



DIGITAL FORENSICS LAB SERIES

Lab 11: Browser Forensics

Objective - Digital Forensics Fundamentals

Document Version: **2015-09-28**



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Introduction	3
Objective: Browser Forensics.....	3
Lab Topology	4
Lab Settings.....	5
1 Introduction to Browsers.....	6
1.1 Meet Your Browser	6
1.2 Conclusion	12
1.3 Discussion Questions.....	12
2 Analyzing Internet Explorer	13
2.1 Analyze Internet Explorer Using Index.dat Viewer	13
2.2 Conclusion	20
2.3 Discussion Questions.....	20
3 Analyzing Google Chrome.....	21
3.1 Analyzing Google Chrome Using SQLite Database Browser	21
3.2 Conclusion	28
3.3 Discussion Questions.....	28
4 Analyzing Mozilla Firefox	29
4.1 Analyzing Mozilla Firefox Using the SQLite Database Browser	29
4.2 Conclusion	34
4.3 Discussion Questions.....	34
References	35



Introduction

This lab includes the following tasks:

1. Introduction to Browsers
2. Analyzing Internet Explorer
3. Analyzing Google Chrome
4. Analyzing Mozilla Firefox

In this lab, the student will analyze three major browsers, Internet Explorer, Google Chrome and Mozilla Firefox.

Objective: Browser Forensics

Performing this lab will provide the student with a hands-on lab experience meeting the Browser Forensics Objective:

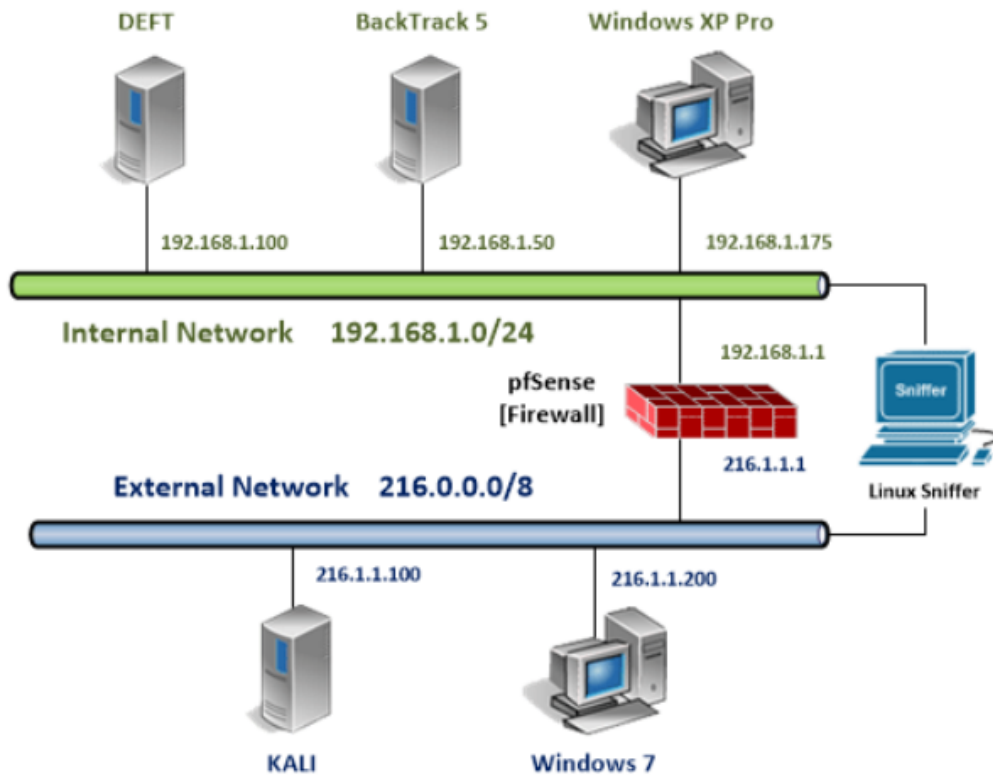
The individual will demonstrate a solid understanding of Browser Forensics.

Browser forensics is the examination and analysis of user activity on the Internet. Tasks such as analyzing Internet history data, rebuilding HTML web pages, and recovering browser artifacts allow the digital forensics investigator to extract potential evidence.

Index.dat Viewer – reads the index.dat files associated with Internet Explorer.

History Viewer – displays the entire history stored by web browsers like Internet Explorer, Firefox and Google Chrome.

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	Account (if needed)	Password (if needed)
BackTrack 5 R3 Internal Machine	192.168.1.50	root	toor
Windows XP Pro Internal Machine	192.168.1.175		
Kali Linux External Machine	216.1.1.100	root	toor



1 Introduction to Browsers

Browsers track the websites we visit. Information about which sites we visit can be used in court cases. The information can be used as evidence to help convict people of crimes and exonerate them from false accusations.

Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

1.1 Meet Your Browser

1. Open the **BackTrack 5 Machine on the Internal Network**. Type **root** for the login and **toor** (*root spelled backwards*) for the password.

The password will not be displayed when you type it, for security purposes.

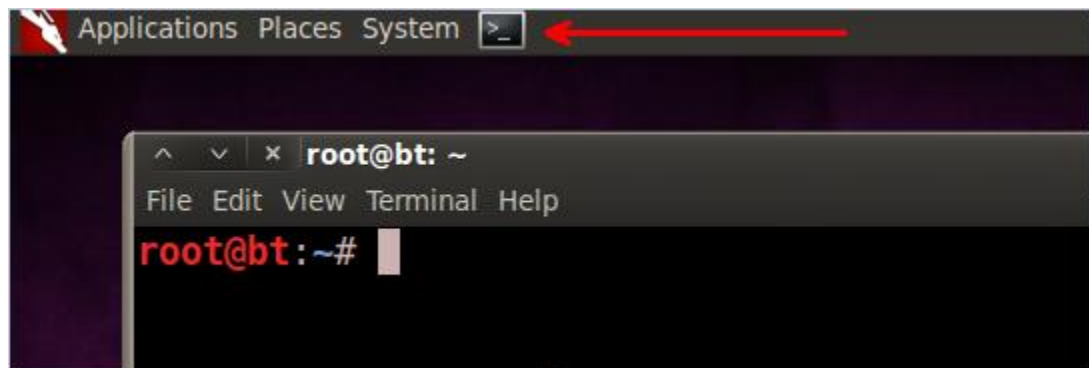
```
BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password: toor
Last login: Tue Aug 13 22:37:12 EDT 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

System information disabled due to load higher than 1.0
root@bt:~# _
```

2. Type the following command to start the Graphical User Interface (GUI):
root@bt:~# startx

```
root@bt:~# startx_
```

3. Open a terminal on the Linux system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen of the BackTrack 5 Machine.



4. To start the webserver, type the following:
root@bt:~# **apache2ctl start**

```
root@bt:~# apache2ctl start
```

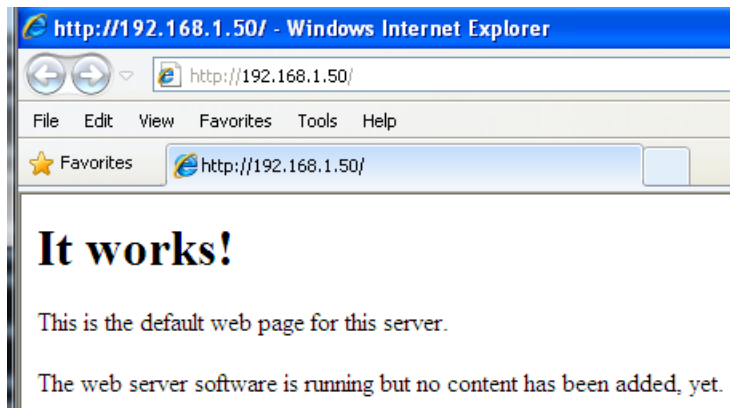
5. To verify the webserver is listening on port 80, type the following:
root@bt:~# **netstat -tan | grep 80**

```
root@bt:~# netstat -tan | grep 80
tcp        0      0 0.0.0.0:80 0.0.0.0:*    LISTEN
```

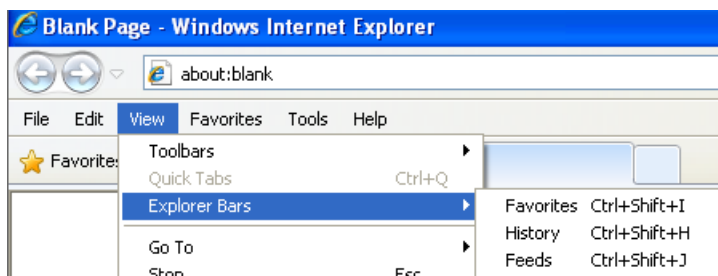
6. Open the **Windows XP Pro Machine**. Open Internet Explorer by double-clicking on the shortcut on the desktop.



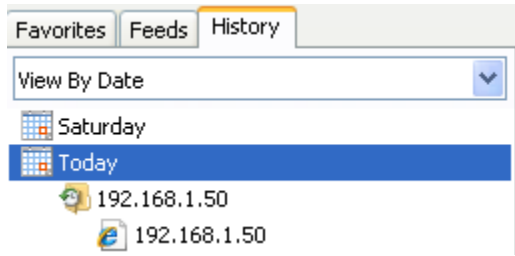
7. Type the following in the address bar: <http://192.168.1.50>



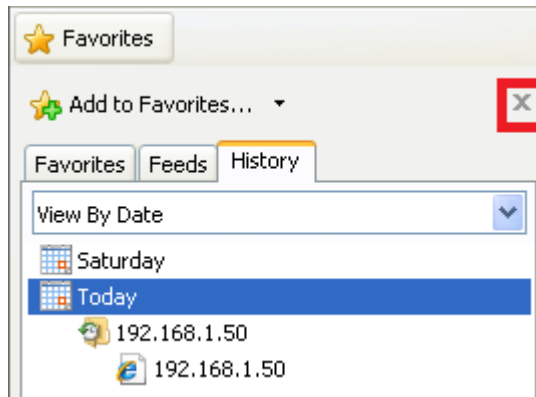
8. Select **View > Explorer Bars > History** from the Internet Explorer menu bar.



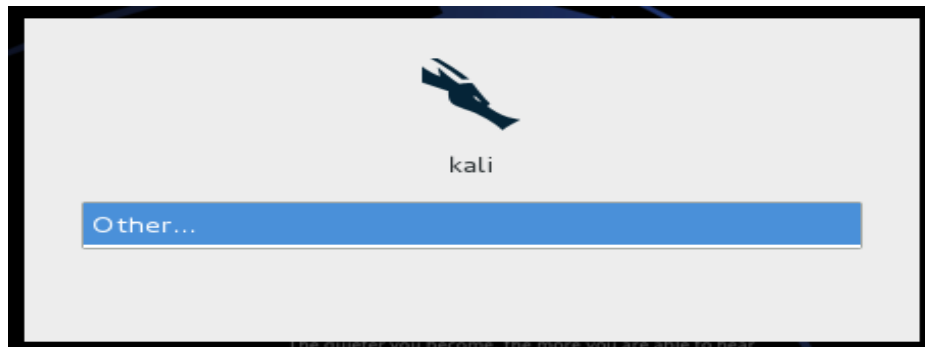
9. Click on Today to expand. Notice that the entry of 192.168.1.50 is present.



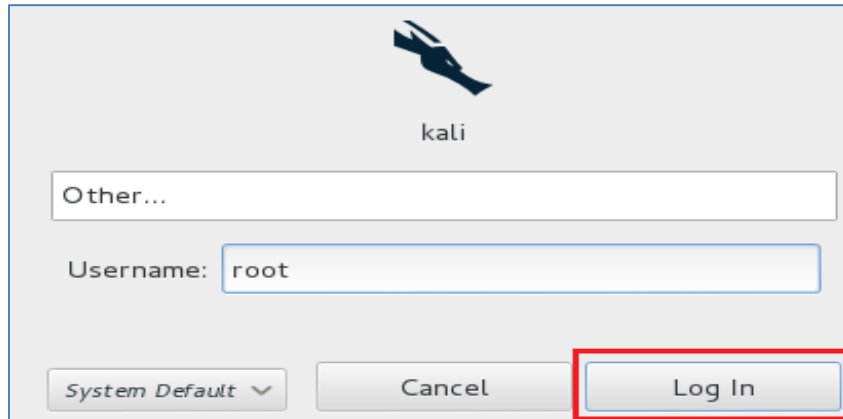
10. Select the **X** in the upper-right corner to close the browser window.



