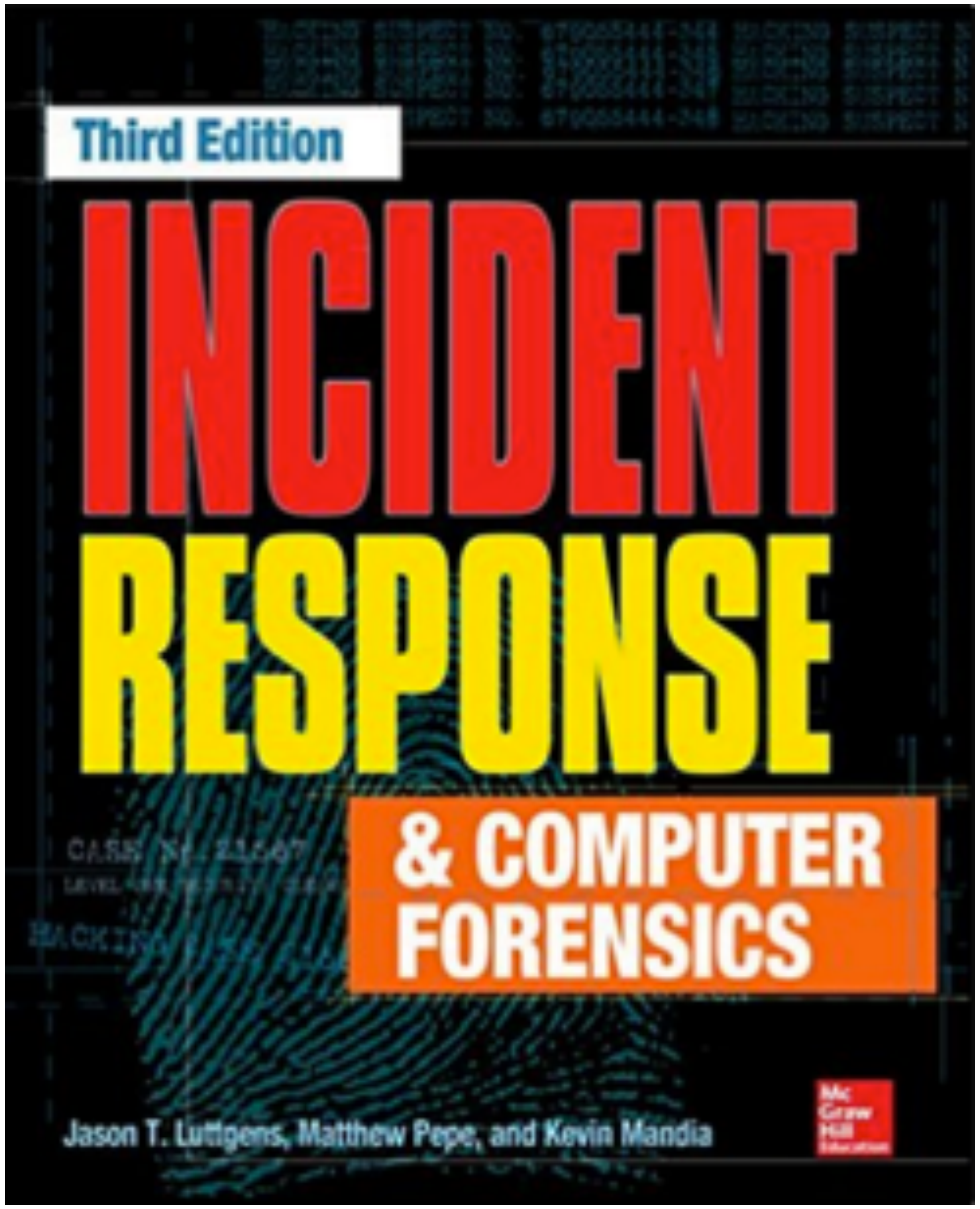
CNIT 121: Computer Forensics



14 Investigating Applications

Applications

- **Not part of the operating system**
- **User applications**
  - **Internet browsers, email clients, office suites, chat programs, and more**
- **Service applications**
  - **Web servers, database servers, email servers, etc.**

Application Data

- **Many different formats**
  - **Text, binary, open- and closed-source**
  - **Sometimes independent of the operating system**
- **Most commonly relevant**
  - **Email clients, web browsers, and instant messaging clients**

Where is Application Data Stored?

Windows

- **Default application installation directory**
  - **C:\Program Files**
  - **C:\Program Files (x86)**
    - **For 32-bit apps on a 64-bit OS**
- **Default application data directory**
  - **C:\Program Data**
  - **C:\Users\*username*\AppData**

Windows

- **Registry uninstall information**
  - **HKLM\SOFTWARE\Microsoft\CurrentVersion\Uninstall**
    - **Value: InstallLocation**
  - **On 64-bit Windows, check HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall**

Windows

- **Default registry configuration data locations**
  - **HKLM\SOFTWARE**
  - **On 64-bit systems, HKLM\SOFTWARE \Wow6432Node**

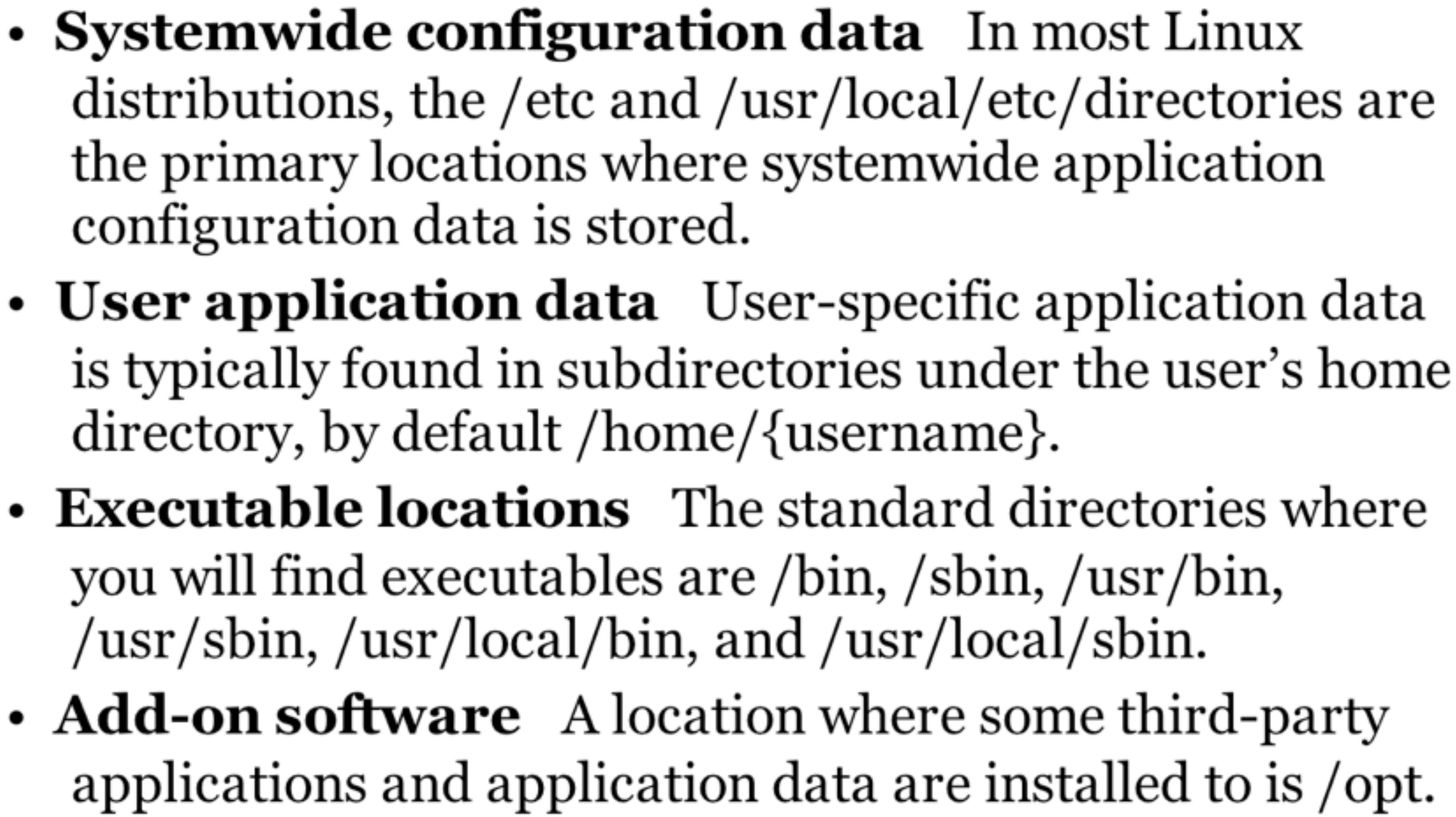
OS X

- **Default application installation directory**
  - **/Applications**
- **Application user data directory**
  - **/Users/*username*/Library/Application Support**

Linux

- Locations vary based on distribution and customizations
- Two ways to locate application data
  - Manually inspect the file system
  - Query the package manager

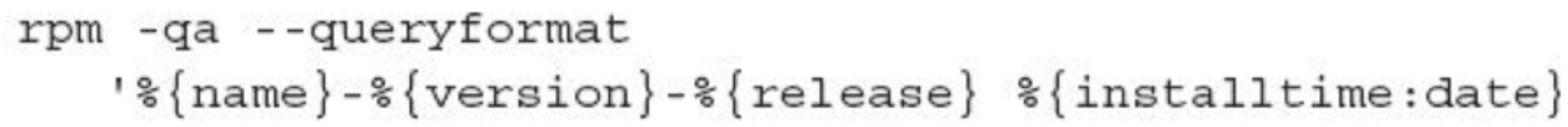
Filesystem Hierarchy Standard (FHS)



- **Systemwide configuration data** In most Linux distributions, the /etc and /usr/local/etc/directories are the primary locations where systemwide application configuration data is stored.
- **User application data** User-specific application data is typically found in subdirectories under the user's home directory, by default /home/{username}.
- **Executable locations** The standard directories where you will find executables are /bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, and /usr/local/sbin.
- **Add-on software** A location where some third-party applications and application data are installed to is /opt.

