Internet Forensics

Check Internet Browsing Activities
Browser Forensics

- civil: violate company policy by visiting certain sites
- criminal: for bomb making and drug trafficking
- time aspect: the computer was connected to a site at the time when something happened

- Common browsers
  - Internet Explorer
  - Mozilla/Firefox/Netscape Navigator

- check out
  http://www.securityfocus.com/infocus/1832
  http://www.securityfocus.com/infocus/1827
Goal

- reconstruct a detailed history of a computer’s use by examining a handful of files that contain a web browser’s past operation
- many places to find evidence:
  - web browsing history: the URLs of web sites visited
  - Favorites folder: the URLs of sites the user wants to remember
  - cookies: cookies that the computer accepted while browsing
  - temporary Internet files (the cache): a copy of the files that were used to construct the web pages on the hard drive [space-time tradeoff]
Internet Explorer
Important Folders

- **IE**
  - **Windows 2000/XP**
    - \Documents and Settings\<username>\Local Settings\Temporary Internet Files\Content.IE5
    - \Documents and Settings\<username>\Local Settings\History\History.IE5
    - \Documents and Settings\<username>\cookies
  - **Windows 95/98/ME**
    - \windows\Temporary Internet Files\Content.IE5
    - \windows\Cookies
    - \windows\History\History.IE5
  - **Windows NT**
    - \winnt\Profiles\<username>\...
Common Sense

- the information is kept in files and the user can choose to delete the files
  - deleting the info does not crash the computer; it makes the work of that user proceed slower
    - why?
  - a forensic search of the disk may be necessary

- the profile of the suspect must be examined as well as the profiles of all other accounts on the system (e.g., Administrator)
IE Cache Directory

- we can use a parser for the cache index.dat file (it is encoded), to reveal information such as
  - URL visited
  - locally cached file name
  - HTTP headers
  - file timestamps (last time accessed, last time modified, last time checked)
- the locally cache file name allows us to view the page that was displayed, which may be different than the page now at the URL
- caching is an example of space-time tradeoff (more space for less time)
Structure of the Cache

- file names and file contents are cached (stored locally) -- great for forensics because of sites with constantly changing content
- you can’t cache files under their original names (e.g., lots of collisions with all the index.html files); IE hashes the file name to reduce the effect of collisions
- an entry in the index.dat contains directory information based on the date and file name information based on the hashed names
Scenarios

- the suspect e-mails relevant documentation from a company account to his personal account, from which he can attempt to sell the information
- sending mail through a web-based e-mail provider will not go undetected
- view the cache files with a browser not connected to the Internet, to avoid having the browser follow absolute URLs, or load the cache files on an empty unconnected web server and change some tags (not forensically sound)
Cookies

- web sites run in a stateless mode: no connection contains information about the state of the session
- cookies are used by a web site to store values on the client that create a web session (e.g., items in your shopping cart); in a sense, they can be used to track you, as each one contains a username
- two types of cookies: session and persistent
  - session cookies are stored in memory
  - persistent cookies are stored on disk
More Cookies

- Each persistent cookie is saved as a small text file containing names and values, the time the cookie was downloaded, the time the cookie expires, and status information; this index.dat stores the history of cookies, not the history of URLs.

- There are no restrictions on what a web site may write as text in a cookie.
- E.g., Mapquest stores the address you entered in a cookie; that is why you see it the next time.

- This information needs to be parsed.
Favorites

• the Favorites folder contains the URLs of web sites saved by the user, probably because they are of interest to the user and are frequently visited
  • explicit storing of these links indicates intent
  • look at C:\Documents and Settings\<username>\Favorites
• for users who move between computers, the Favorites folder is often copied to these computers, perhaps in other locations on the disk
Viewing Favorites

- at least copy the Favorites folder to a clean forensic workstation and view the URL links independently over an Internet connection
- one view presents the Date Modified, which is the date when the link was added to the folder
- investigate subfolders
- the link Name defaults to the <title> tag in the HTML of the page
  - this is user-changeable, so do not be fooled by the name; Right-click on the link, select Properties then Web Document to see the real URL
Time: Back to the Past

- what you are seeing on the clean forensic workstation are the contents of the URL now, not necessarily on the date that the user visited the site.
- to view sites the way they appeared at that time, try the Way Back machine at http://www.archive.org
Site Re-direction

- one more place to check, the folder C:\WINDOWS\system32\drivers\etc which contains a text file named hosts
- this is used by Windows to resolve web host names before checking over the network with the Domain Name Server (DNS)
  - this is useful for testing, but it can be used to hide the tracks of nefarious web activity
  - someone might substitute 69.128.0.1 for cbc.ca