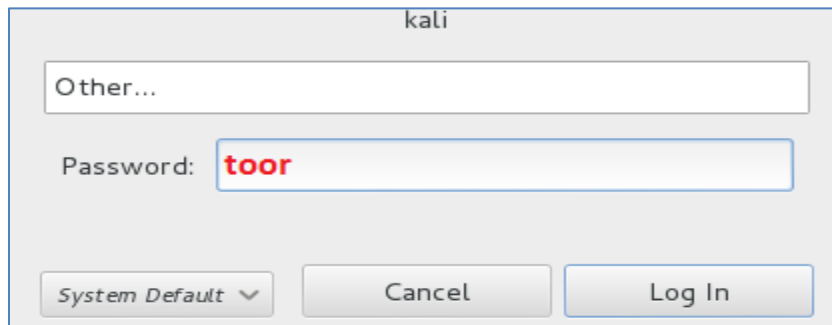
11. Log onto the **Kali Machine on the External Machine**, click the **Other** link.



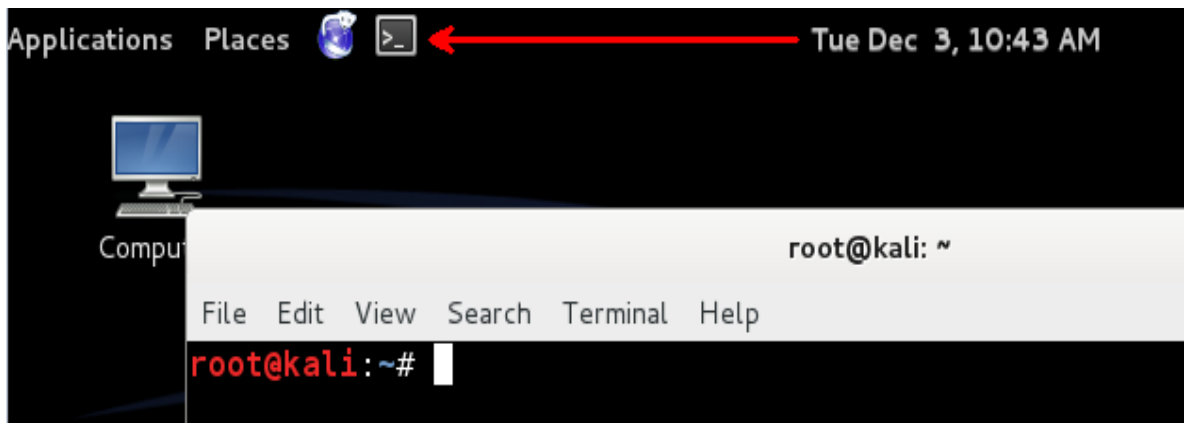
12. For the username for the Kali Linux system, type **root**, then click the **Log In** button.



13. For the password, type **toor**, then click the Log In button:



14. Open a terminal by clicking on the black icon to the right of the world icon.



15. To start the webserver on the Kali Linux External Machine, type the following:
 root@kali:~# **apache2ctl start**

```
root@kali:~# apache2ctl start
apache2: Could not reliably determine the server's fully qualified domain name
using 127.0.1.1 for ServerName
```