Package Managers

- **RPM (RPM Package Manager)**
  - **Used by Red Hat Enterprise Linux (RHEL), CentOS, OpenSUSE, and Fedora**
  - **This command shows all installed packages and the date installed**



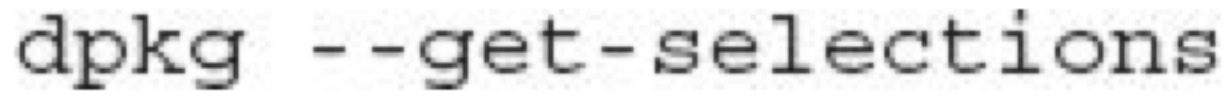
```
rpm -qa --queryformat
   '%{name}-%{version}-%{release} %{installtime:date}
```

Package Managers

- **Yellowdog Updater, Modified (yum)**
  - **Used in conjunction with RPM on some distributions**
  - **Log in /var/log/yum.log shows history of packages installed, updated, and erased**

Package Managers

- **Debian-based distributions**
    - **Including Ubuntu and Knoppix**
    - **dpkg package manager**
    - **Packages have .deb extension**
    - **This command gives a basic list of installed packages**



```
dpkg --get-selections
```

Package Managers

- **Dpkg log is in /var/log/dpkg.log**
- **Ubuntu also uses the Advanced Package Tool (apt)**
- **Log files in /var/log/apt directory**

General Investigation Methods

Research

- **Determine what artifacts an application creates that may be helpful to an investigation**

- **Some applications are not well documented**

- **For criminal cases and other serious matters, consider hiring a forensics expert to assist**

- **Performing your own research may be acceptable for less serious matters**

Resources

- **Forensic Focus**
- **Forensics Wiki**
- **Support or message boards maintained by the application developers**
- **Private message boards for commercial forensic software**
  - **EnCase and FTK**

Research Steps

- **Configure an environment**
- **Obtain the application**
- **Configure instrumentation**
- **Perform installation**
- **Execute the application**
- **Review instrumentation data**
- **Adjust instrumentation and re-perform testing as needed**

Environment

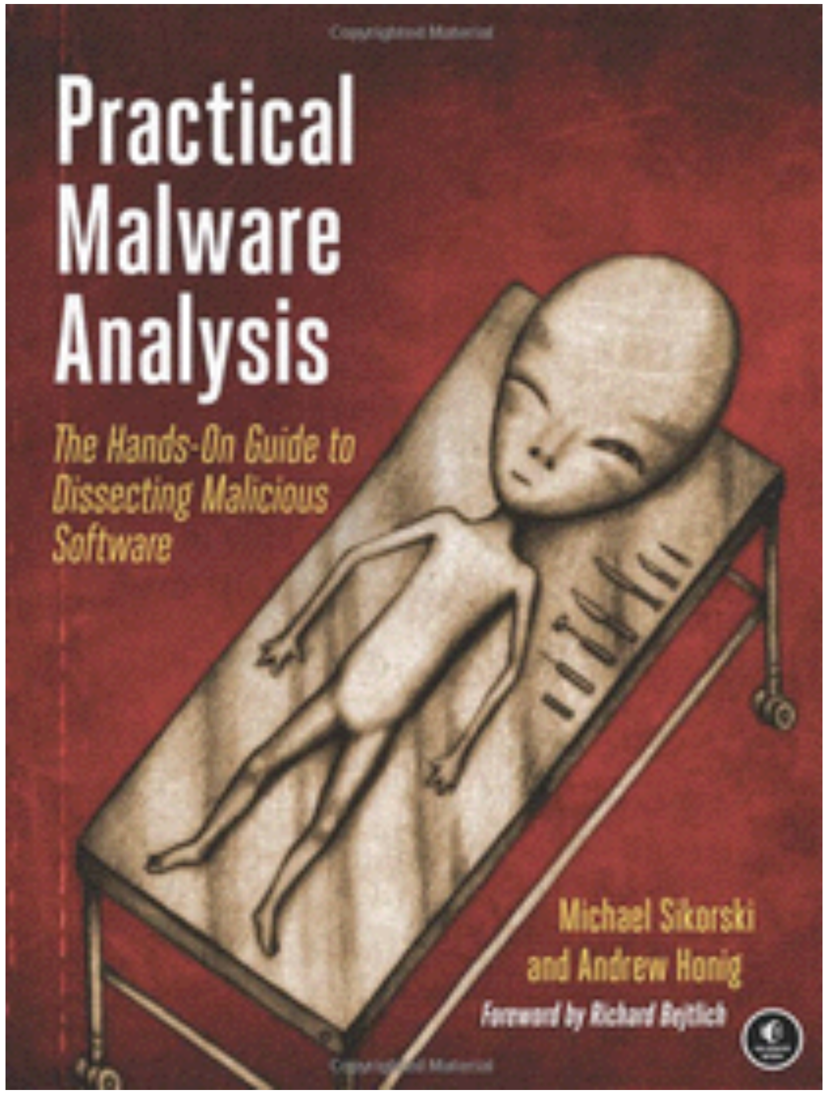
- **Typically a virtual machine with snapshot capability**
- **You will frequently need to re-run tests**

Instrumentation

- **Software or tools to monitor execution**
- **Identify potential artifacts of interest**
- **WIndows: Process Monitor**
- **OS X: dtruss**
- **Linux: strace displays all syscalls that a process makes**

Malware Analysis

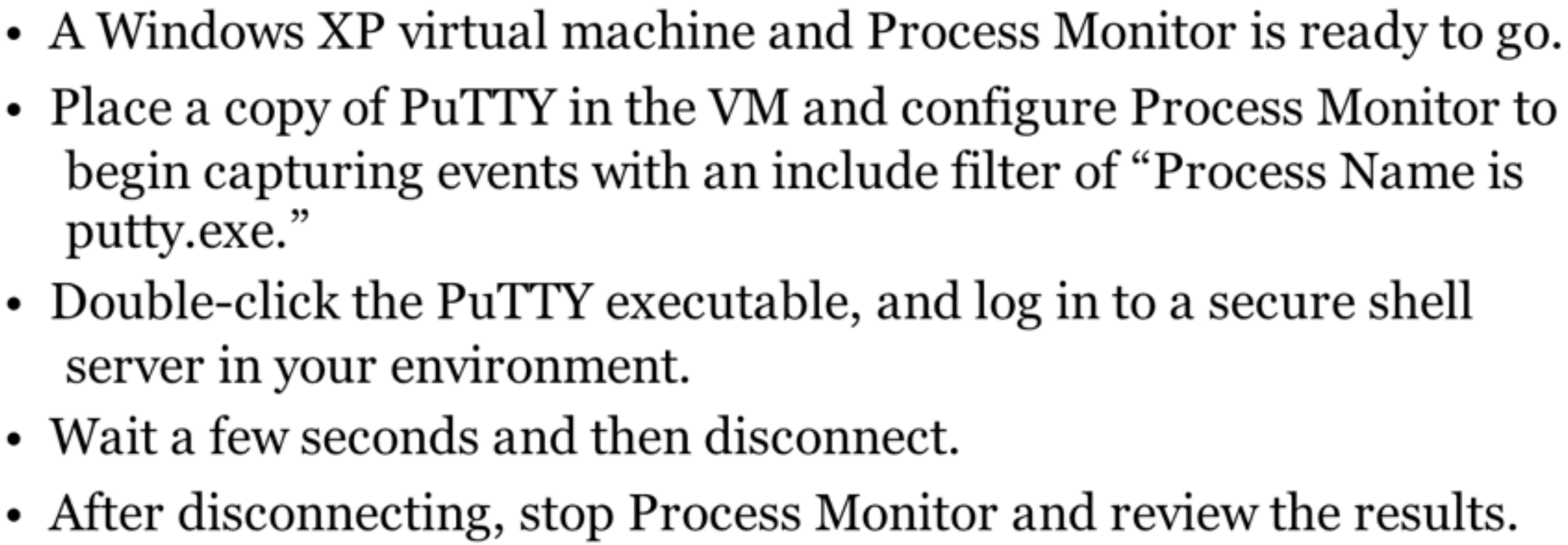
- **CNIT 126**
- **Next semester**


Copyrighted Material
Practical Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich
Copyrighted Material

Example

- **Prefetch folder contains PuTTY, an SSH client**
  - **PuTTY is no longer installed on the system**
- **Can you determine what servers the attacker connected to?**

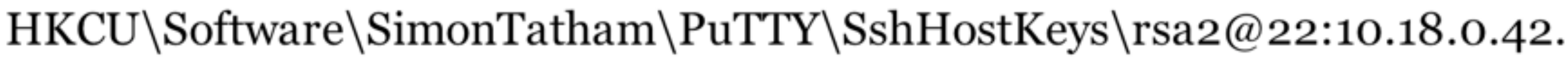
Analysis



- A Windows XP virtual machine and Process Monitor is ready to go.
- Place a copy of PuTTY in the VM and configure Process Monitor to begin capturing events with an include filter of “Process Name is putty.exe.”
- Double-click the PuTTY executable, and log in to a secure shell server in your environment.
- Wait a few seconds and then disconnect.
- After disconnecting, stop Process Monitor and review the results.

