Forensics – Week 12

Web Forensics & Searching the Network

Web Forensics

Purpose of Investigation

- Theft of intellectual property
- Misuse of company resources
- Stalking
- Possession or distribution of contraband

Internet Addressing

- Uniform Resource Locator (URL) points to a specific object with Internet availability
- Scheme identifies protocol used to access the resource (http, https, ftp, etc.)
- Domain name points to the specific network
- Suffix (.com, .edu, etc.) points to top level domain
- All together, they make the fully qualified domain name

Browsers

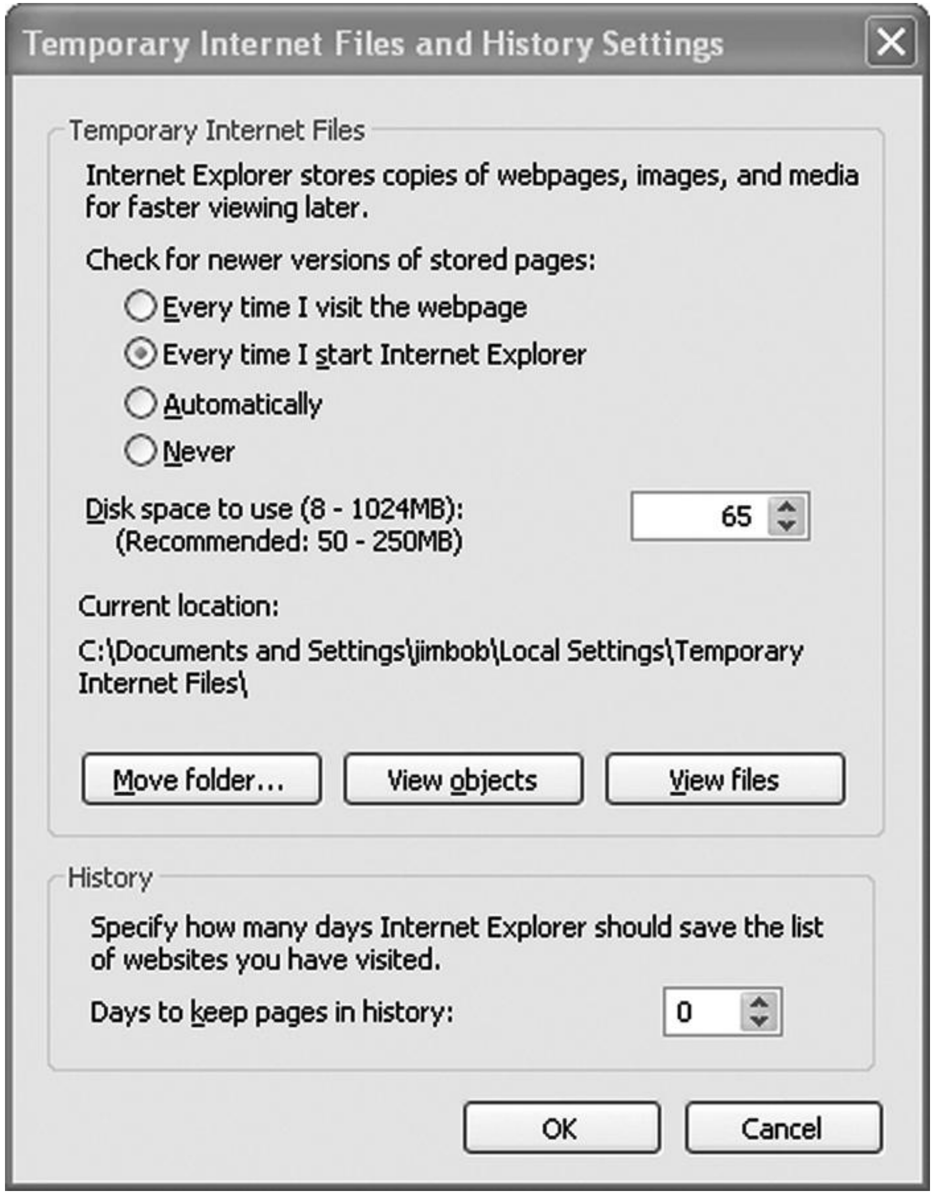
- Uses markup language to open web pages
- Hyperlinks redirect user to specific resources
- Content can be either web pages or files that are the targets of hyperlinks