16. To verify the webserver is listening on port 80, type the following:

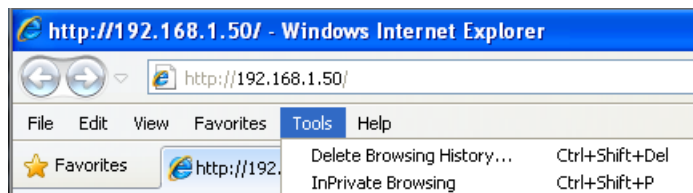
root@kali:~# **nmap -sT 127.0.0.1**

```
root@kali:~# nmap -sT 127.0.0.1

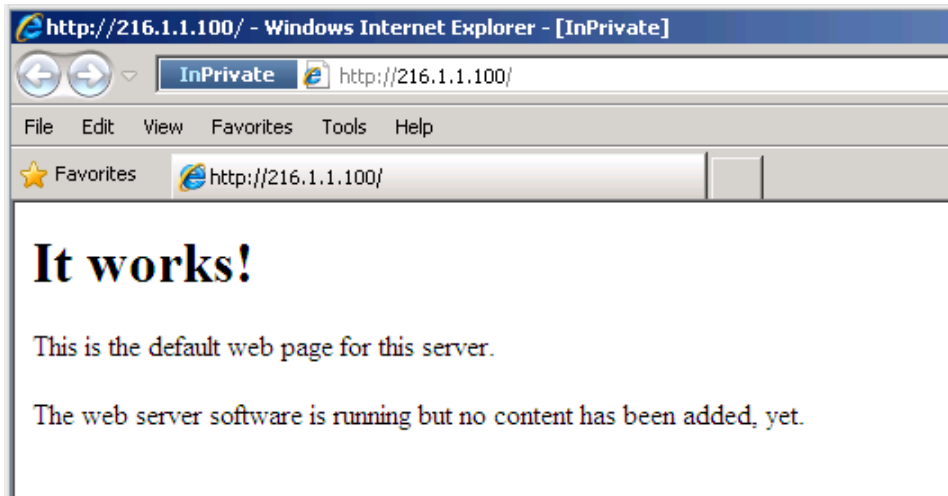
Starting Nmap 6.25 ( http://nmap.org ) at 2013-12-29 13:48 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00023s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

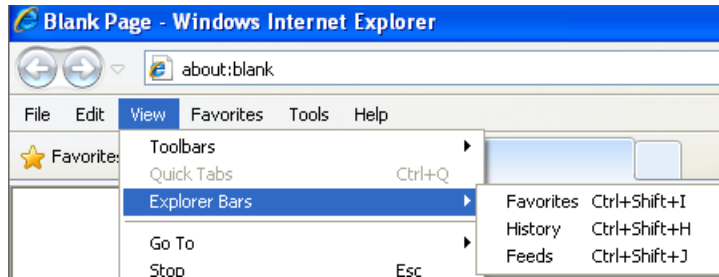
17. Return to the Windows XP Pro Machine and launch Internet Explorer. Select **Tools > InPrivate Browsing** from the menu bar.



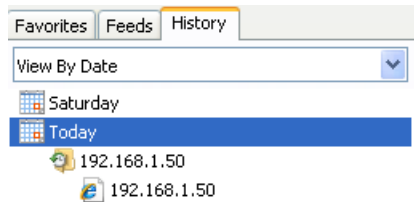
18. Type the following in the address bar: <http://216.1.1.100> and press Enter.



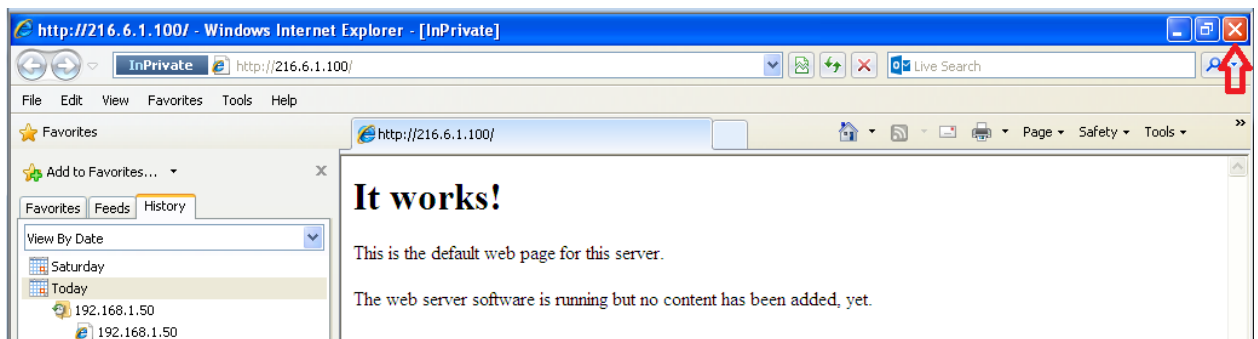
19. Select **View > Explorer Bars > History** from the Internet Explorer menu bar.



20. Expand Today. Notice that an entry of 216.6.1.100 is not present.



21. Close Internet Explorer by clicking the X in the right corner of the application.



1.2 Conclusion

Browser history can tell you a lot about a person. Internet Explorer, Firefox, Chrome, and other browsers give you the ability to view a person's browser history. Most browsers include a "stealth mode", which will allow the user to surf websites without being tracked.

1.3 Discussion Questions

1. Where do you go to view your Internet history in Internet Explorer?
2. How can you prevent the websites you visit from being recorded in IE?
3. What does InPrivate Browsing mode do for a user?
4. How do you get to InPrivate Browsing mode in Internet Explorer?



2 Analyzing Internet Explorer

When analyzing browser activity, there are two primary areas of interest in Internet Explorer. One is the **index.dat** file, which is used by the web browser and the browser cache and is in the format of MSIECF (Microsoft Internet Explorer Cache Format). The other area of interest is the browser's cache files.

There are several different index.dat files for Internet Explorer. The index.dat files in Windows XP are in several locations:

index.dat file locations in Windows XP
\Documents and Settings\<Username>\Cookies\index.dat
\Documents and Settings\<Username>\Local Settings\History\History.IE5\index.dat
\Documents and Settings\<Username>\Local Settings\History\History.IE5\MSHist012001123120020101\index.dat
\Documents and Settings\<Username>\Local Settings\History\History.IE5\MSHist012002010720020114\index.dat
\Documents and Settings\<Username>\Local Internet Files\Content.IE5\index.dat

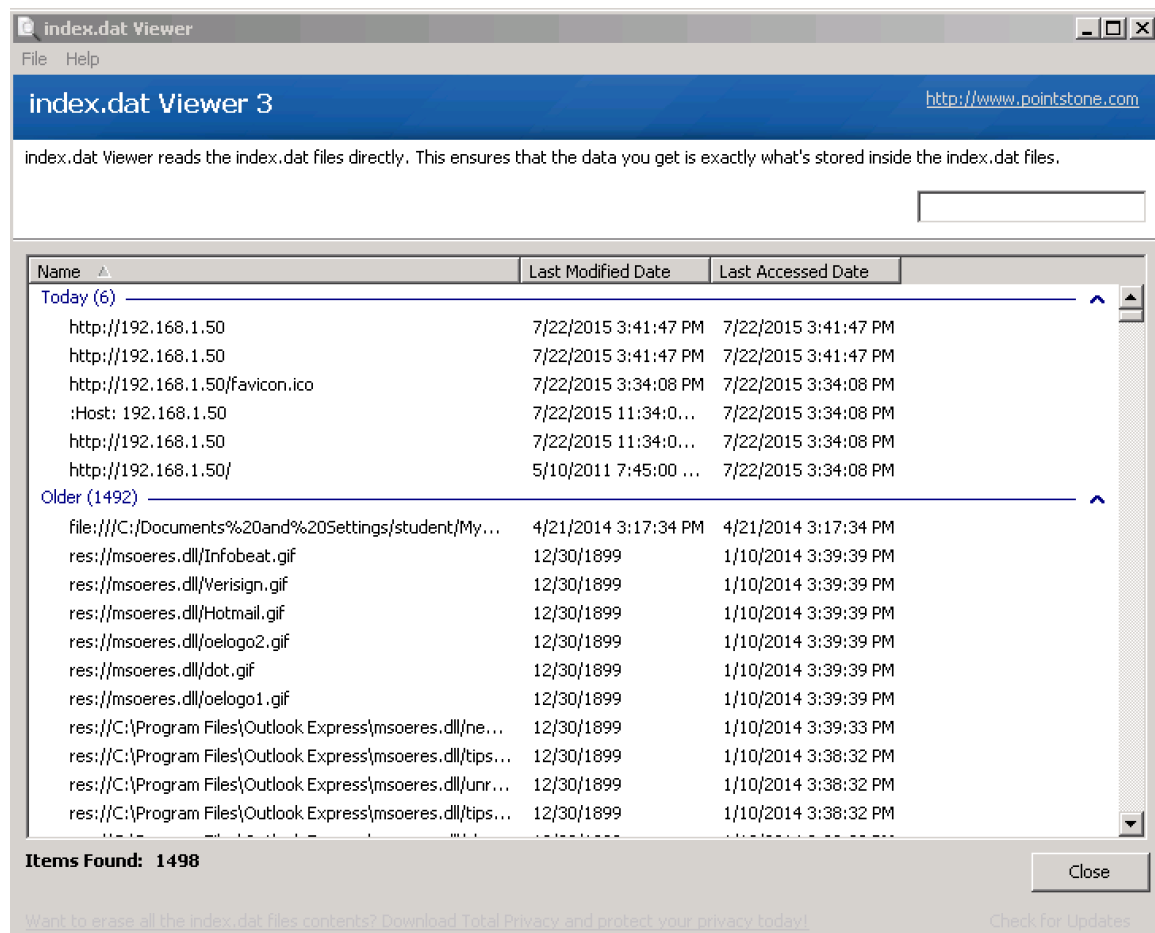