Results in Process Monitor

- **463 events captured over 16 seconds**
- **No file activity**
- **This RegSetValue operation**



HKCU\Software\SimonTatham\PuTTY\SshHostKeys\rsa2@22:10.18.0.42.

Jumping to Conclusions

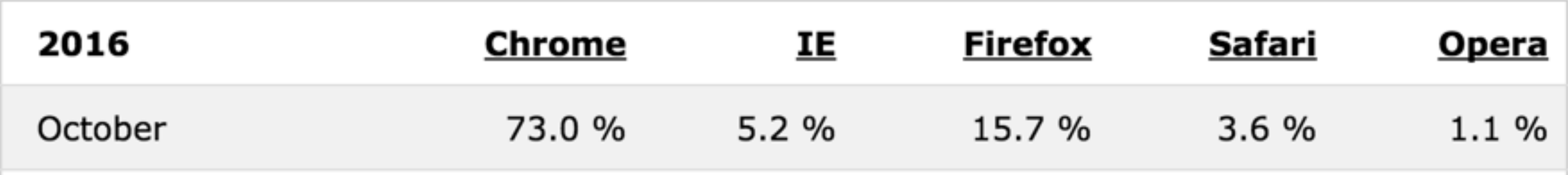
- **"Simon Tatham"**
    - **Not the user**
    - **The author of PuTTY**

Issues

- This key may show servers PuTTY connected to
- But there won't be timestamps
  - Registry timestamps are on keys, not values
- This hive is user-specific
  - Search each user's hive to find all the evidence

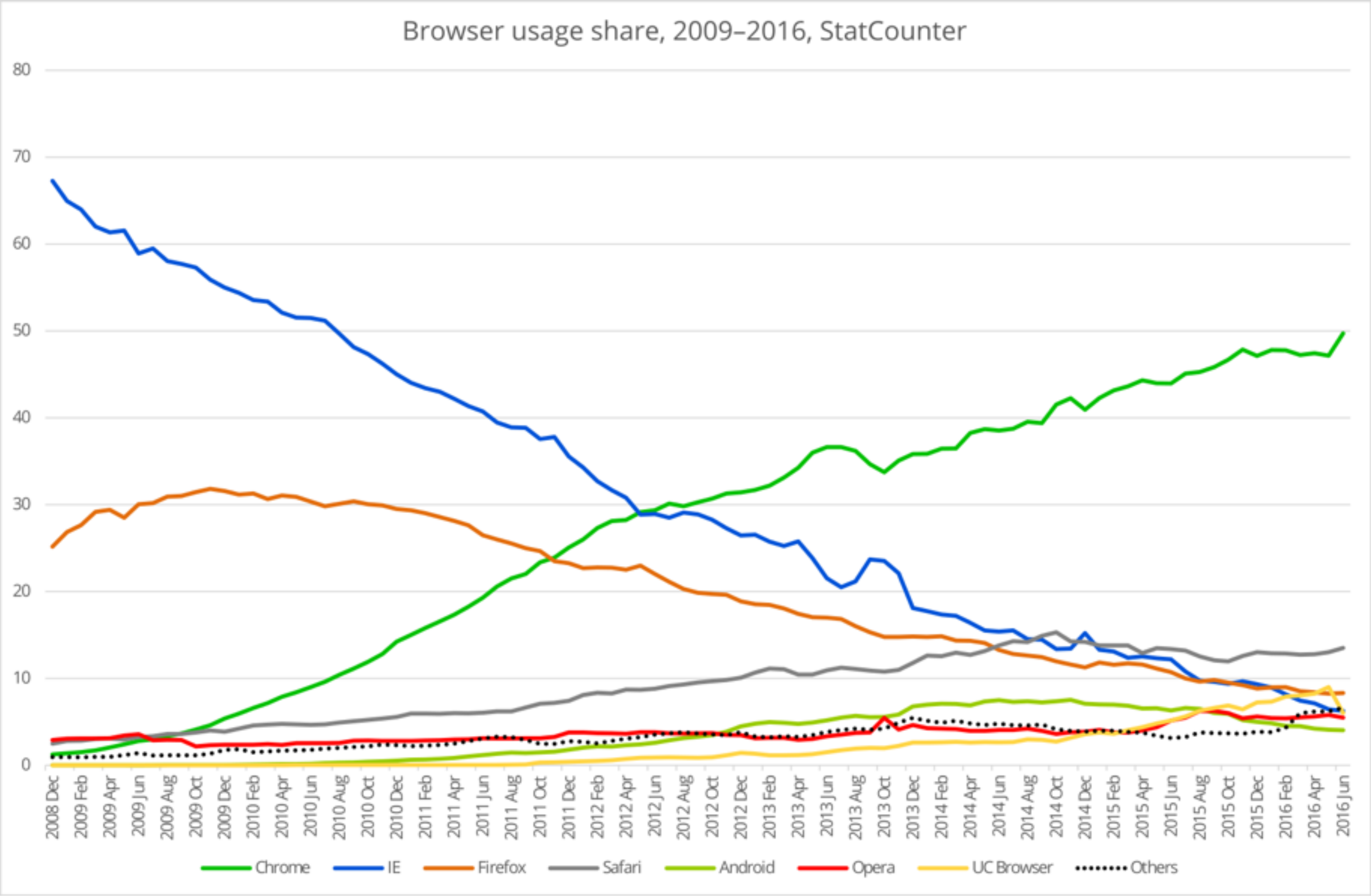
Web Browsers

Browser Popularity



2016	Chrome	IE	Firefox	Safari	Opera
October	73.0 %	5.2 %	15.7 %	3.6 %	1.1 %

- **Link Ch 15g**


Browser usage share, 2009–2016, StatCounter
80
70
60
50
40
30
20
10
0
2008 Dec
2009 Feb
2009 Apr
2009 Jun
2009 Aug
2009 Oct
2009 Dec
2010 Feb
2010 Apr
2010 Jun
2010 Aug
2010 Oct
2010 Dec
2011 Feb
2011 Apr
2011 Jun
2011 Aug
2011 Oct
2011 Dec
2012 Feb
2012 Apr
2012 Jun
2012 Aug
2012 Oct
2012 Dec
2013 Feb
2013 Apr
2013 Jun
2013 Aug
2013 Oct
2013 Dec
2014 Feb
2014 Apr
2014 Jun
2014 Aug
2014 Oct
2014 Dec
2015 Feb
2015 Apr
2015 Jun
2015 Aug
2015 Oct
2015 Dec
2016 Feb
2016 Apr
2016 Jun
Chrome
IE
Firefox
Safari
Android
Opera
UC Browser
Others