Function of Browsers

- An address bar (manual mapping to URL)
- Forward and Back buttons
- Bookmarking capabilities
- Intrapage search capabilities
- Configuration utilities

Artifacts of Browsing

- Internet history
- Cookies
- Temporary Internet files
- Registry entries



Temporary Internet Files and History Settings

Temporary Internet Files

Internet Explorer stores copies of webpages, images, and media for faster viewing later.

Check for newer versions of stored pages:

○ Every time I visit the webpage
● Every time I start Internet Explorer
○ Automatically
○ Never

Disk space to use (8 - 1024MB): 65
(Recommended: 50 - 250MB)

Current location:

C:\Documents and Settings\jimbob\Local Settings\Temporary Internet Files\

History

Specify how many days Internet Explorer should save the list of websites you have visited.

Days to keep pages in history: 0

Deleting Temporary Files

- Browser settings can be adjusted to automatically delete files upon closing the browser
  - Temporary files can be recovered the same as any other deleted file
  - Cookies may or may not be included, depending on the browser and its configuration
- Internet history files and cache files are not the same

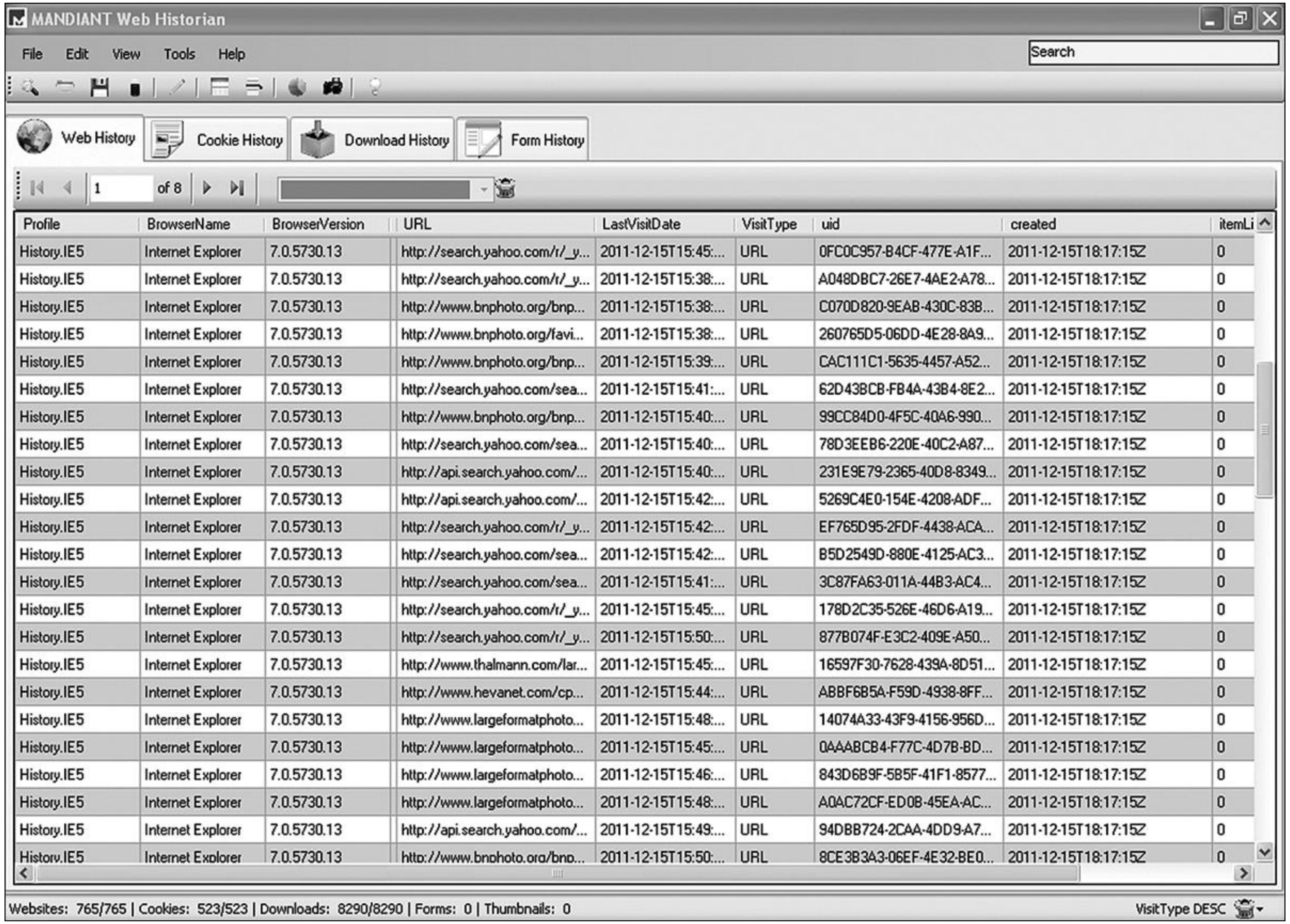
Browser History

- A database of recently visited sites
- Cache files are stored separately
- Each operating system/browser combination has a different default location for history and cache files
- Some utilities that analyze Internet usage can automatically detect browser settings

Browser History Analysis Tools

- Nirsoft (www.nirsoft.net) makes available a number of different browser analysis tools as open source freeware. These include specialized history tools for IE, Firefox, Safari, Chrome, and Opera.
- The Linux forensic application The Sleuth Kit does an excellent job of analyzing Internet history on most browsers.
- Web Historian is useful whenever the investigator is unsure which browser may have been used. This utility scans the directory structure of the computer and identifies valid history files for IE, Mozilla, Netscape, Safari, and Opera.
- Web Historian analyzes the files it finds and has the ability to output data into Excel format, HTML, or a comma-delimited text file that can be imported into virtually any database application. When data is output to a spreadsheet or database, an investigator can sort information in a variety of ways. Sorting by timestamp and then by URL is a good way to generate a timeline of activity.

