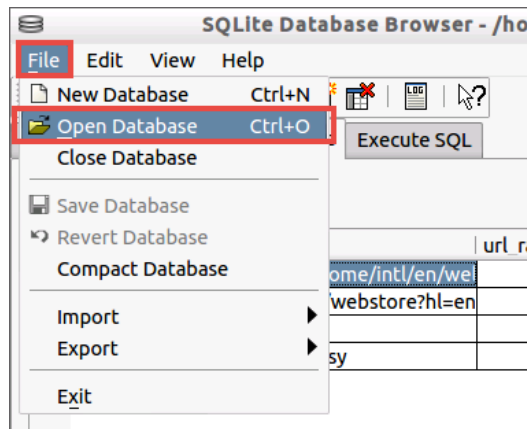


24. Expand the **url** column and analyze the *Top Sites* information.

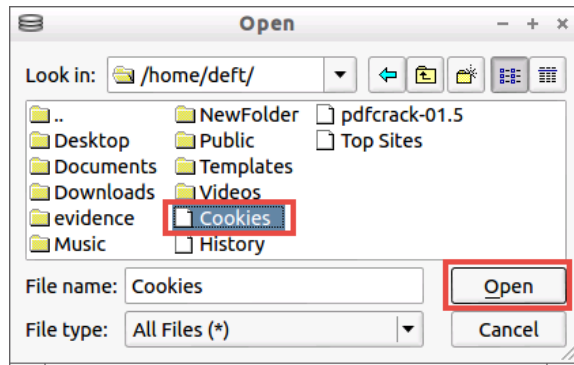


Notice that *Google Chrome* and the *Chrome Web Store* are listed as top sites.

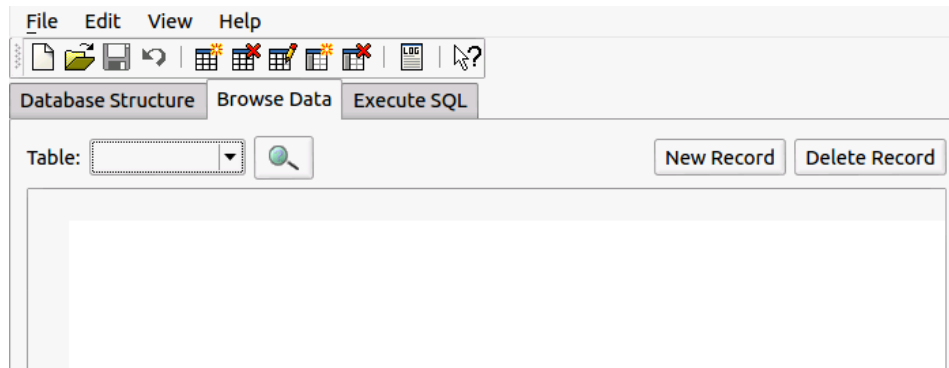
25. Switch to the *Cookies* database. Click **File** and select **Open Database**.



26. In the *Open* dialog window, change the location to **/home/deft/** and select the **Cookies** file. Click **Open**.



27. Using *SQLite*, make sure that the *Browse Data* tab is selected and take a look at the **drop-down menu** for database tables.



Notice that there is an empty table which signifies that the *Chrome* browser was either not used as much or thoroughly cleaned.

28. Close all **PC Viewers** and end the reservation to complete the lab.