Artifacts

- **History**
- **Cache**
- **Cookies**

Commercial Tools

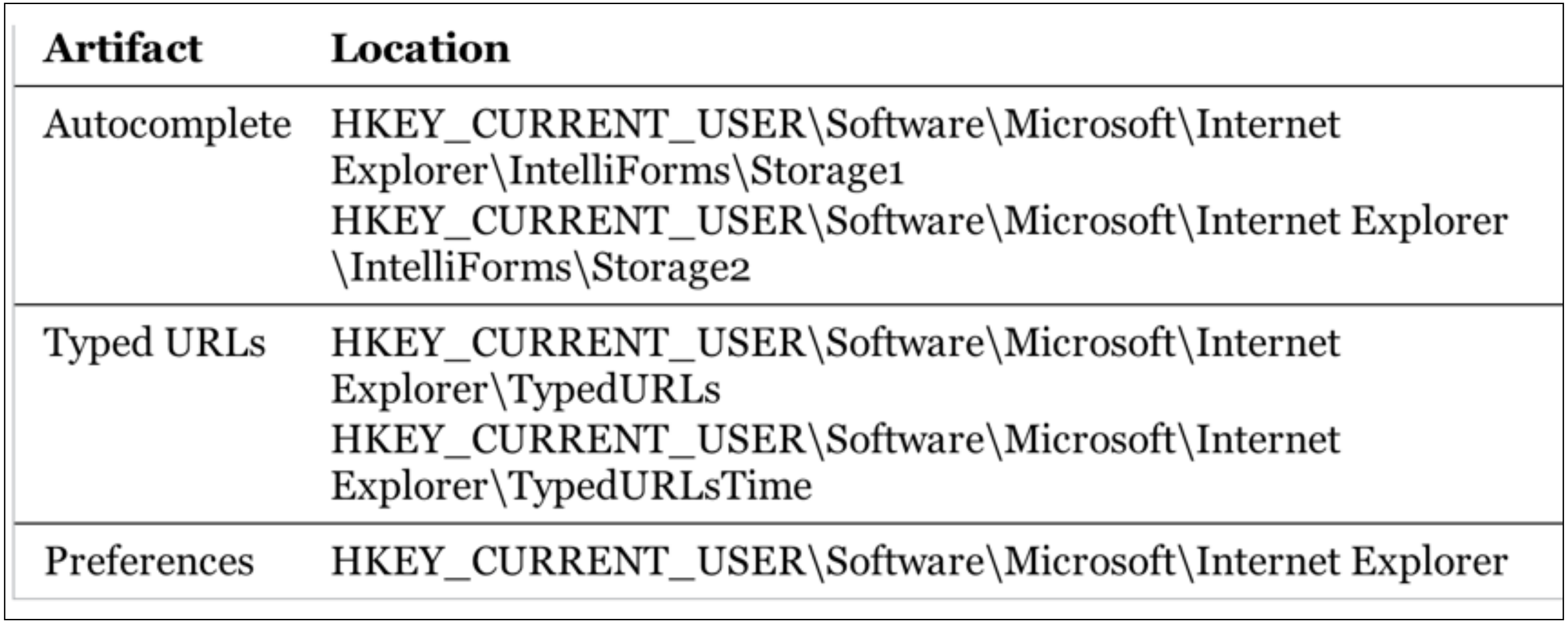
- **Digital Detective NetAnalysis**
- **Magnet Forensics Internet Evidence Finder**

Free Tools

- **These tools work for multiple browsers**
  - **NirSoft's BrowsingHistoryViewer**
  - **Mandiant's RedLine**

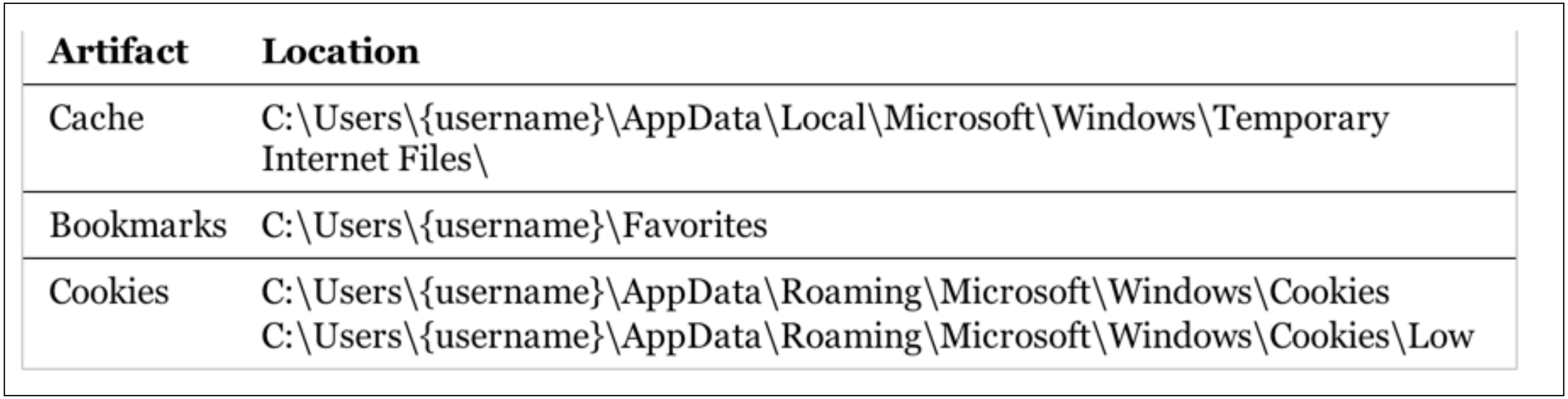
Internet Explorer

- **The standard at corporations**
- **Autocomplete, Typed URLs and preference settings all saved in the Registry**



Artifact	Location
Autocomplete	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage1 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2
Typed URLs	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLsTime
Preferences	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer

Cache, Bookmarks, Cookies

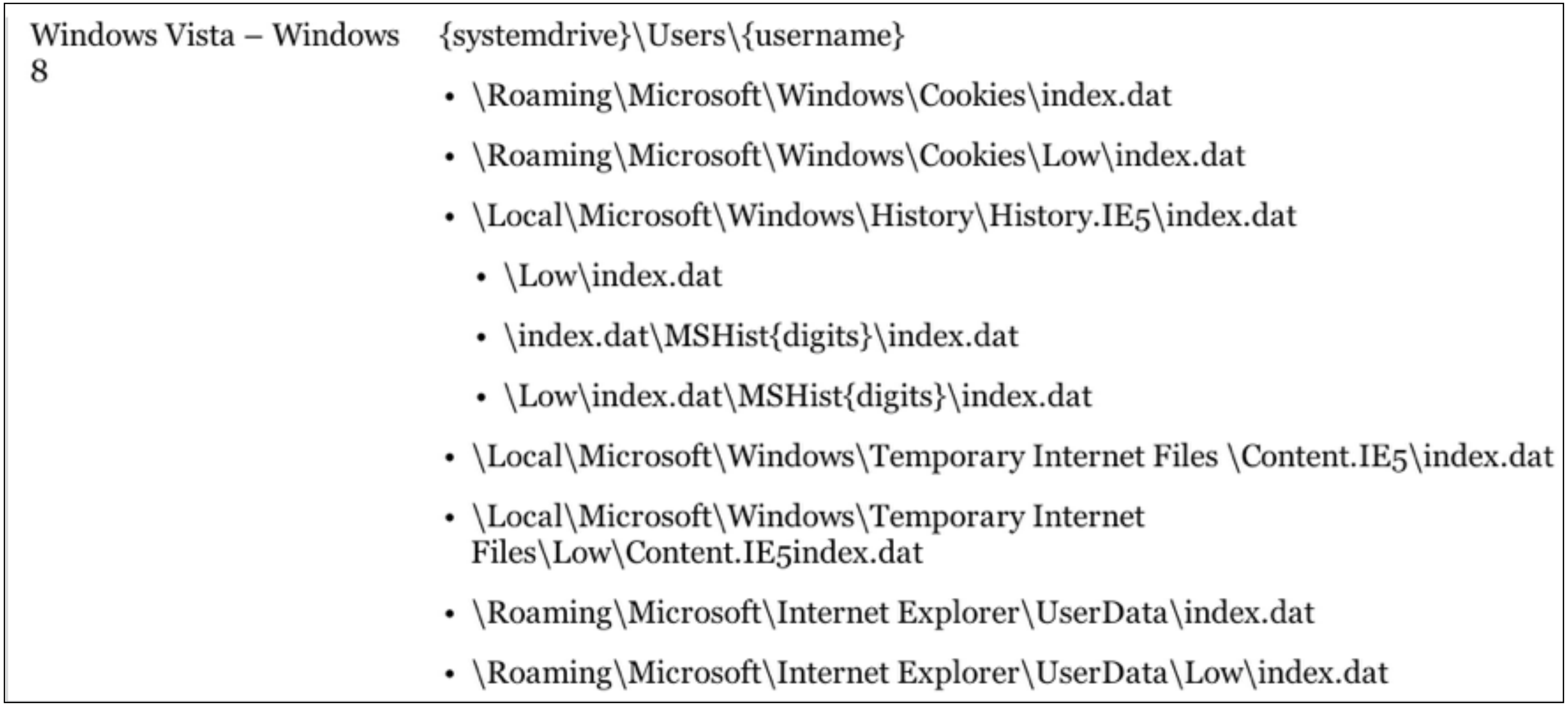


Artifact	Location
Cache	C:\Users\{username}\AppData\Local\Microsoft\Windows\Temporary Internet Files\
Bookmarks	C:\Users\{username}\Favorites
Cookies	C:\Users\{username}\AppData\Roaming\Microsoft\Windows\Cookies C:\Users\{username}\AppData\Roaming\Microsoft\Windows\Cookies\Low