Browser History Analysis Tools



Profile	BrowserName	BrowserVersion	URL	LastVisitDate	VisitType	uid	created	itemLi
History.IE5	Internet Explorer	7.0.5730.13	http://search.yahoo.com/r/_y...	2011-12-15T15:45:...	URL	0FC0C957-B4CF-477E-A1F...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://search.yahoo.com/r/_y...	2011-12-15T15:38:...	URL	A048DBC7-26E7-4AE2-A78...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://www.bnphoto.org/bnp...	2011-12-15T15:38:...	URL	C070D820-9EAB-430C-83B...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://www.bnphoto.org/favi...	2011-12-15T15:38:...	URL	260765D5-06DD-4E28-8A9...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://www.bnphoto.org/bnp...	2011-12-15T15:39:...	URL	CAC111C1-5635-4457-A52...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://search.yahoo.com/sea...	2011-12-15T15:41:...	URL	62D43BCB-FB4A-43B4-8E2...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://www.bnphoto.org/bnp...	2011-12-15T15:40:...	URL	99CC84D0-4F5C-40A6-990...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://search.yahoo.com/sea...	2011-12-15T15:40:...	URL	78D3EEB6-220E-40C2-A87...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://api.search.yahoo.com/...	2011-12-15T15:40:...	URL	231E9E79-2365-40D8-8349...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://api.search.yahoo.com/...	2011-12-15T15:42:...	URL	5269C4E0-154E-4208-ADF...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://search.yahoo.com/r/_y...	2011-12-15T15:42:...	URL	EF765D95-2FDF-4438-ACA...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://search.yahoo.com/sea...	2011-12-15T15:42:...	URL	B5D2549D-880E-4125-AC3...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://search.yahoo.com/sea...	2011-12-15T15:41:...	URL	3C87FA63-011A-44B3-AC4...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://search.yahoo.com/r/_y...	2011-12-15T15:45:...	URL	178D2C35-526E-46D6-A19...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://search.yahoo.com/r/_y...	2011-12-15T15:50:...	URL	877B074F-E3C2-409E-A50...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://www.thalmann.com/lar...	2011-12-15T15:45:...	URL	16597F30-7628-439A-8D51...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://www.hevanet.com/cp...	2011-12-15T15:44:...	URL	ABBF6B5A-F59D-4938-8FF...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://www.largeformatphoto...	2011-12-15T15:48:...	URL	14074A33-43F9-4156-956D...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://www.largeformatphoto...	2011-12-15T15:45:...	URL	0AAABCB4-F77C-4D7B-BD...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://www.largeformatphoto...	2011-12-15T15:46:...	URL	843D6B9F-5B5F-41F1-8577...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://www.largeformatphoto...	2011-12-15T15:48:...	URL	A0AC72CF-ED0B-45EA-AC...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://api.search.yahoo.com/...	2011-12-15T15:49:...	URL	94DBB724-2CAA-4DD9-A7...	2011-12-15T18:17:15Z	0
History.IE5	Internet Explorer	7.0.5730.13	http://www.bnphoto.org/bnp...	2011-12-15T15:50:...	URL	8CE3B3A3-06EF-4E32-BE0...	2011-12-15T18:17:15Z	0

Websites: 765/765 | Cookies: 523/523 | Downloads: 8290/8290 | Forms: 0 | Thumbnails: 0

VisitType DESC

Browser History

- Internet Explorer stores information useful to the investigator in at least three different places. Users Windows 2000 and earlier
  - C:\Documents and Settings\@user:\Local Settings\Temporary Internet Files\Content.IE5\. This is the default location IE uses for putting pages and images viewed by that particular user.
  - C:\Documents and Settings\@user:\Local Settings\History\History.IE5\ stores a noncached history without the actual pages and images.
  - Cookies are generally stored in C:\Documents and Settings\@user:\Cookies\.
- Windows 7 , 8, 8.1 and 10
  - C:\Users\@user:\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5.
  - Cookies
    - C:\Users\@user:\AppData\Roaming\Microsoft\Windows\Cookies
    - C:\Users\@user:\AppData\Roaming\Microsoft\Windows\Cookies\Low

Analyzing User Activity

- Cookies generally identify the website from whence they came
- History records are a database file that shows user activity (may be deleted periodically)
- Temporary Internet files can be recovered by file recovery utilities even if automatically deleted

History Files

- URL
- File Name: as it exists on the local system
- Record Type: browsed or redirected
- Access Time: time the file was last accessed
- Modified Time: time the file was last changed
- Directory Name: local directory in which the file is stored
- HTTP Headers: as originally received

Finding “Stuff” is Not Enough

- The defendant has knowledge of possession of contraband
- The defendant took specific actions to obtain the contraband
- The defendant had control over the contraband
- If deleted, the defendant took active measures to destroy the actual materials
- There was sufficient quantity of contraband to justify prosecution

Knowledge of Possession

- “Present Possession” concept: The user must know that it is there
- Redirected sites will store temporary files and images without notifying the user
- Any attempt to manipulate or manually delete the file suggests knowledge of possession
- But what user was logged on when these actions took place?

Knowledge of Possession (Case Example)

- Evidence of deleted files has been accepted as evidence that the user knew of the material’s existence.
- In *The United States v. Tucker* , the defendant claimed that he had no knowledge of possession because the computer automatically stored the images in cache without any intervention on his part.
- The court finding disagreed with that argument, stating in its decision that possession “is not only evidenced by his showing and manipulation of the images, but also by the telling fact that he took the time to delete the image links from his computer cache file.”
- This demonstrated knowledge of existence and the ability to control the image.