2.1 Analyze Internet Explorer Using Index.dat Viewer

We will need a tool to investigate the index.dat files. We will use a freeware tool installed on the Windows XP Pro Internal machine called Index.dat Viewer. This tool looks at all the index.dat files and provides a comprehensive picture.

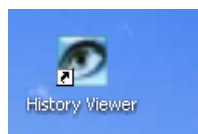
1. On the Windows XP Pro Internal Machine, click on the Index.Dat Viewer 3 icon on the desktop.



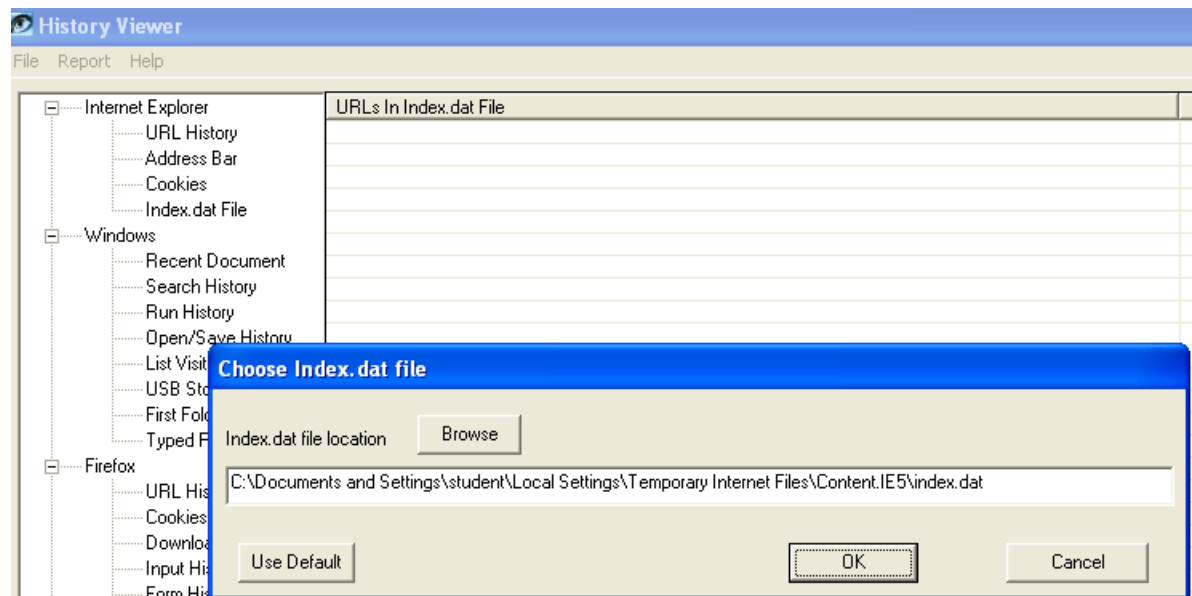
- The index.dat Viewer lists a combined view of all of the index.dat files including cookies, URLs, and searches. Notice that the Last Accessed and Last Modified dates are also listed.



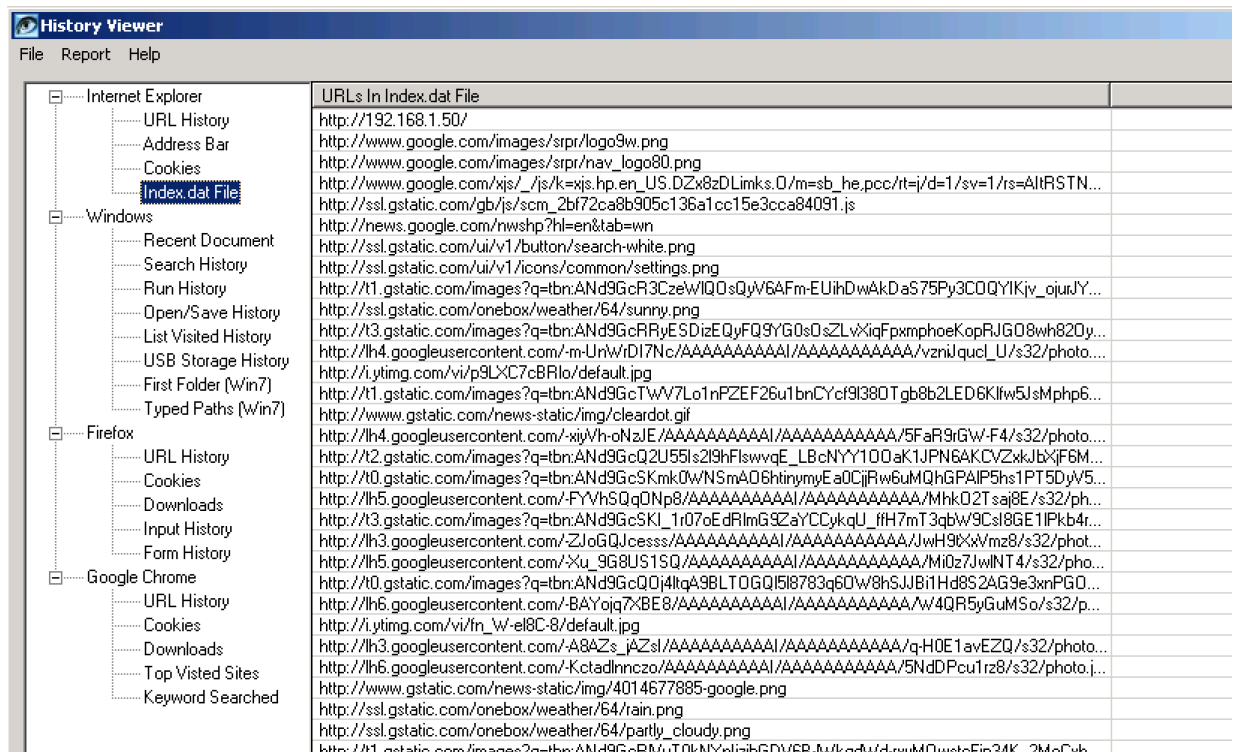
- Close Index.dat Viewer when you are finished examining the Internet history of the system.
- We can look at an individual index.dat by launching History Viewer.



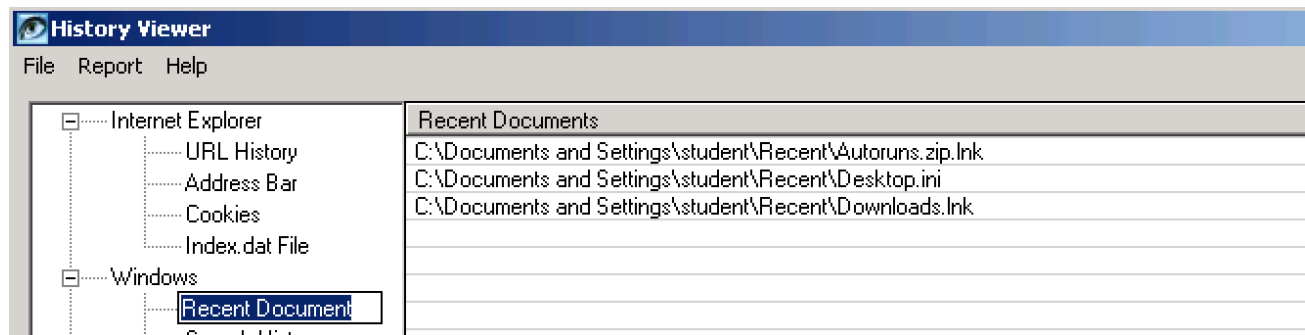
- Another index.dat file can be viewed by clicking on **Index.dat File**. Click the OK button.



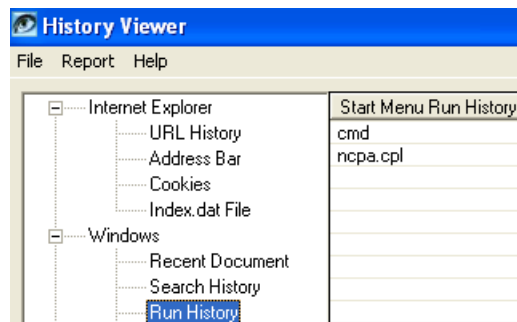
- You can see how much information is stored in the index.dat files for Internet Explorer.



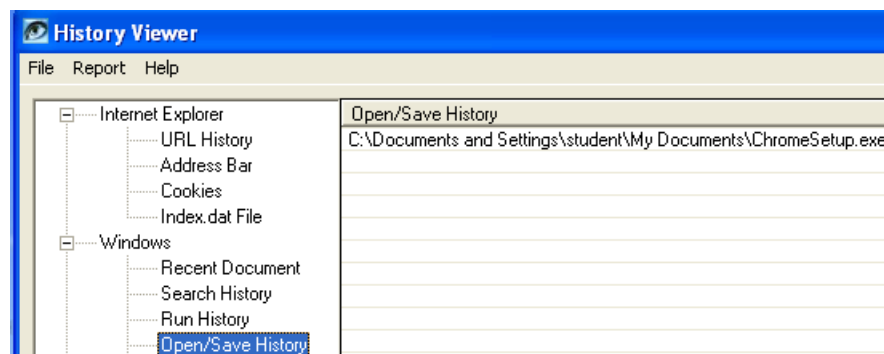
9. Just like the Registry Viewer, the History Viewer program also allows you to view recent documents opened. However, unlike the Registry Viewer program, you do not need to navigate the registry subkeys. Click **Recent Document** under Windows.



10. Click **Run History** under Windows to view any commands that were typed into the run box. For example in the graphic below, the commands include cmd.exe for command line and ncpa.cpl for networking were run. (Run History may be empty if no commands were typed into the run box prior to this lab)

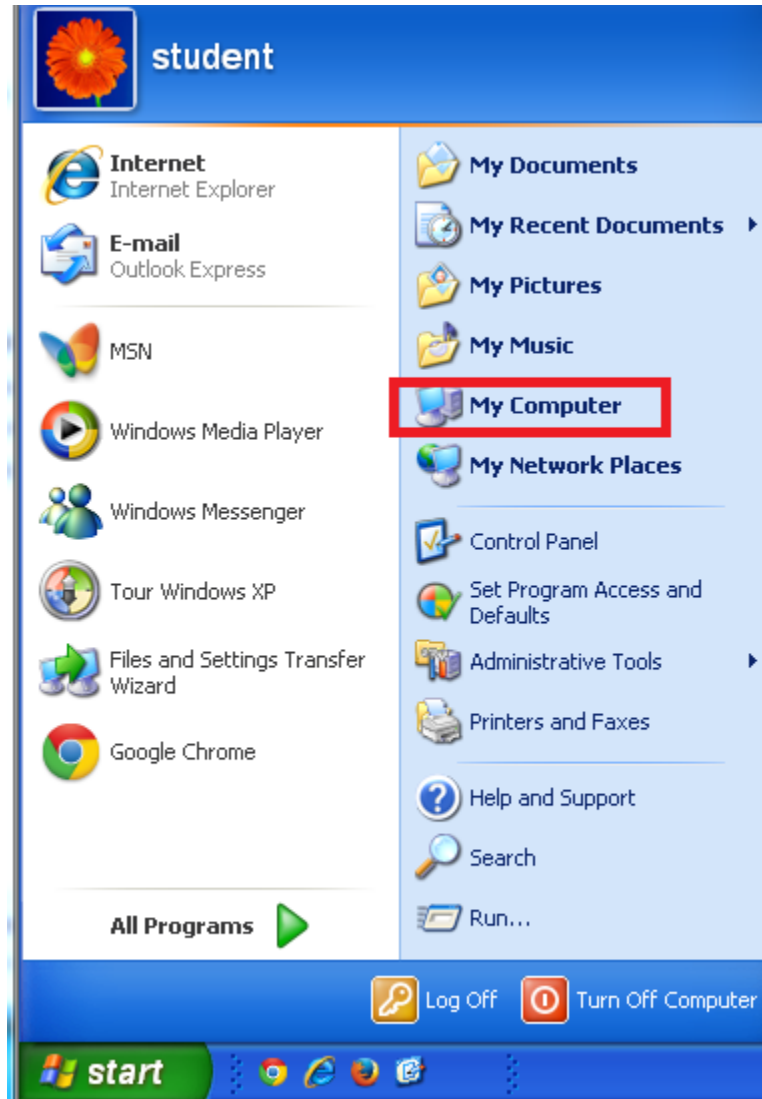


11. Click **Open/Save History** under Windows to view any files saved in the Save As box. (Open/Save History may be empty if no files were saved prior to this lab).

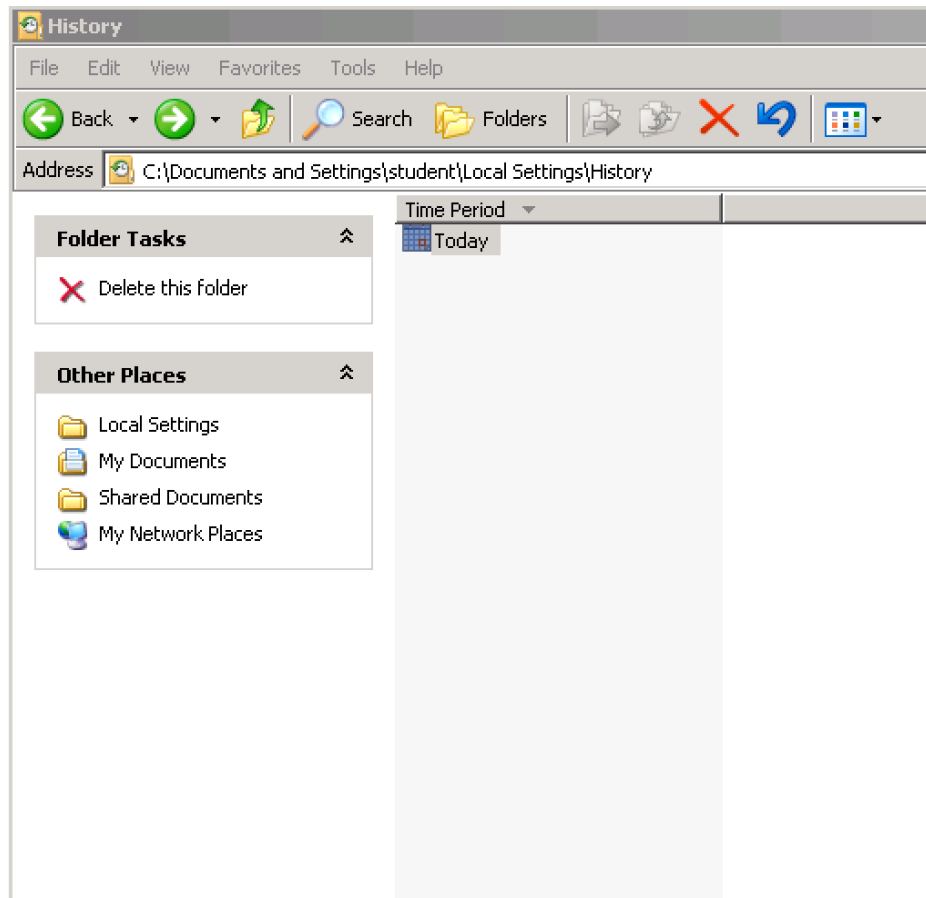


12. Close the History Viewer.

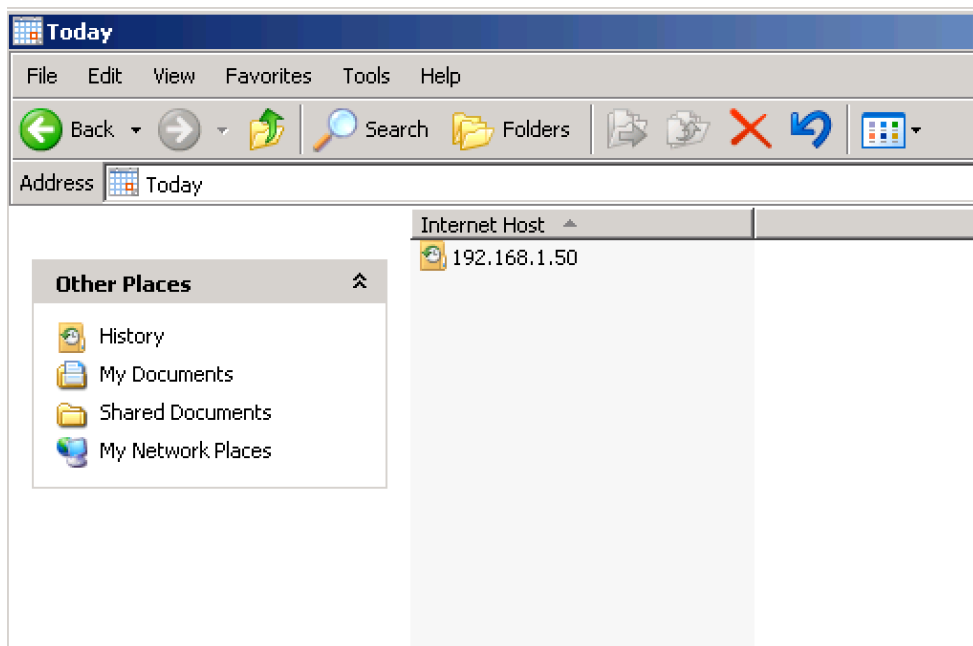
13. We will examine areas of the hard drive that show us the Internet Explorer browsing history. Click on the Start button and select the My Computer link from the Start menu.



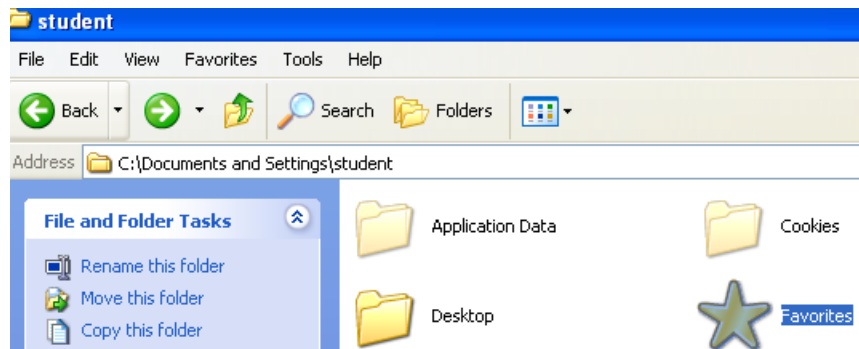
14. Double-click on **Local Disk C: > Documents and Settings > student > Local Settings > History**. (You may only see the Today calendar)



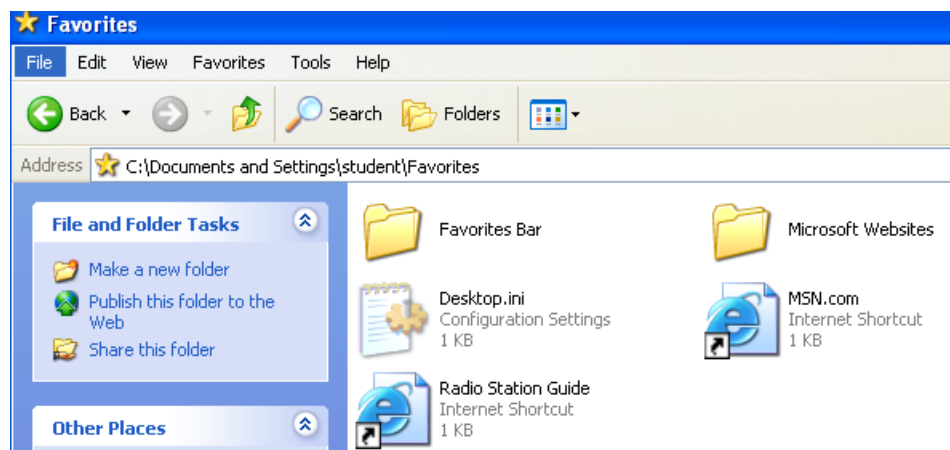