IE History

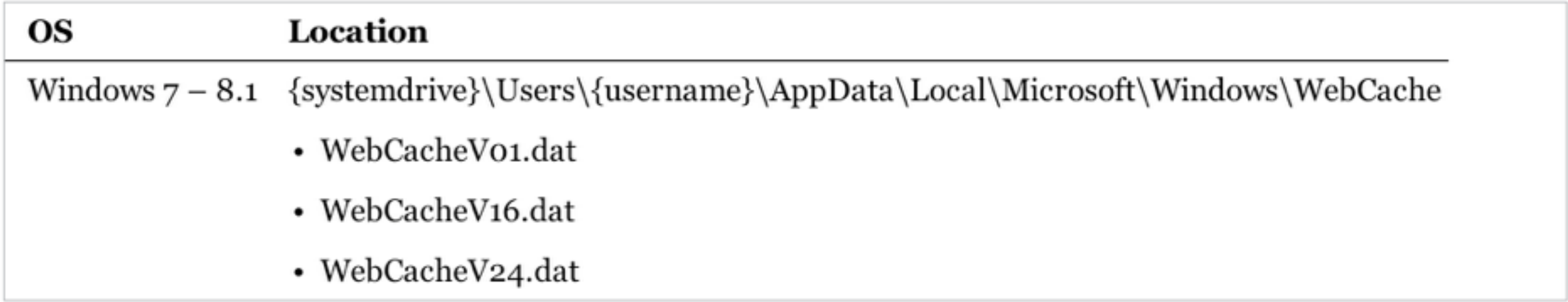
- **Older versions used index.dat files**
- **IE 10 uses Extensible Storage Engine (ESE) database format**
  - **Link Ch 14b, 14c**

Index.dat Locations



Windows Vista – Windows 8	{systemdrive}\Users\{username} • \Roaming\Microsoft\Windows\Cookies\index.dat • \Roaming\Microsoft\Windows\Cookies\Low\index.dat • \Local\Microsoft\Windows\History\History.IE5\index.dat • \Low\index.dat • \index.dat\MSHist{digits}\index.dat • \Low\index.dat\MSHist{digits}\index.dat • \Local\Microsoft\Windows\Temporary Internet Files \Content.IE5\index.dat • \Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5index.dat • \Roaming\Microsoft\Internet Explorer\UserData\index.dat • \Roaming\Microsoft\Internet Explorer\UserData\Low\index.dat

ESE Locations



OS	Location
Windows 7 – 8.1	{systemdrive}\Users\{username}\AppData\Local\Microsoft\Windows\WebCache • WebCacheV01.dat • WebCacheV16.dat • WebCacheV24.dat

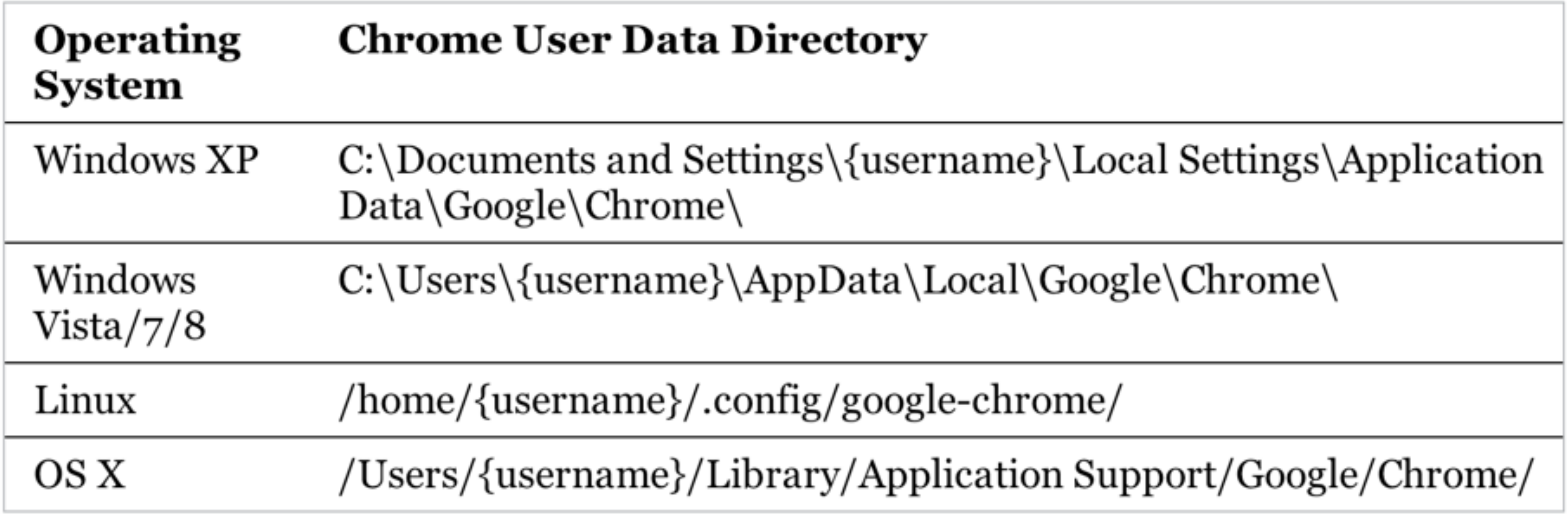
Tools

- **Nirsoft IE Cache Viewer (Link Ch 14d)**
- **Also history, cookie, and autocomplete viewers**
    - **Link Ch 14e**

Google Chrome

Chrome's Data

- **Chrome stores data in SQLite databases and JavaScript Object Notation (JSON) files**
- **Most with no file extension**



Operating System	**Chrome User Data Directory**
Windows XP	C:\Documents and Settings\{username}\Local Settings\Application Data\Google\Chrome\
Windows Vista/7/8	C:\Users\{username}\AppData\Local\Google\Chrome\
Linux	/home/{username}/.config/google-chrome/
OS X	/Users/{username}/Library/Application Support/Google/Chrome/

History

- **Stored in "urls" and "visits" tables in the file "History"**
- **This query shows a user's browsing history**
  - **SELECT datetime(((visits.visit_time/1000000)-11644473600), "unixepoch"), urls.url, urls.title FROM urls, visits WHERE urls.id = visits.url;**
  - **Link Ch 14f**

Archived History

- **Stripped-down version of History**
- **Tracks activity older than three months**

History Index

- **Chrome uses the address bar as a search field**
- **"History Index" is used to rapidly suggest sites the user has viewed before**
- **Investigators find text content the user was searching for, in addition to URLs**

Cache

- **Located at User Data\Default\Cache**
- **Contains source code of websites, images, other supporting files**

Cookies

- **Chrome uses a database to save cookies**
- **Contains domain, creation timestamp, last accessed timestamp, and more**

Downloads

- **In "downloads" and "downloads_url_chains" tables**

- **Retains URL, total size, how many bytes were actually downloaded, and time download started**

- **In newer Chrome versions, also retains**

    - **When the download finishes, and whether Chrome thought the file was malicious**

Autofill

- **Enabled by default**
- **Records**
  - **What the user enters into each text field**
  - **The field name**
  - **Timestamp**

Bookmarks

- **Bookmarks and Bookmarks.bak**
  - **In JSON format, containing**
    - **Date bookmark added**
    - **URL**
    - **Bookmark title**
    - **Folder structure of bookmarks**

Preferences

- **Stored as a JSON object in User Data\Default \Preferences**
- **List of installed plugins and extensions**
- **If Google Sync is on, details of what items are synced, when the last sync was, and the associated Google account**

Preferences

- **Items that reveal locations of interest in the file system**
  - **savefile.default_directory, selectfile.last_directory, and download.default_directory**
- **profile.per_host_zoom_levels**
  - **Remembers zoom setting for websites**
  - **Persists when browser history is cleared**