Establishing User Actions

- Repeated searches suggest intent
- Innocent searches can bring up unexpected content
- Popups are not under the control of the user
- Meta-refresh will automatically redirect the user against their will
- The TypedURL registry entry proves that a website was accessed intentionally

Establishing User Actions (Case Example)

- It is true that many Web sites launch obnoxious pop-up windows that the user did not wish to see and had no intention of launching; however, repeated searches can reveal intent.
- In *The State of Florida v. Casey Marie Anthony* (2008), the digital investigators were able to demonstrate that Anthony had performed numerous searches for chloroform and its effects.
- This was in spite of the fact that Anthony had made a concerted effort to erase her browser’s history.
- Prosecutors used the searches as the foundation for showing premeditation in the act.
- While the defendant was found not guilty in this particular case, it is still a good illustration of how this type of evidence is used in real-life situations.

Establishing Control of Material

- The Trojan Horse defense (the Devil made me do it)
  - A malware analysis can prove or disprove this claim
  - But rootkits can foil the malware analysis
- Accessing a file a significant time after the original create date suggests control
- Manually deleting or editing a file suggests control

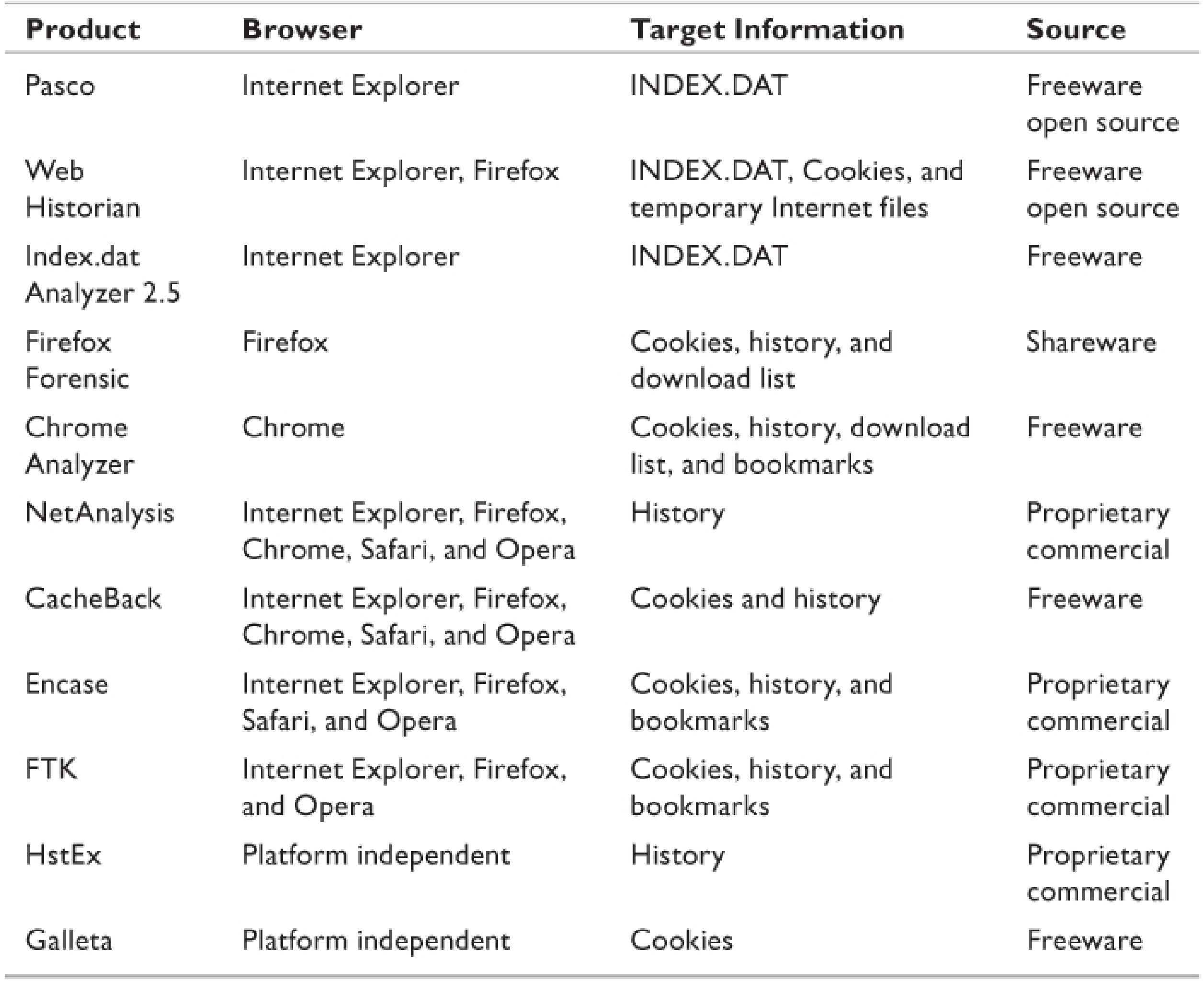
Determining Active Measure

- Intentional deletion
  - Many document management solutions automatically audit file deletions and indicate what user initiated the action, along with an exact time and date
- Modify dates after the create date
- Moving a file from one location to another
- Renaming a file

Determining Sufficient Quantity

- That’s not your job – leave it to the legal team
- Your job is only to ascertain the quantity

Tools for Browser Analysis



Product	Browser	Target Information	Source
Pasco	Internet Explorer	INDEX.DAT	Freeware open source
Web Historian	Internet Explorer, Firefox	INDEX.DAT, Cookies, and temporary Internet files	Freeware open source
Index.dat Analyzer 2.5	Internet Explorer	INDEX.DAT	Freeware
Firefox Forensic	Firefox	Cookies, history, and download list	Shareware
Chrome Analyzer	Chrome	Cookies, history, download list, and bookmarks	Freeware
NetAnalysis	Internet Explorer, Firefox, Chrome, Safari, and Opera	History	Proprietary commercial
CacheBack	Internet Explorer, Firefox, Chrome, Safari, and Opera	Cookies and history	Freeware
Encase	Internet Explorer, Firefox, Safari, and Opera	Cookies, history, and bookmarks	Proprietary commercial
FTK	Internet Explorer, Firefox, and Opera	Cookies, history, and bookmarks	Proprietary commercial
HstEx	Platform independent	History	Proprietary commercial
Galleta	Platform independent	Cookies	Freeware