15. Clicking on the Today calendar link will display information about browsed sites.



16. Click the Back button three times to navigate back to the Student folder. Double click on the Favorites folder to view the user's favorite websites.



17. View the user's favorite websites. Additional links may reside in the sub-folders.



18. Close the Favorites window.

2.2 Conclusion

Browser history can provide a wealth of information about a person. Internet Explorer comes installed by default on the Microsoft Windows operating system; so many people use it as their default browser. Tools like Index.dat Viewer and History Viewer allow you to view a user's Internet history.

2.3 Discussion Questions

1. Name some tools that allow you to view Internet Explorer History.
2. Where is the Internet Explorer History located on the hard drive?
3. Where are the Internet Explorer Favorites located on the hard drive?
4. Name some tools that allow you to view Internet Explorer cookies.

3 Analyzing Google Chrome

Google Chrome does not store information regarding Internet searches, URLs, cookies, etc. on the Windows hard drive or an indiscreet file like index.dat. Instead, the information is stored in a series of SQLite databases.

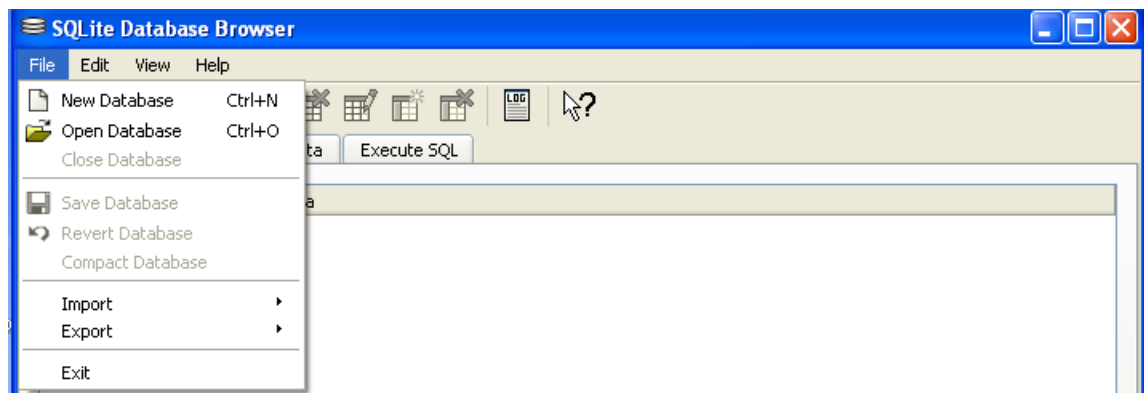
3.1 Analyzing Google Chrome Using SQLite Database Browser

We will use SQLite Database Browser to look at the databases within Chrome. The location of the databases is C:\Documents and Settings\%username%\Local Settings\Application Data\Google\Chrome\User Data\Default.

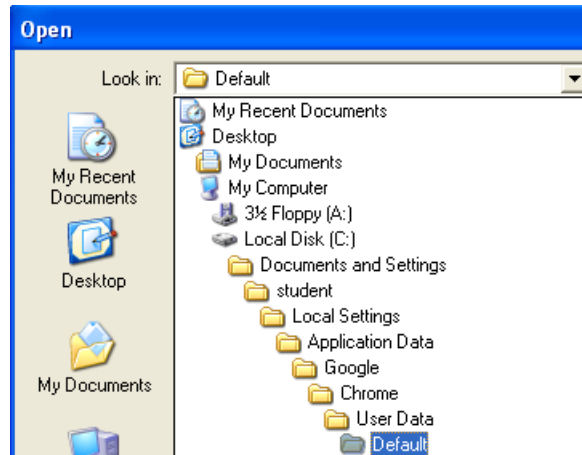
1. Double-click on the **Shortcut to SQLite Database Browser** on the Windows XP Pro desktop.



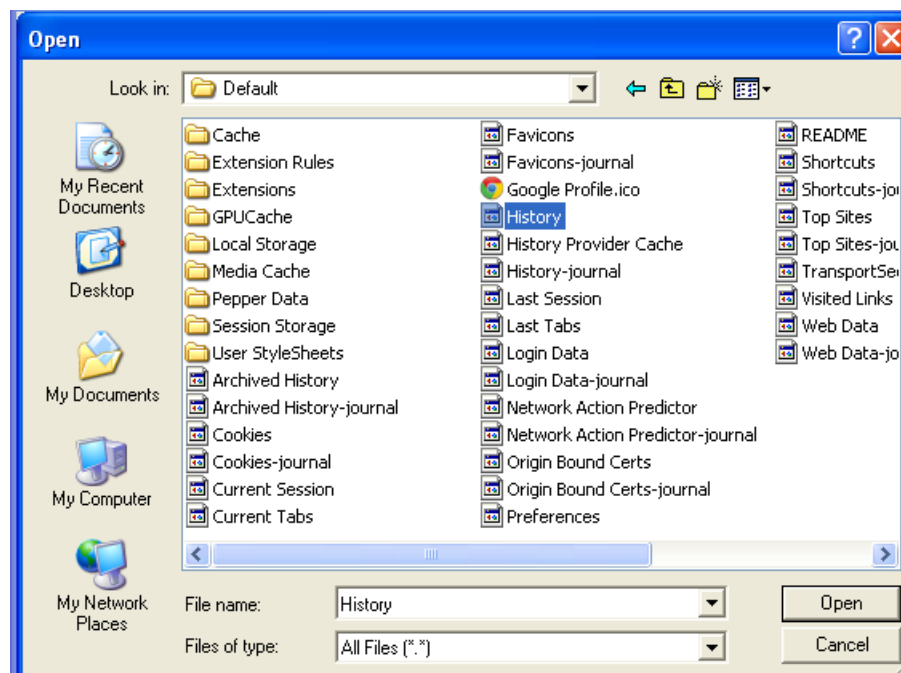
2. Click **File** from the menu bar and select **Open Database**.



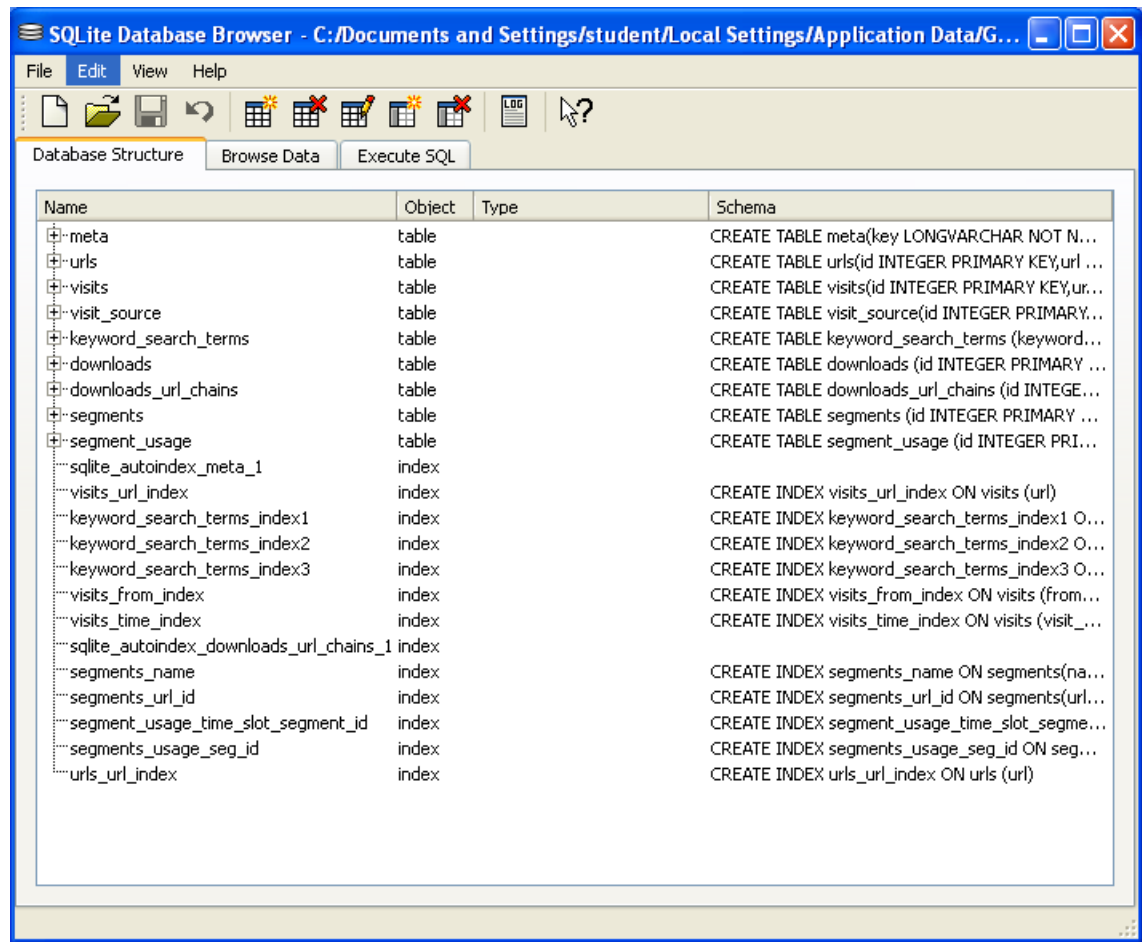
3. Navigate to the following directory on the hard disk to access the Chrome History file:
C:\student\Local Settings\Application Data\Google\Chrome\User Data\Default



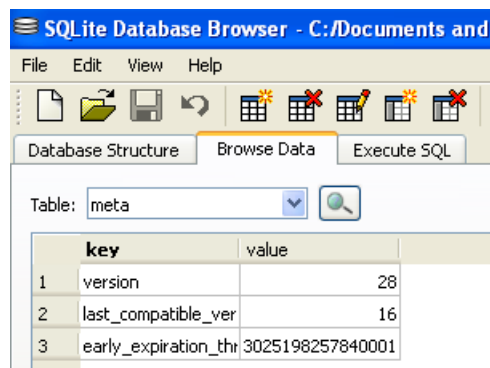
4. Double-click on the **History** file to open the Chrome History file.



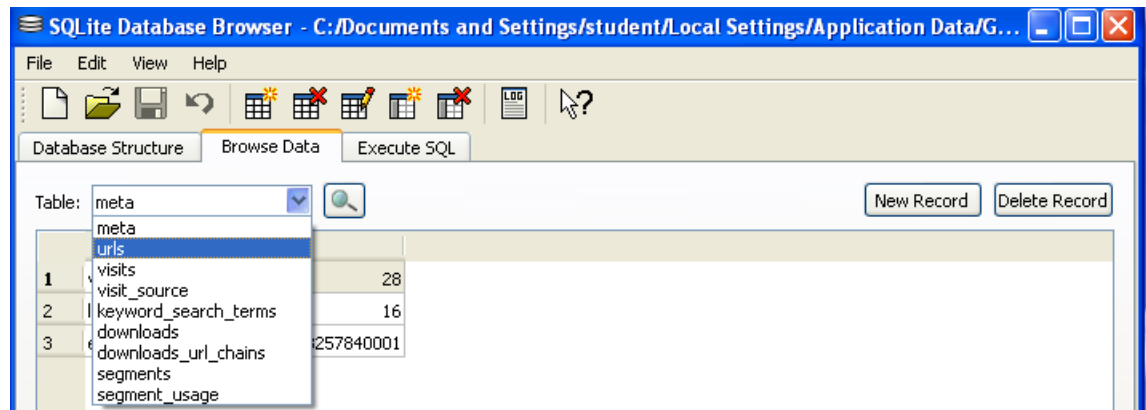
5. You will first see the database structure.



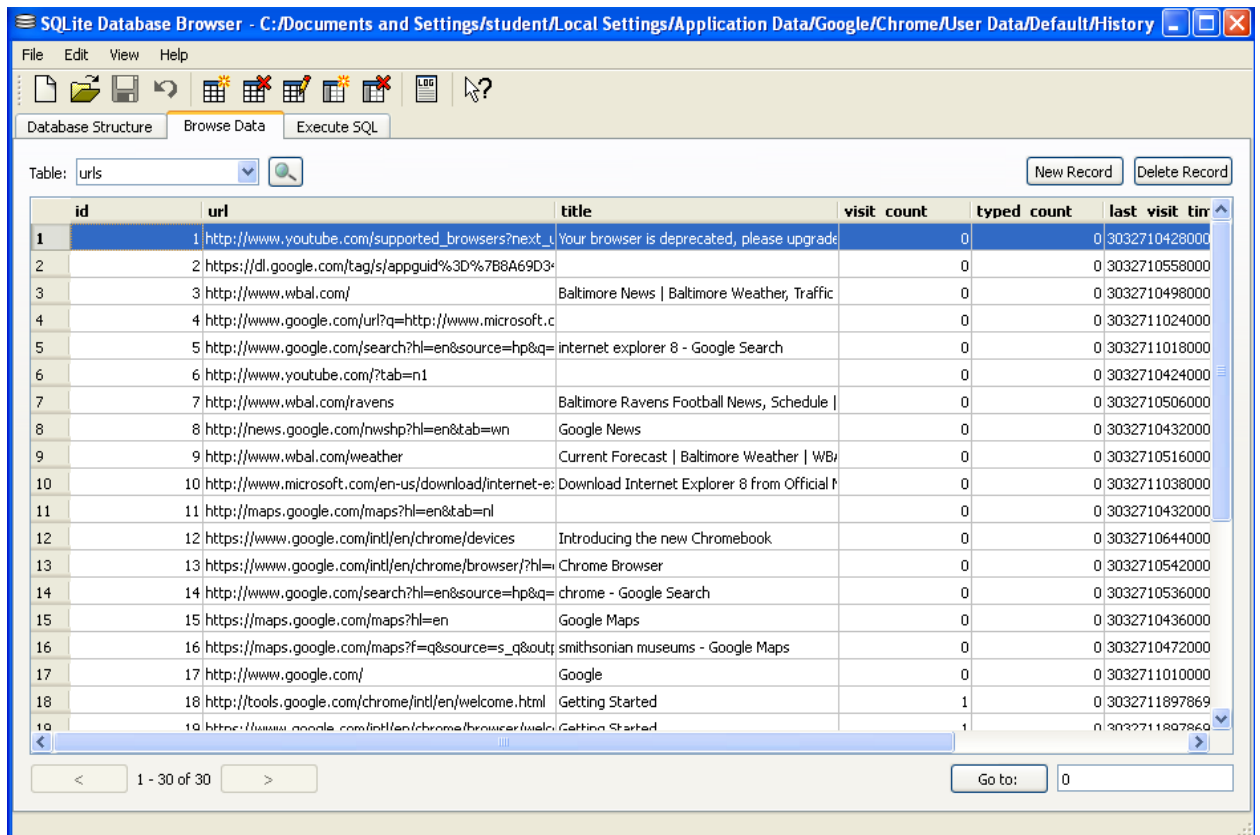
6. Click on the **Browse Data** tab.



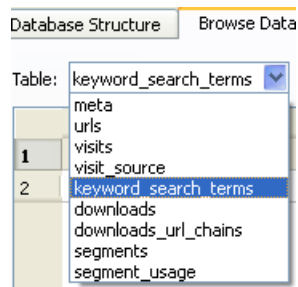
7. You are viewing the meta data. From the Table drop-down, select **urls**.



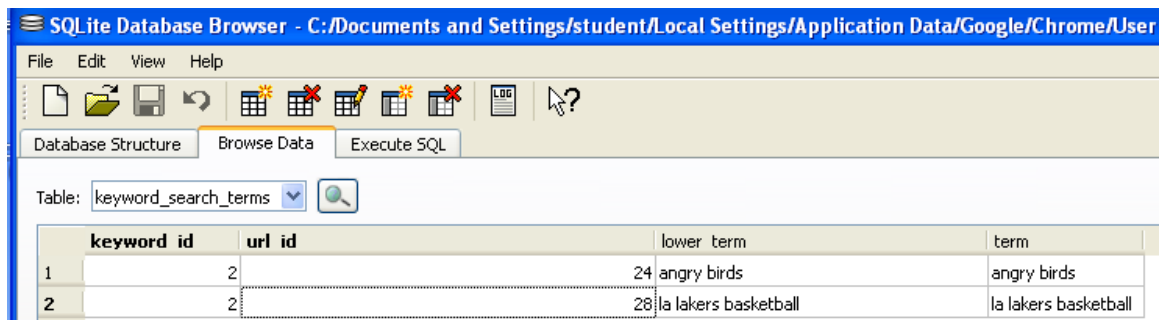
8. The URLs that were recently pulled up in the browser are displayed.



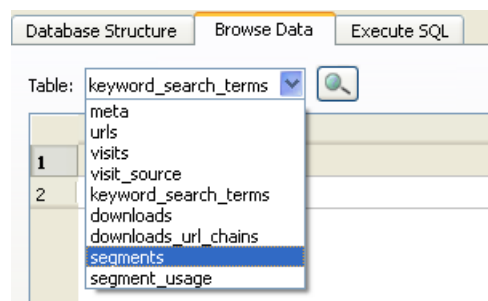