- Favorites can be exported to a local HTML file, with the default name Bookmarks.htm; look for this file as well
History Files

• a list of web sites visited, with times
• the URL listed (e.g., http://www.acme.com) may be the actual string typed (URL) or it may be another site chosen by web server balancing
• in IE, look at C: \Documents and Settings \<username> \Local Settings \History
• might use a utility like NetAnalysis or Pasco for easy viewing and analysis
The Registry

- when a user types information (names, addresses, passwords) into a form field, IE offers to remember the info (to speed up future typing); this info is stored encrypted in the Registry
  - software like Windows Secret Explorer (LastBit) can view it

- typed URLs: when you type a specific URL in the address bar (no click), the URL is stored in the Registry in a separate location from the History info -- this info shows intent
The Clean Forensic Workstation (CFW)

- It should have an empty cache, an empty cookie directory, and an empty history file.
- If you copy the cookies from the suspect computer and visit the web sites in the history file, the web sites will think that the CFW is the suspect user/computer and will potentially cough up information (e.g., on books ordered).
- If the CFW is off-line and has its cache filled with the suspect cache entries, typing a cached URL into the address bar of the browser will cause the local cached copy to be displayed.
More on History

- the index.dat file contains a record of all URLs visited during the History period
- this is used for AutoComplete on the browser address bar and for visited link highlighting
  - when you begin typing “www” in the address bar and a list of sites starting with that appears, this is the file being used (sites that were clicked on)
  - when a list of URL links appears in two different colours on a page, the ability to distinguish between visited and not-yet-visited comes from the index.dat file
- check for filler data with value 0B AD FO 0D
Commercial Tools

- Encase
- FTK
Open Source Web Browing Analysis Tools
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>History File: index.dat Version: 5.2</td>
<td>MODIFIED TIME</td>
<td>ACCESS TIME</td>
<td>FILENAME</td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td>3/10/2005 17:45</td>
<td>B1563000[1].htm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Command Prompt:

```
C:\Documents and Settings\kjas\Desktop\Content.IES\dir /s
```

Directory of C:\Documents and Settings\kjas\Desktop\Content.IES

```
03/18/2005 11:40 AM 0196 bytes 294.912 index.dat
03/18/2005 11:40 AM 0196 bytes 294.977 bytes
03/18/2005 11:40 AM 0196 bytes 294,977 bytes Free
```

```
pasco (options) < filename >
```

```
-d No date
-t Field Delimiter (TAB by default)
```
Galetta

- Cookie parsing utility
Firefox
Where are the histories stored

- **Firefox**
  - used in the open source community
  - designed for cross-platform compatibility, so the forensic metadata that it keeps is in industry-standard file names, as opposed to the way Microsoft IE does it
  - \Documents and Settings\<username>\Application Data\Mozilla\Firefox\Profiles\<random text>\history.dat

- **Mozilla/Netscape**
  - \Documents and Settings\<username>\Application Data\Mozilla\Profiles\<random text>\history.dat
Firefox History

- the history file is at
  C:\Documents and Settings\<username>\Application Data\Mozilla\Firefox\Profiles\<profilename>\history.dat
- the file needs to be parsed, perhaps with NetAnalysis
- the field of # of times the URL has been accessed is useful; anything greater than 1 tells us the user did not accidentally visit the site
Firefox Cookies

- All cookies for a user are stored in
  `C:\Documents and Settings\<username>\Application Data\Mozilla\Firefox\Profiles\<profilename>\cookies.txt`
- It is human-readable
Firefox Caching

- relatively easy
- the actual place for the temporary Internet files is `C:\Documents and Settings\<username>\Local Settings\Temp`
- you can also fire up Firefox and type about:cache in the browser address bar
- you see Memory Cache Device and Disk Cache Device; we are interested typically in the disk
Website Forensics
Police office got an anonymous phone call reporting a possible child pornography website
Website

- A collection of Webpages on a WWW server
  - text, picture, video/audio
- HTML
- http://www.utica.edu
- Could be script based
What you saw in the browser is not all
Capture the page

- Screenshot
- Save as
- Website capture tools
- Site may have changed since the initiation of the investigation
Locating and seizing the Web server

- What can you get?
  - Content and source files
  - Transaction logs
  - Username/passwords, payment histories
- How to locate the Web server?
Other considerations

- Suspect may be monitoring traffic to the site
  - Don’t use known LE computers