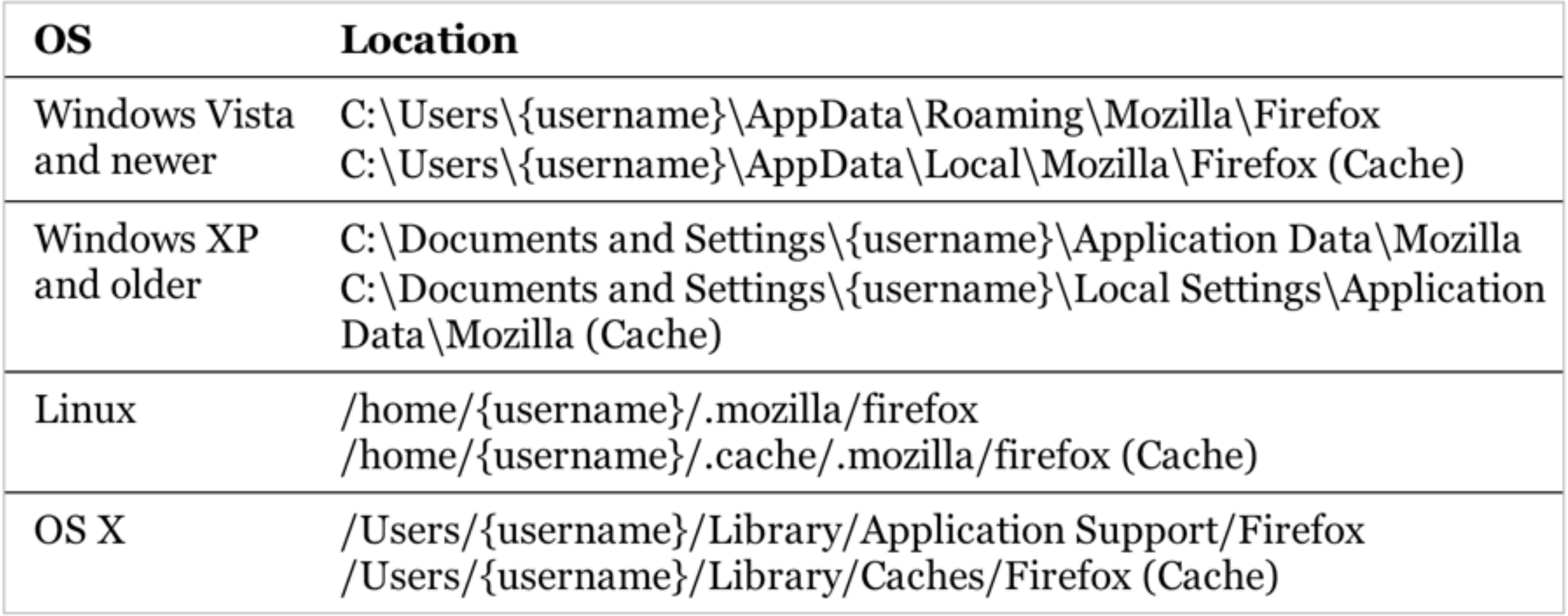
Tools

- **Chrome changes very quickly and autoupdates**
- **So few specialized tools can be maintained**
- **Generic viewers for SQLite and JSON work**
- **Nirsoft has some CHrome-specific tools**

Firefox

Data Formats and Locations

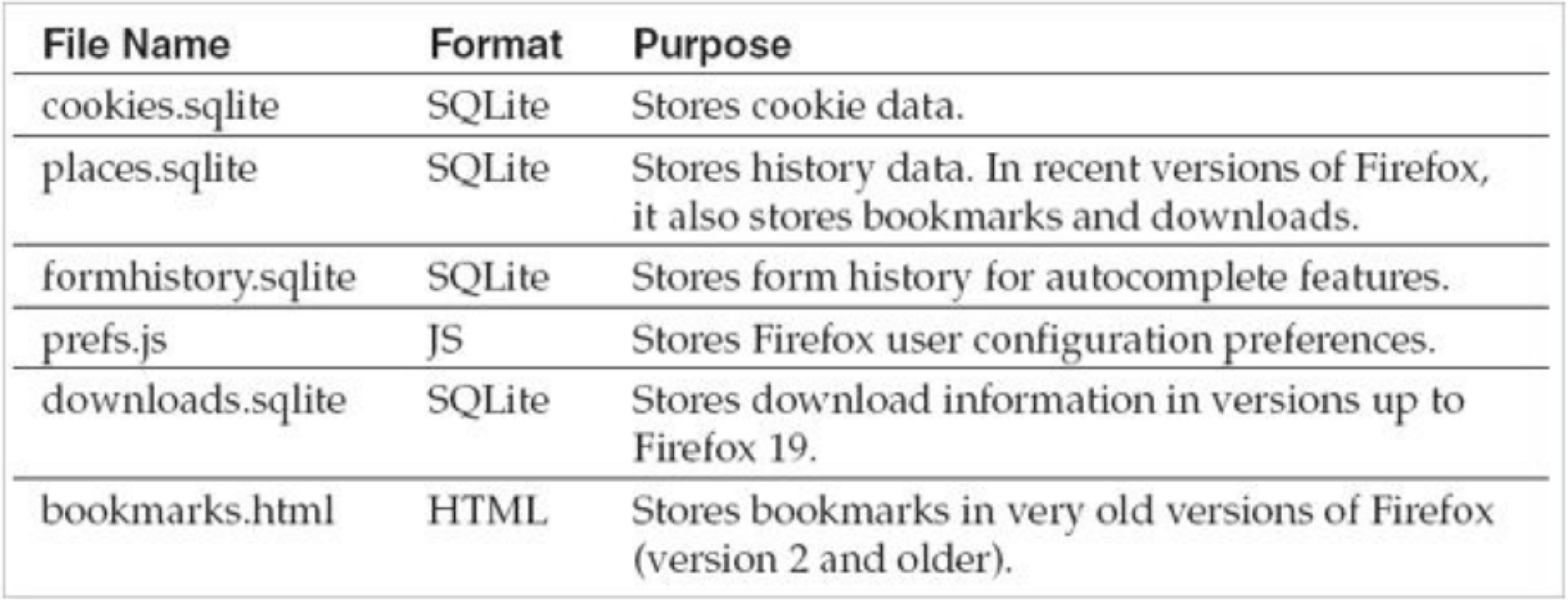
- **SQLite and JSON formats**



OS	Location
Windows Vista and newer	C:\Users\{username}\AppData\Roaming\Mozilla\Firefox C:\Users\{username}\AppData\Local\Mozilla\Firefox (Cache)
Windows XP and older	C:\Documents and Settings\{username}\Application Data\Mozilla C:\Documents and Settings\{username}\Local Settings\Application Data\Mozilla (Cache)
Linux	/home/{username}/.mozilla/firefox /home/{username}/.cache/.mozilla/firefox (Cache)
OS X	/Users/{username}/Library/Application Support/Firefox /Users/{username}/Library/Caches/Firefox (Cache)

Profile Data

- **In Profiles/*random*.default**



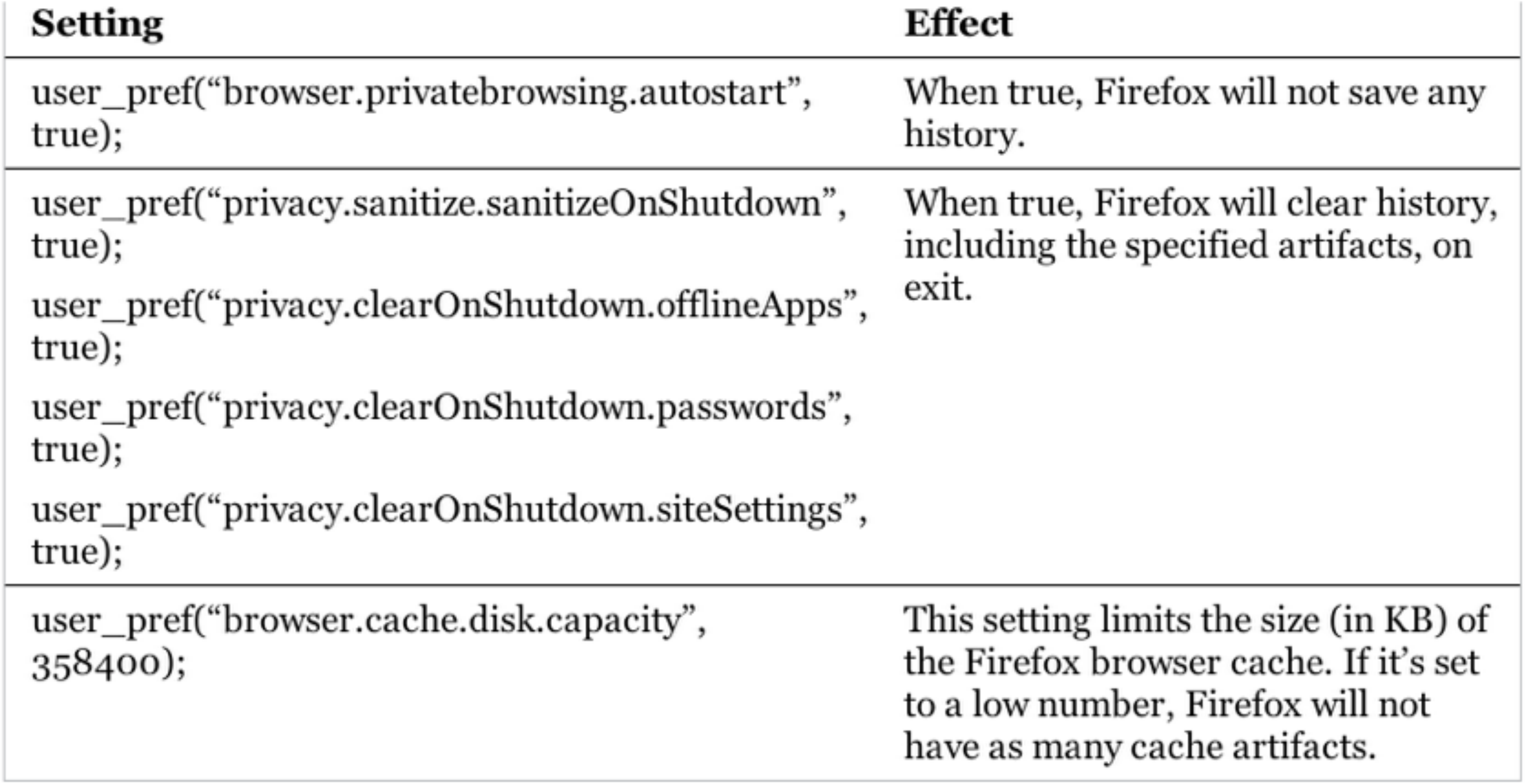
File Name	Format	Purpose
cookies.sqlite	SQLite	Stores cookie data.
places.sqlite	SQLite	Stores history data. In recent versions of Firefox, it also stores bookmarks and downloads.
formhistory.sqlite	SQLite	Stores form history for autocomplete features.
prefs.js	JS	Stores Firefox user configuration preferences.
downloads.sqlite	SQLite	Stores download information in versions up to Firefox 19.
bookmarks.html	HTML	Stores bookmarks in very old versions of Firefox (version 2 and older).