9. Select **keyword search terms** from the Table drop-down.



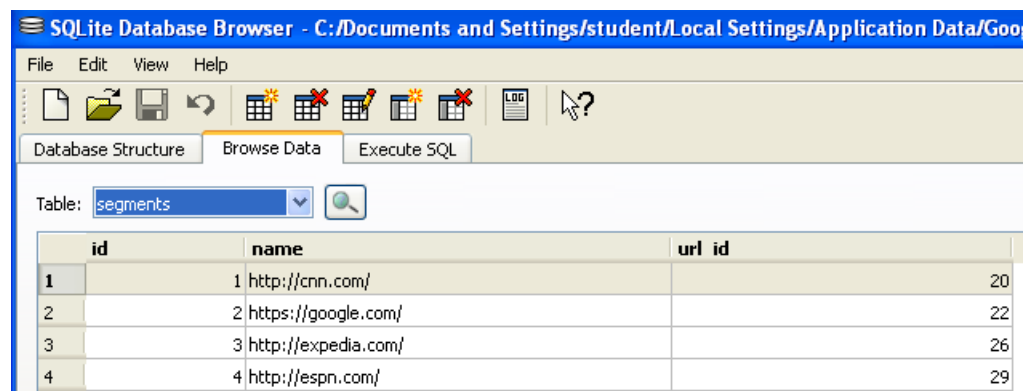
10. These keywords were typed in the search field in the browser.



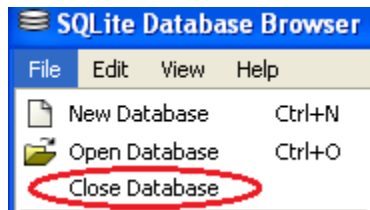
11. Select **segments** from the Table drop-down.



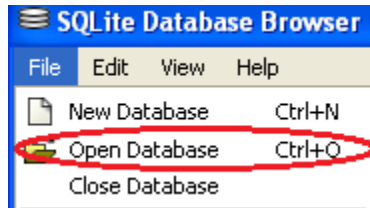
12. View the listed segments. The segments listed in the table are the beginning parts of the URLs typed into the URL field, without any trailing subdirectories.



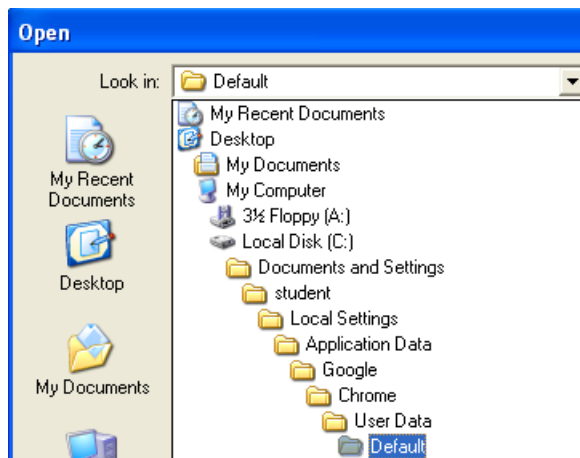
13. Close the History database by selecting **File** and choosing **Close Database**.



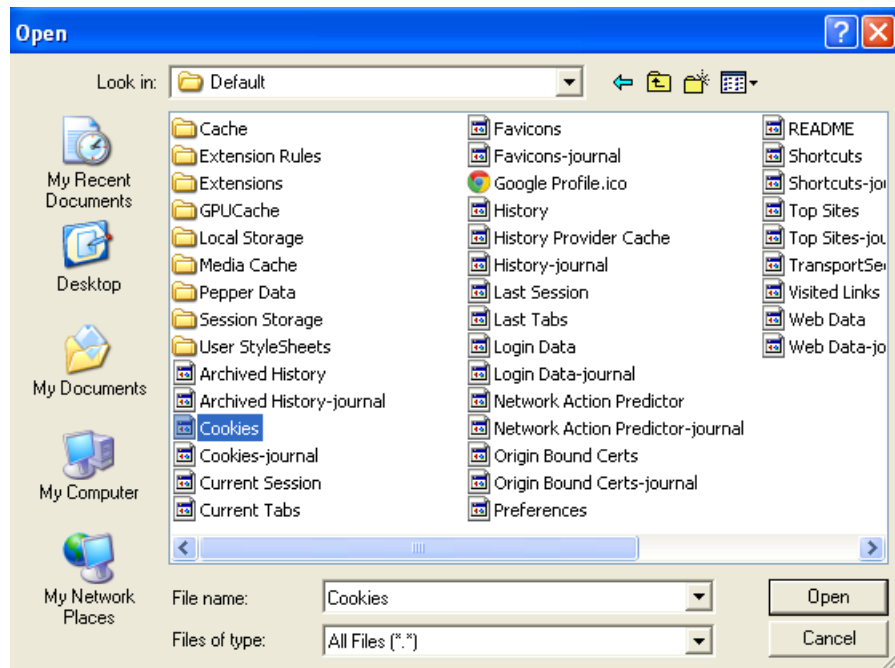
14. To open the cookie database, select **File** and choose **Open database**.



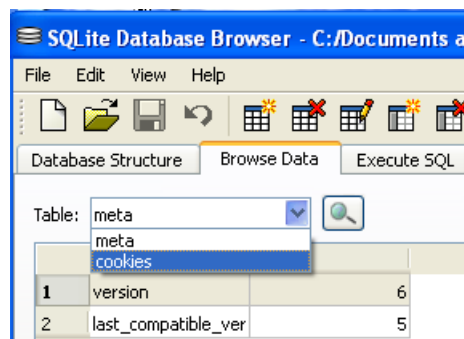
15. Navigate to the following directory on the hard disk to access the Chrome History file: **C:\student\Local Settings\Application Data\Google\Chrome\User Data\Default**



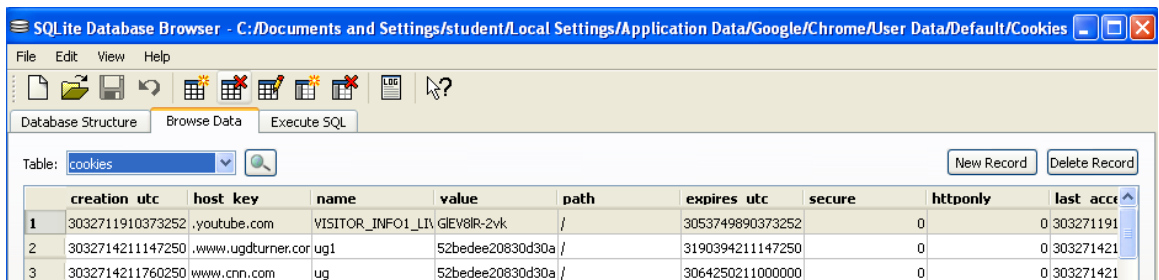
16. Double-click on the **Cookies** file to open the Chrome Cookies file.



17. On the Browse Data tab, select **cookies** from the Table dropdown.



18. The cookies dropped from various websites that were visited are listed here.



19. Close the SQLite Database Browser.

3.2 Conclusion

Browser history can provide a wealth of information about a person. The Chrome browser is widely used because of the number of users using Google and Google related services such as Gmail and Google+.

3.3 Discussion Questions

1. Name some tools that allow you to view Chrome history.
2. Where is the Chrome History file located on the hard drive?
3. Where is the Chrome Cookies file located on the hard drive?
4. Name some tools that allow you to view Chrome Cookies.

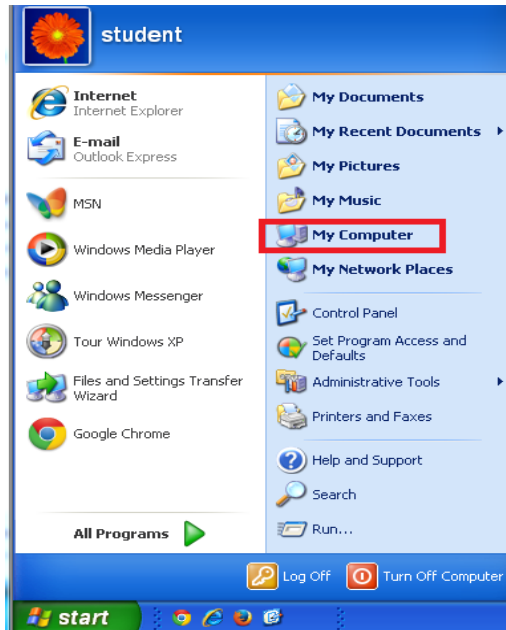


4 Analyzing Mozilla Firefox

Firefox is similar to Chrome in that they both store their information in SQLite databases.

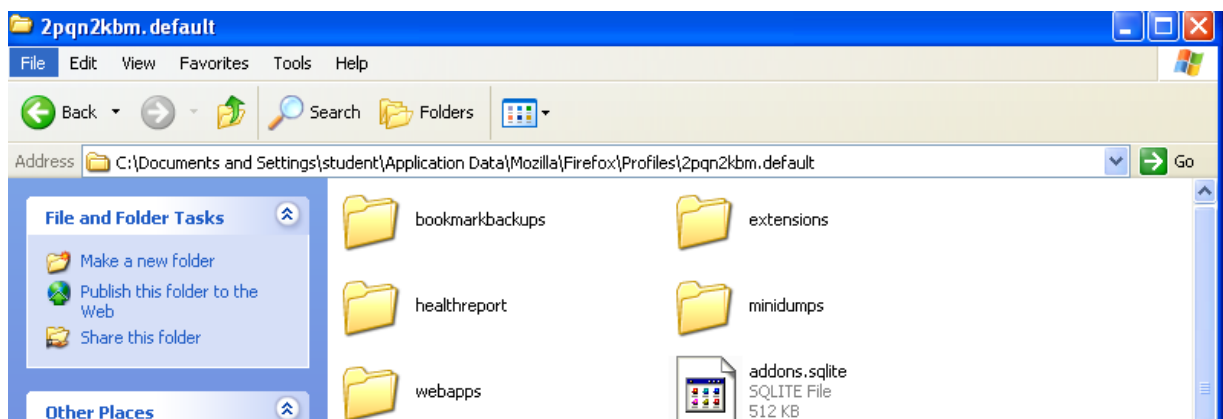
4.1 Analyzing Mozilla Firefox Using the SQLite Database Browser

1. We will examine areas of the hard drive that show us the Firefox browser files. Using the Windows XP Machine, click on the Start button and select the **My Computer** link from the Start Menu.



2. Navigate to **C:\Documents and Settings\student\Application Data\Mozilla\Firefox\Profiles\random_characters.default**. This is the location where Mozilla stores its databases.

For the subfolder named *random_characters.default*, the *random_characters* will vary on your system.