Investigating Web Servers

- Server log files
  - Access logs
  - Error logs
- Proxy Servers

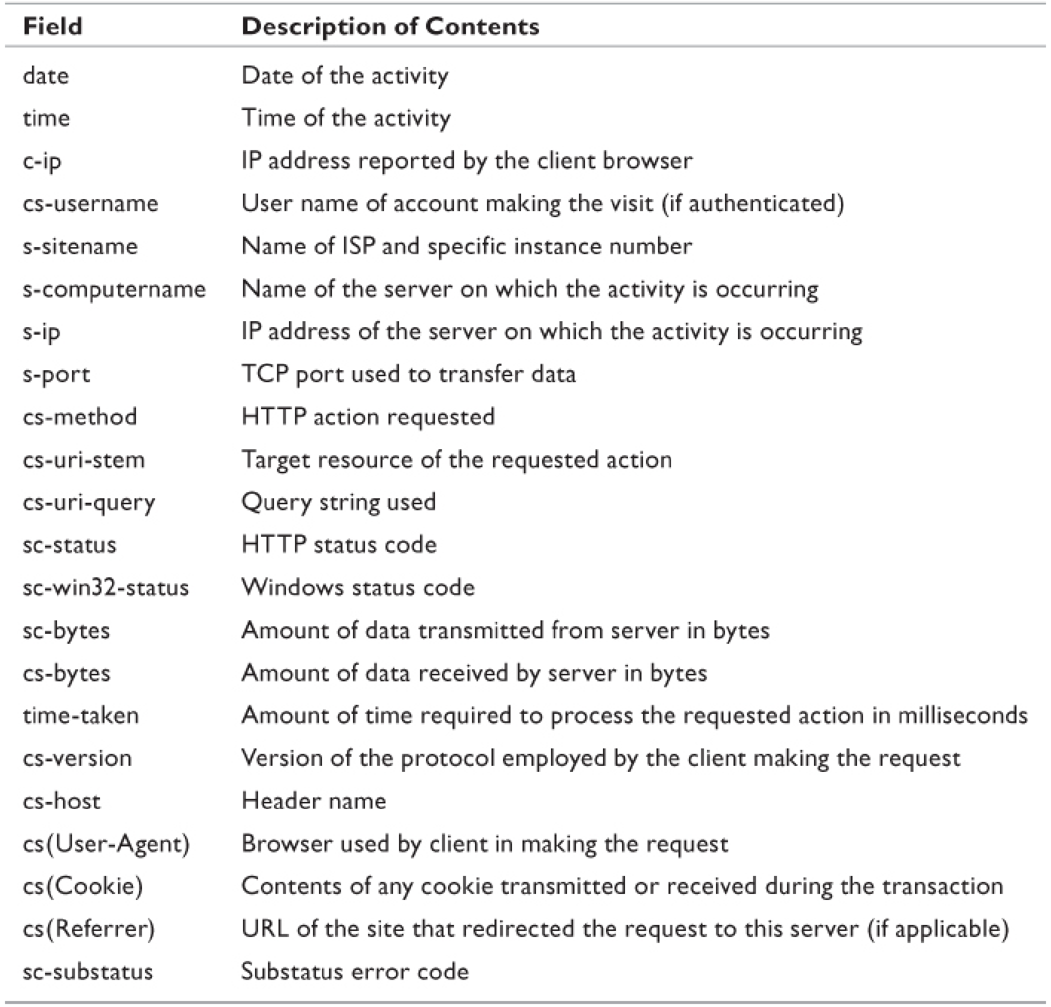
Web Server Log Files

- IIS Log Files: These files are generally the most interesting to the investigator, as they contain information about all client requests against the Web server. By default, these files are located in the c:\%system%\system32\LogFiles\W3SVC1 directory. The files have a conventional naming system of EXxxxxxx.log, where xxxxxx is a number generated by IIS.
- IISMSID: Logs Mobile Station Identifiers. A mobile station identifier is a number associated with a wireless service provider that identifies a particular unit on the network. This log is only present on a Microsoft Web server if the MSIDFILT or CLOGFILT functions are enabled.
- HTTPERR: HTTPERR logs record all invalid requests made to the Web server. These files are stored in the %systemroot%\System32\LogFiles\HTTPERR directory.
- URLSCAN: The URLSCAN tool is a utility that can be installed on a Microsoft Web server that allows the administrator to block specific HTTP requests. If the tool is installed on the Web server (and unless logging is disabled), a log file records all denied requests. By default the file is located in the directory %systemroot%\inetsrv\urlscan\logs.

Analyzing Log Files

- The server logs provide a large amount of information about any given HTTP transaction that the investigator can use in determining what happened and the order of events.
- While each type of Web server differs somewhat in how it records its log files, Microsoft Internet Information Service is fairly typical of most server logs. The next slide lists the significant fields recorded in an IIS server log.
- It should be noted that since IIS uses W3C format, the content contained by the files may be customized by the Webmaster.
- Some of these fields may be absent.