Artifacts

- **History**
- **Downloads**
- **Bookmarks**
- **Autofill**
- **Cookies**
- **Cache**

Preferences

- **These affect the creation of artifacts**



Setting	Effect
user_pref("browser.privatebrowsing.autostart", true);	When true, Firefox will not save any history.

user_pref("privacy.sanitize.sanitizeOnShutdown", true);
user_pref("privacy.clearOnShutdown.offlineApps", true);
user_pref("privacy.clearOnShutdown.passwords", true);
user_pref("privacy.clearOnShutdown.siteSettings", true);
	When true, Firefox will clear history, including the specified artifacts, on exit.

user_pref("browser.cache.disk.capacity", 358400);	This setting limits the size (in KB) of the Firefox browser cache. If it's set to a low number, Firefox will not have as many cache artifacts.

Tools

- **SQLite viewer works**
- **Good tools from Nirsoft**

Email Clients

Importance of Email

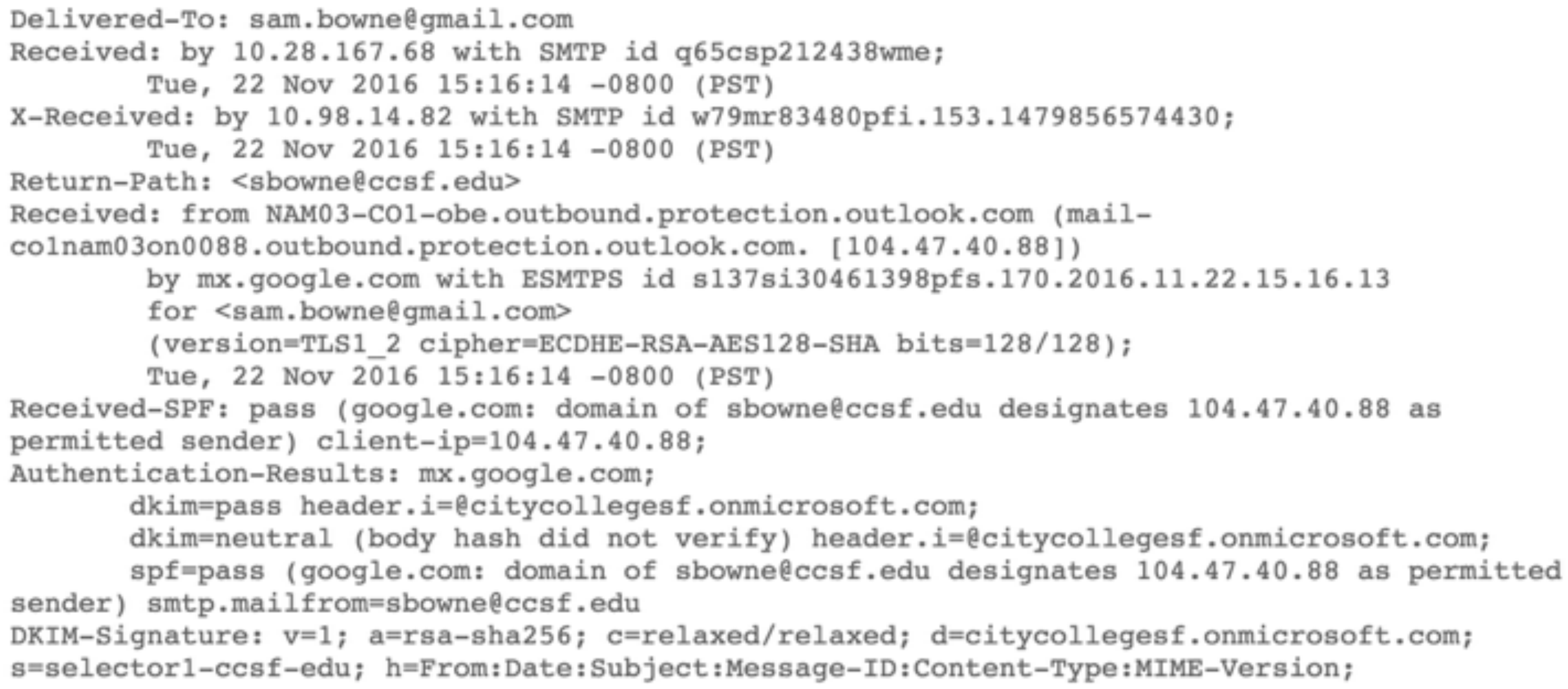
- **Phishing**
  - **Common initial attack vector**
- **Use by criminals**
  - **To coordinate activity or steal data**
- **As a target**
  - **Attackers stealing emails**

Email Structure

- **Headers**
  - **To, From, Cc, Bcc, Date, Subject**
  - **"Metadata"**
- **Body (the text itself) and attachments**
  - **Often in Multipurpose Internet Mail extensions (MIME) format**

Email Headers

- **Very complex, difficult to interpret**
  - **Link Ch 14i**



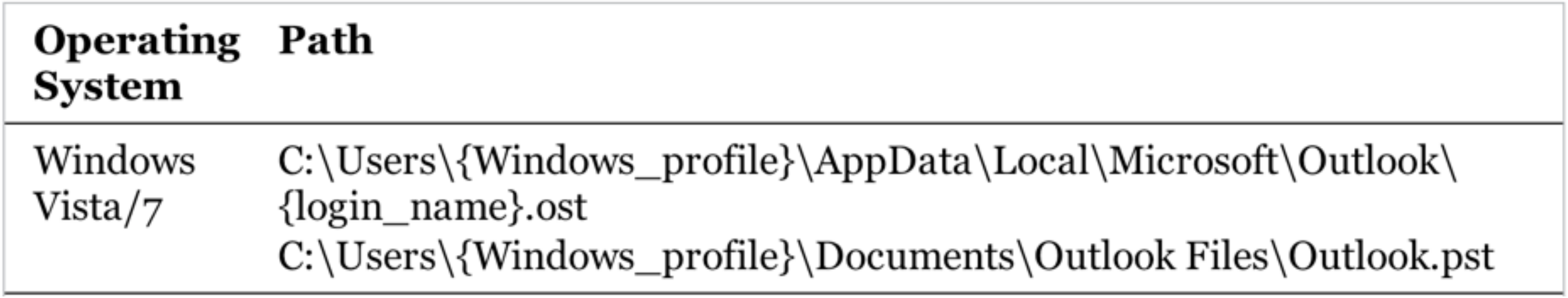
```
Delivered-To: sam.bowne@gmail.com
Received: by 10.28.167.68 with SMTP id q65csp212438wme;
        Tue, 22 Nov 2016 15:16:14 -0800 (PST)
X-Received: by 10.98.14.82 with SMTP id w79mr83480pfi.153.1479856574430;
        Tue, 22 Nov 2016 15:16:14 -0800 (PST)
Return-Path: <sbowne@ccsf.edu>
Received: from NAM03-CO1-obe.outbound.protection.outlook.com (mail-
co1nam03on0088.outbound.protection.outlook.com. [104.47.40.88])
        by mx.google.com with ESMTPS id s137si30461398pfs.170.2016.11.22.15.16.13
        for <sam.bowne@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
        Tue, 22 Nov 2016 15:16:14 -0800 (PST)
Received-SPF: pass (google.com: domain of sbowne@ccsf.edu designates 104.47.40.88 as
permitted sender) client-ip=104.47.40.88;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@citycollegesf.onmicrosoft.com;
       dkim=neutral (body hash did not verify) header.i=@citycollegesf.onmicrosoft.com;
       spf=pass (google.com: domain of sbowne@ccsf.edu designates 104.47.40.88 as permitted
sender) smtp.mailfrom=sbowne@ccsf.edu
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=citycollegesf.onmicrosoft.com;
s=selector1-ccsf-edu; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version;
```

Web Email

- **Most email doesn't use a client, but a cloud solution like Gmail or Yahoo! mail**
  - **However, many corporations still use "thick" clients like Microsoft Outlook**
- **Web-based email doesn't store content on the local system**
  - **Few browser artifacts**
  - **Best tools are commercial, such as Magnet Forensics Internet Evidence Finder**

Microsoft Outlook for Windows

- **Outlook uses Personal Folder File (PFF) format**
- **In a Microsoft Exchange environment, outlook stores a copy of email offline in an "Offline Storage Table" file, a form of PFF**
- **IN non-Exchange snvironments, it uses Personal Storage Table (PST) format, another form of PFF**