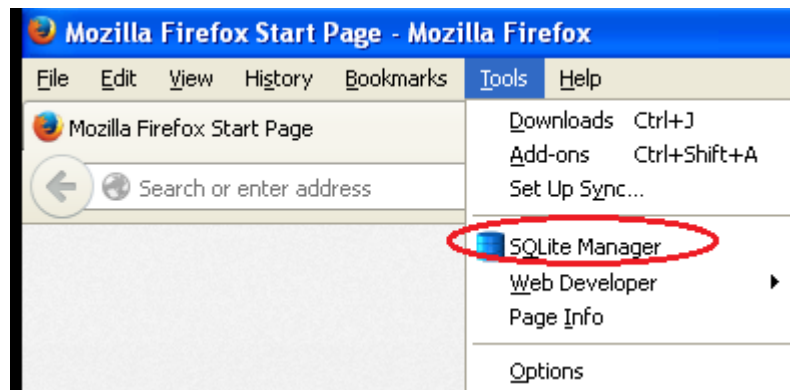


- Open Firefox by double-clicking on the shortcut on the desktop.

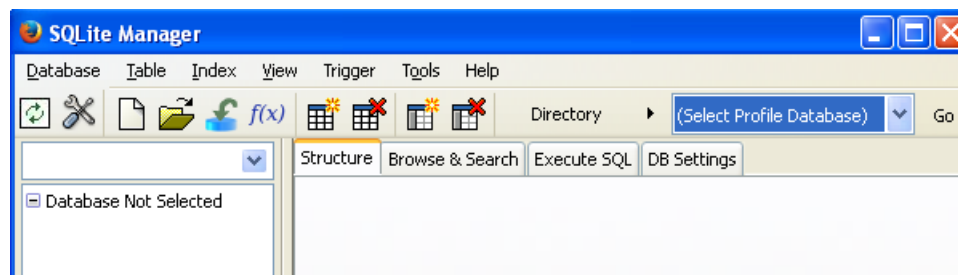


In this task, we will use a different method for viewing the SQLite databases. We will view them directly from within Firefox. In Firefox, SQLite Manager is a Firefox add-on.

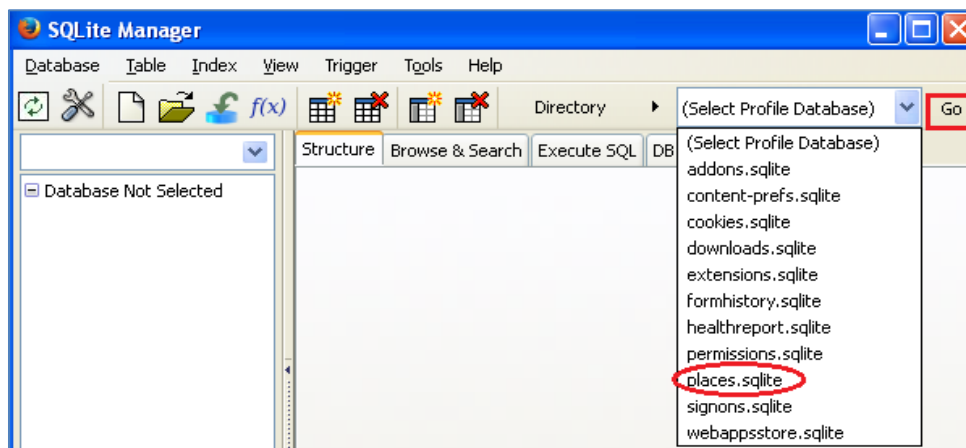
- From the Mozilla Firefox Start Page menu bar, go to **Tools > SQLite Manager**.



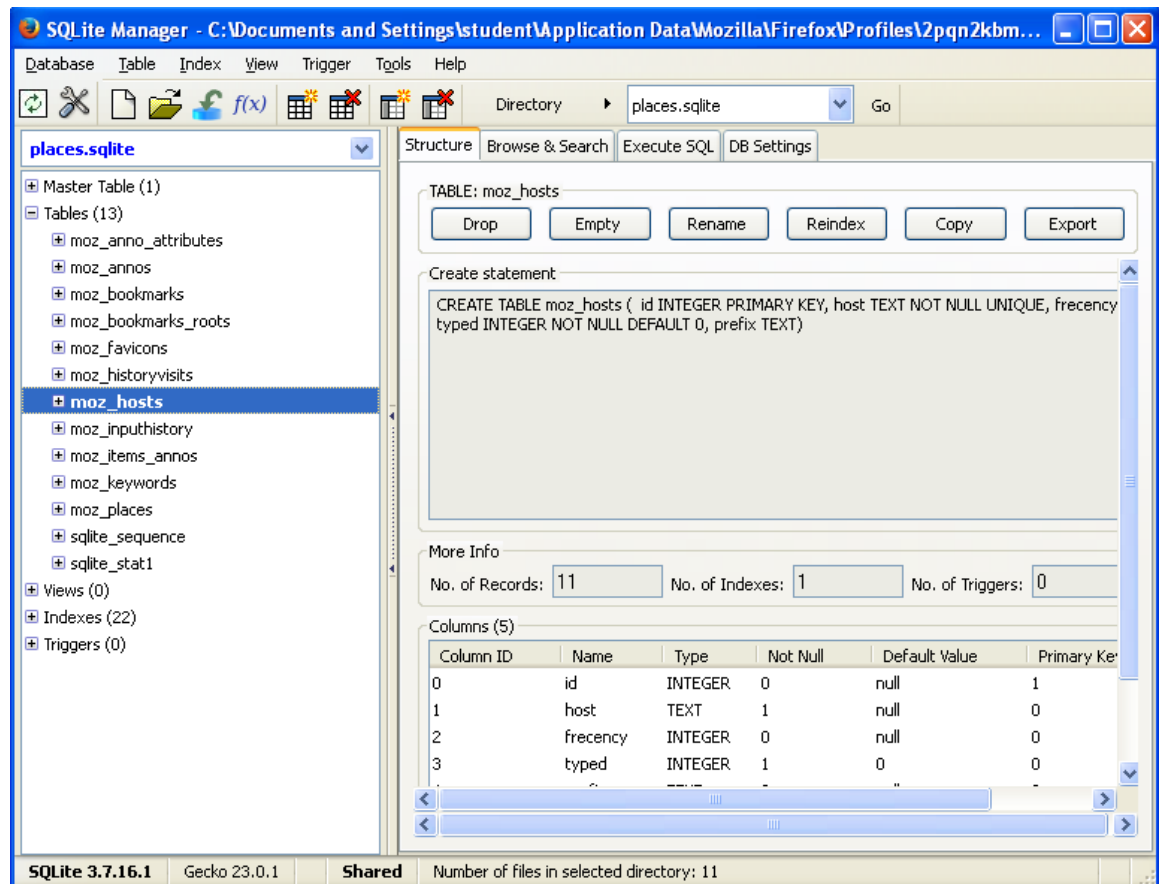
- The SQLite Manager will open. It will state, *Database Not Selected*.



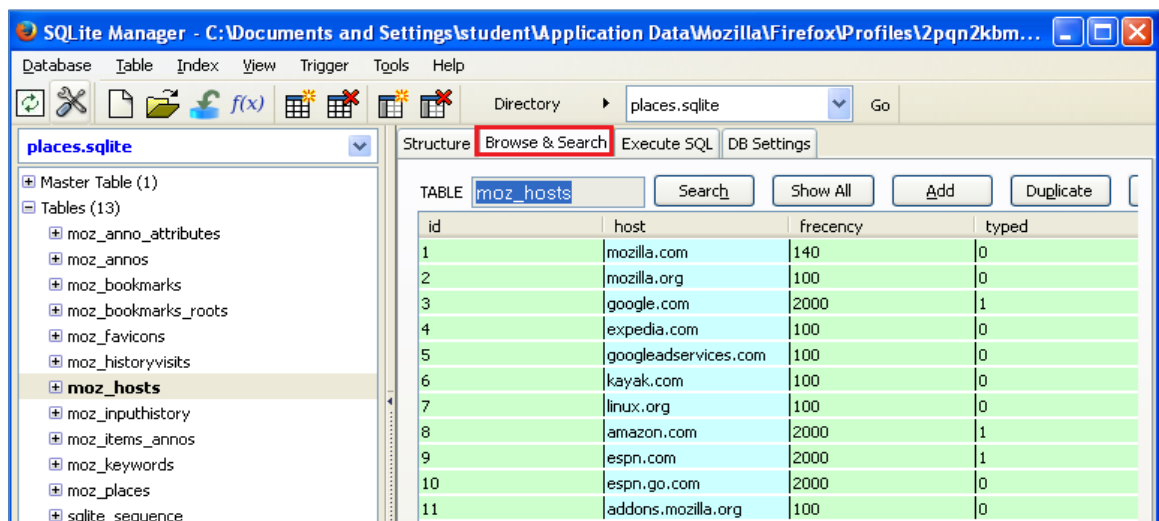
- From the Directory drop-down, select **places.sqlite** and click **Go**.

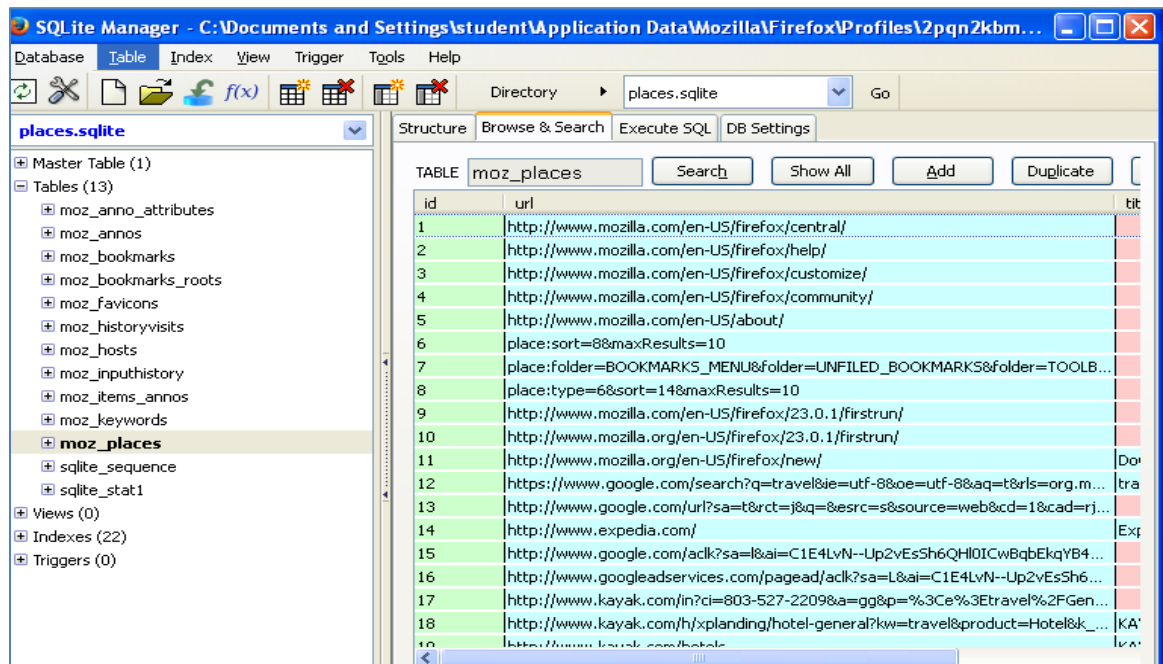


7. This file stores Internet history. On the left, click **moz_hosts**.



8. Click the **Browse & Search** tab to view the websites that were visited.



9. Click **moz_places** to see a complete URL path.


SQLite Manager - C:\Documents and Settings\student\Application Data\Mozilla\Firefox\Profiles\2pqn2kbm...

Database: Table Index View Trigger Tools Help

Directory: places.sqlite Go

places.sqlite

Master Table (1)

Tables (13)

- moz_anno_attributes
- moz_annos
- moz_bookmarks
- moz_bookmarks_roots
- moz_favicons
- moz_historyvisits
- moz_hosts
- moz_inputhistory
- moz_items_annos
- moz_keywords
- moz_places**
- sqlite_sequence
- sqlite_stat1

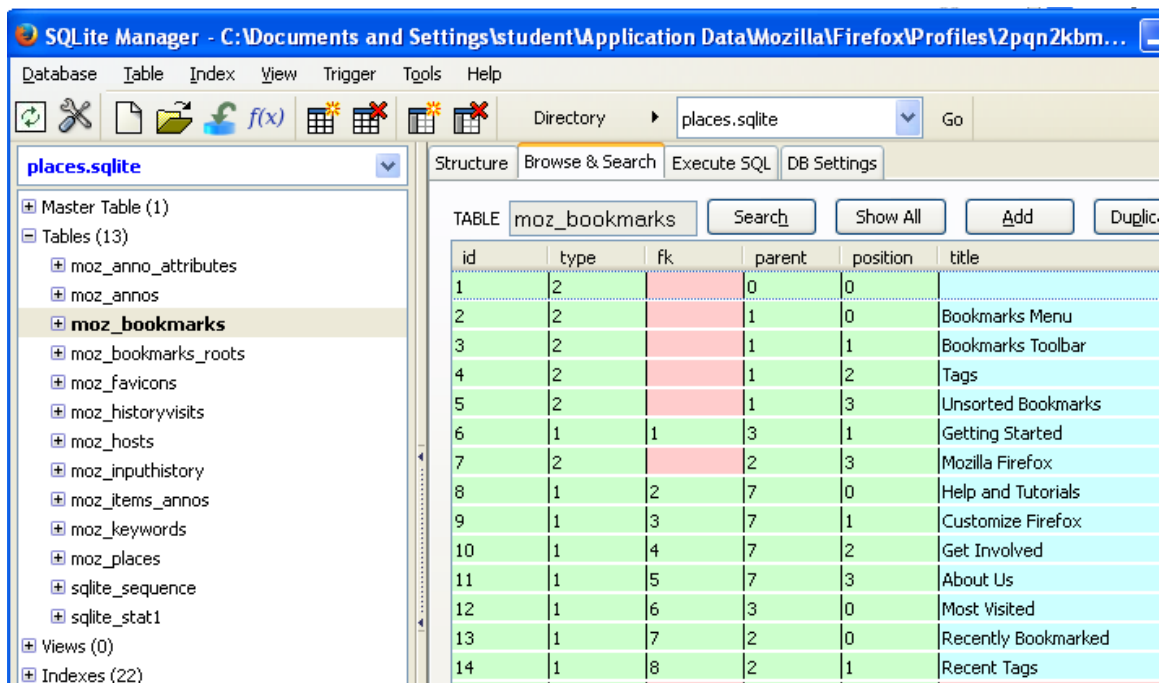
Views (0)

Indexes (22)

Triggers (0)

TABLE: moz_places

id	url	title
1	http://www.mozilla.com/en-US/firefox/central/	
2	http://www.mozilla.com/en-US/firefox/help/	
3	http://www.mozilla.com/en-US/firefox/customize/	
4	http://www.mozilla.com/en-US/firefox/community/	
5	http://www.mozilla.com/en-US/about/	
6	place:sort=8&maxResults=10	
7	place:folder=BOOKMARKS_MENU&folder=UNFILED_BOOKMARKS&folder=TOOLB...	
8	place:type=6&sort=14&maxResults=10	
9	http://www.mozilla.com/en-US/firefox/23.0.1/firstrun/	
10	http://www.mozilla.org/en-US/firefox/23.0.1/firstrun/	
11	http://www.mozilla.org/en-US/firefox/new/	
12	https://www.google.com/search?q=travel&ie=utf-8&oe=utf-8&aq=t&rls=org.m...	Do
13	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rj...	tra
14	http://www.expedia.com/	Exp
15	http://www.google.com/ack?sa=l&ai=C1E4LvN--Up2vEsSh6QH0ICwBqbEkqYB4...	
16	http://www.googleadservices.com/pagead/ack?sa=L&ai=C1E4LvN--Up2vEsSh6...	
17	http://www.kayak.com/in?ci=803-527-2209&a=gg&p=%3C%3Etravel%2FGen...	
18	http://www.kayak.com/h/xplanding/hotel-general?kw=travel&product=Hotel&k...	KA