Analyzing Log Files



Field	Description of Contents
date	Date of the activity
time	Time of the activity
c-ip	IP address reported by the client browser
cs-username	User name of account making the visit (if authenticated)
s-sitename	Name of ISP and specific instance number
s-computername	Name of the server on which the activity is occurring
s-ip	IP address of the server on which the activity is occurring
s-port	TCP port used to transfer data
cs-method	HTTP action requested
cs-uri-stem	Target resource of the requested action
cs-uri-query	Query string used
sc-status	HTTP status code
sc-win32-status	Windows status code
sc-bytes	Amount of data transmitted from server in bytes
cs-bytes	Amount of data received by server in bytes
time-taken	Amount of time required to process the requested action in milliseconds
cs-version	Version of the protocol employed by the client making the request
cs-host	Header name
cs(User-Agent)	Browser used by client in making the request
cs(Cookie)	Contents of any cookie transmitted or received during the transaction
cs(Referrer)	URL of the site that redirected the request to this server (if applicable)
sc-substatus	Substatus error code

Searching the Network

Purpose of Investigation

- Internal investigations
- Misuse of company resources
- Penetration analysis
- Intrusion detection

Scope of the Investigation

- Local area networks
- Application Service Providers (ASP)
- Cloud computing

Initial Response

- Identify the actual problem
- Decide on an action
    - Should the connections be broken or back-traced?
    - Is conviction worth the risk of data loss?
- Lock down a time frame
- Isolate the source of the nefarious activity
- Identify the potential suspect(s)

Point of a Response Plan

- Have a list of IT personnel available
- Have tools in place for analyzing network activity
- Prepare secure lines of communication that can’t be tapped
- Create and test a plan of action for returning systems to normal
- Have a good review process in place

When to do Proactive Collection

- Current and ongoing intrusions
- Ongoing theft of data
- Misuse of company resources
- Suspicion of data export
- Internal systems may have been compromised
- When ascertaining whether malicious software has been embedded in the system
- To determine how the intrusion was accomplished

Proactive Methods

- Keyloggers
  - Can be hardware or software based
  - May be subject to legal challenge
- System auditing
  - Know what to audit and how
  - Collect audit logs before they are automatically deleted

Keyloggers

- Keyloggers, whether software or hardware based, fall under the category of interception devices. This is based on a court decision that “interception occurs when a communication is captured or redirected in any way” (*U.S. v. Rodriguez* 1992). As such, their use is governed by federal and state law.
- In the corporate environment, it generally will not be a problem to insert keystroke loggers into any computer system owned by the company. To be safe, the company should have each employee read and sign a standard policy document that defines what rights the company reserves in this regard.
- *United States v. Simons* established that the presence of an established company policy, combined with a legitimate business interest in monitoring employee conduct, dispelled any perceived expectation of privacy
- In *United States v. Nicodema S. Scarfo, et al.,* the court held that the use of a keystroke logger did not violate the ECPA. However, in this case, the software was designed specifically to work only when the computer was not hooked up to the modem.

Network Capture

- Determining authenticity
  - Proxy servers alter IP addresses
  - Onion routing encapsulates original packets
  - IP spoofing rewrites the originating IP address
- Identifying traffic
  - Narrow the range of targeted traffic
  - Identify a specific acquisition window

Performing a Network Capture

- Put network interface into promiscuous mode
- Configure utility (such as Wireshark) to collect packets
- Identify and configure a storage pool for captured traffic

Analyzing the Capture

- Protocol identification
- IP address inventory
- Message sessionizing
  - A to B
  - B to A
  - A or B to any

Collecting Live Connection Data

- A small batch file can collect:
  - Time/data information
  - NetBIOS connections
  - User statistics
  - File shares open
  - Open sessions
- Collect information only as it currently exists

Post Incident Collection

- Event logs
  - Application log
  - Security log
  - System log
- Application logs (not Windows)

Router and Switch Forensics

- Don’t analyze device over network
- Enable logging before connecting to the device
- Record all volatile information first
- Record time-date stamps

Router Data to Collect

- Router OS
- Router logs
- Startup and running configurations
- Routing tables
- Access lists
- NAT translation tables
- List of interfaces