10. Click **moz_bookmarks** to view all bookmarks.


SQLite Manager - C:\Documents and Settings\student\Application Data\Mozilla\Firefox\Profiles\2pqn2kbm...

Database: Table Index View Trigger Tools Help

Directory: places.sqlite Go

places.sqlite

Master Table (1)

Tables (13)

- moz_anno_attributes
- moz_annos
- moz_bookmarks**
- moz_bookmarks_roots
- moz_favicons
- moz_historyvisits
- moz_hosts
- moz_inputhistory
- moz_items_annos
- moz_keywords
- moz_places
- sqlite_sequence
- sqlite_stat1

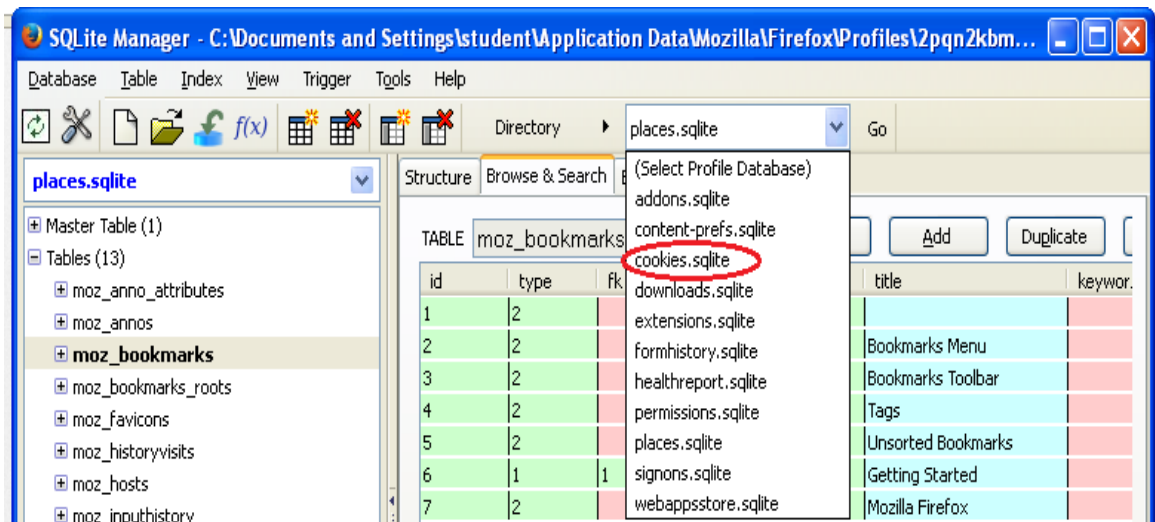
Views (0)

Indexes (22)

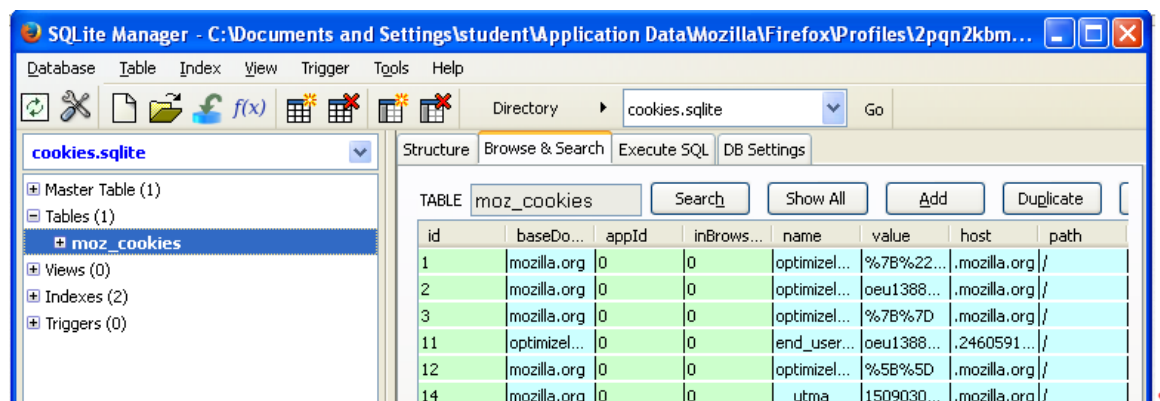
TABLE: moz_bookmarks

id	type	fk	parent	position	title
1	2	0	0	0	
2	2	1	0	0	Bookmarks Menu
3	2	1	1	1	Bookmarks Toolbar
4	2	1	2	2	Tags
5	2	1	3	3	Unsorted Bookmarks
6	1	1	3	1	Getting Started
7	2	2	3	3	Mozilla Firefox
8	1	2	7	0	Help and Tutorials
9	1	3	7	1	Customize Firefox
10	1	4	7	2	Get Involved
11	1	5	7	3	About Us
12	1	6	3	0	Most Visited
13	1	7	2	0	Recently Bookmarked
14	1	8	2	1	Recent Tags

11. From the Directory dropdown, select **cookies.sqlite** and click **Go**.



12. In the left pane, click **moz_cookies** to view the Firefox Cookies.



Other tables that you can examine:

Table	Description
Formhistory.sqlite	contains data about typed usernames, submitted inputs, and inputs in search boxes
Signons.sqlite	stores saved passwords in Firefox
Downloads.sqlite	stores data about downloaded files

13. Close all open windows and the Windows XP Pro PC Viewer.

4.2 Conclusion

Browser history can provide a wealth of information about a person. The Firefox browser is a versatile choice, because it can be used on Mac OS X, Microsoft Windows, and on Linux. The add-ons for the browser, like the SQLite Manager, help to make the browser a popular alternative to the native OS browser.

4.3 Discussion Questions

1. Browser history for Firefox is stored in what folder?
2. Mozilla Firefox stores data in what type of database?
3. What tools can be used to view the files associated with Firefox?
4. What are some reasons that Firefox is such a popular browser?



References

1. Index.dat Viewer Download:
<http://www.pointstone.com/products/index.dat-Viewer/>
2. History Viewer Download:
<http://www.historyviewer.net/>
3. SQLite Manage Add-on:
<https://addons.mozilla.org/en-US/firefox/addon/sqlite-manager/>
4. Internet Explorer History Locations:
http://www.forensicswiki.org/wiki/Internet_Explorer_History_File_Format
5. InPrivate Browsing:
<http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/in-private>