Operating System	Path
Windows Vista/7	C:\Users\{Windows_profile}\AppData\Local\Microsoft\Outlook\{login_name}.ost C:\Users\{Windows_profile}\Documents\Outlook Files\Outlook.pst

Tools

- **Commercial forensic tools**
  - **EnCase & FTK**
- **Open source tools**
  - **libpff, a tool you must compile and run in Cygwin**

Apple Mail

- **All user data in /Users/*username*/Library/Mail**
- **In plaintext "emlx" format**
- **Examine with grep and strings**
- **Encase shows emails in a familiar tree-structured displey**

Microsoft Outlook for Mac

- **Stores user data in /Users/*username*/Documents/ Microsoft User Data/Office 2011 Identities**
- **Proprietary database named "Database", and folders with each email in a separate file as plaintext ASCII or Unicode**
- **grep and strings are difficult to use because of the Unicode**
- **Tools like Aid4Mail or Emailchemy are better**

Instant Message Clients

Instant Messages

- **Communication can be two-way or involve multiple parties in a group conversation**

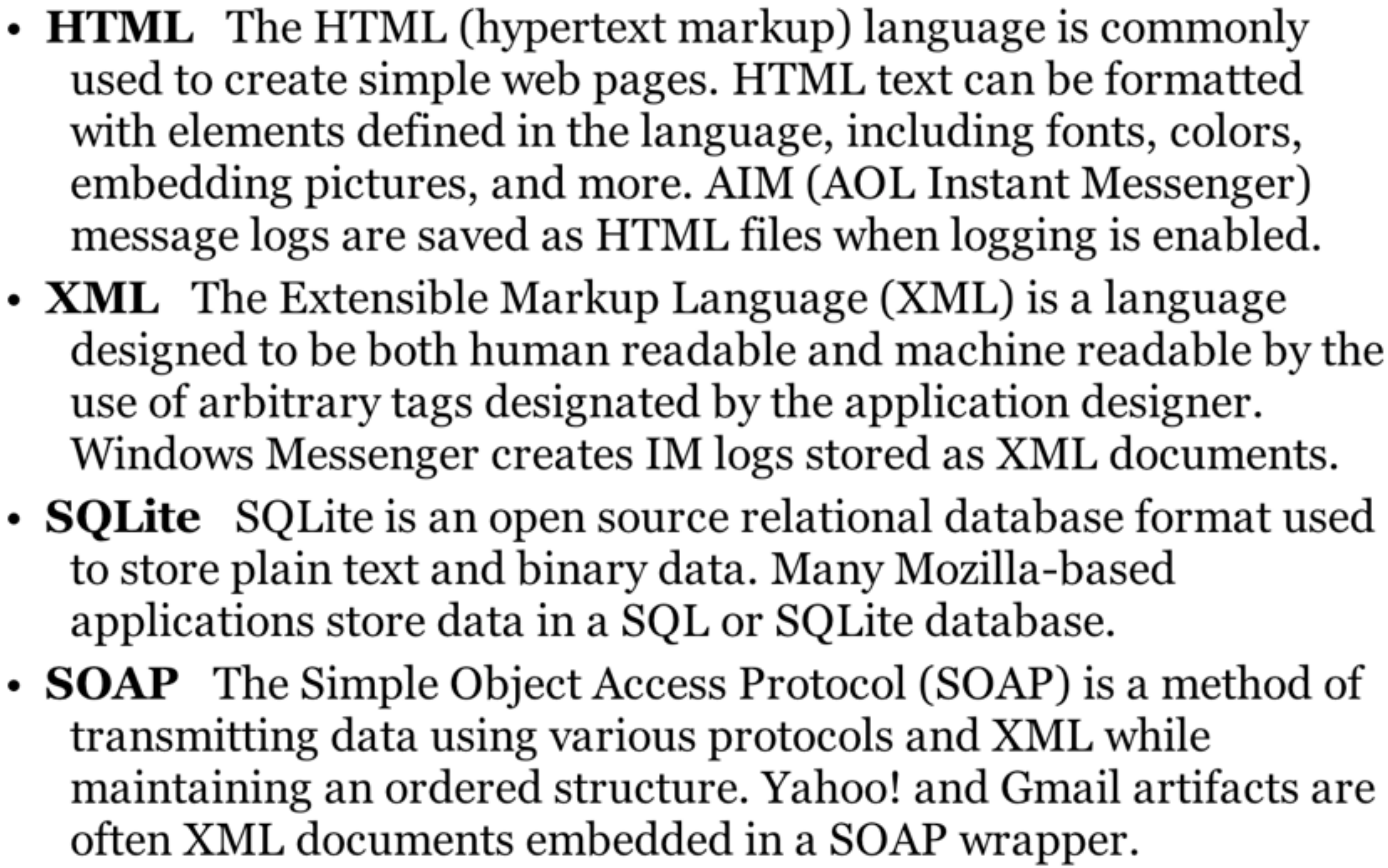
- **Includes file transfers, voice chat, videoconferencing, voice-to-telephone chats, recording, and saving voicemail**

- **Chat participants can see status of partners: online, offline, away, and more**

Methodology

- **IM client update frequently**
- **Properly test each client, following a documented methodology**
- **Tests environment: best is a clean VM with the OS used by the subject of investigation**

Commin IM Technologies



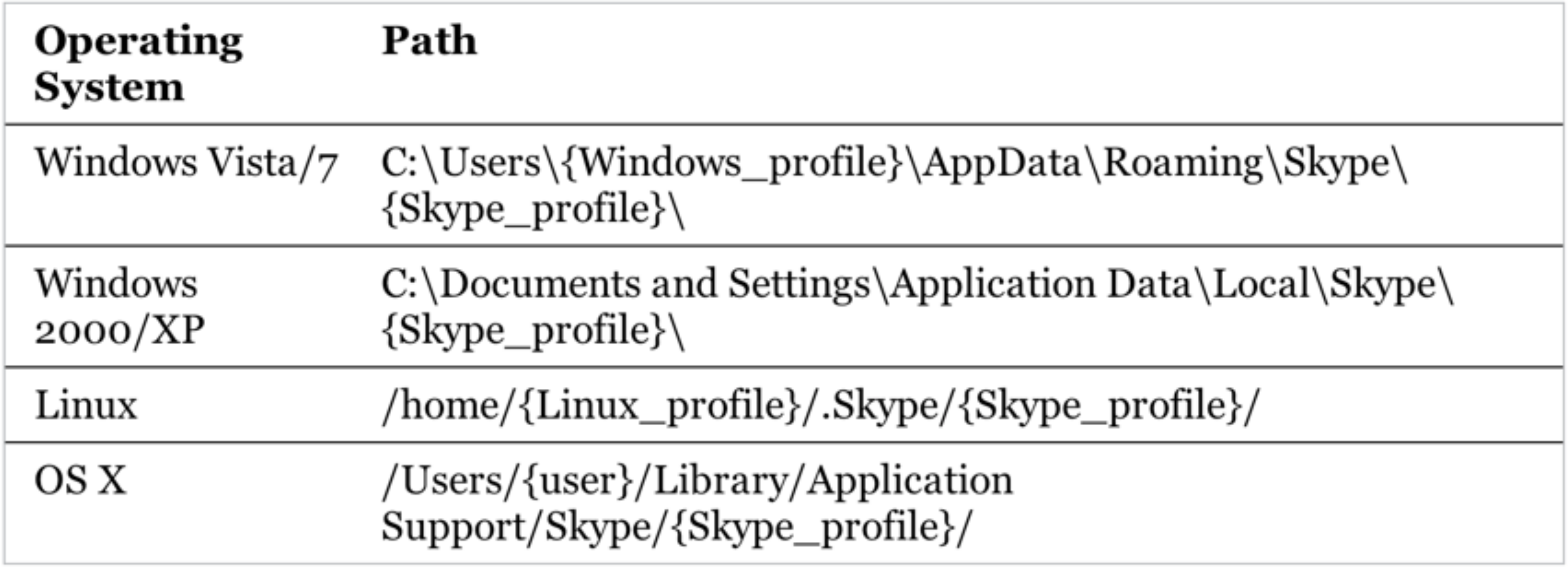
- **HTML** The HTML (hypertext markup) language is commonly used to create simple web pages. HTML text can be formatted with elements defined in the language, including fonts, colors, embedding pictures, and more. AIM (AOL Instant Messenger) message logs are saved as HTML files when logging is enabled.
- **XML** The Extensible Markup Language (XML) is a language designed to be both human readable and machine readable by the use of arbitrary tags designated by the application designer. Windows Messenger creates IM logs stored as XML documents.
- **SQLite** SQLite is an open source relational database format used to store plain text and binary data. Many Mozilla-based applications store data in a SQL or SQLite database.
- **SOAP** The Simple Object Access Protocol (SOAP) is a method of transmitting data using various protocols and XML while maintaining an ordered structure. Yahoo! and Gmail artifacts are often XML documents embedded in a SOAP wrapper.

IM Clients

- **Skype**
- **Facebook Chat**
- **AOL Instant Messenger (AIM)**

Skype

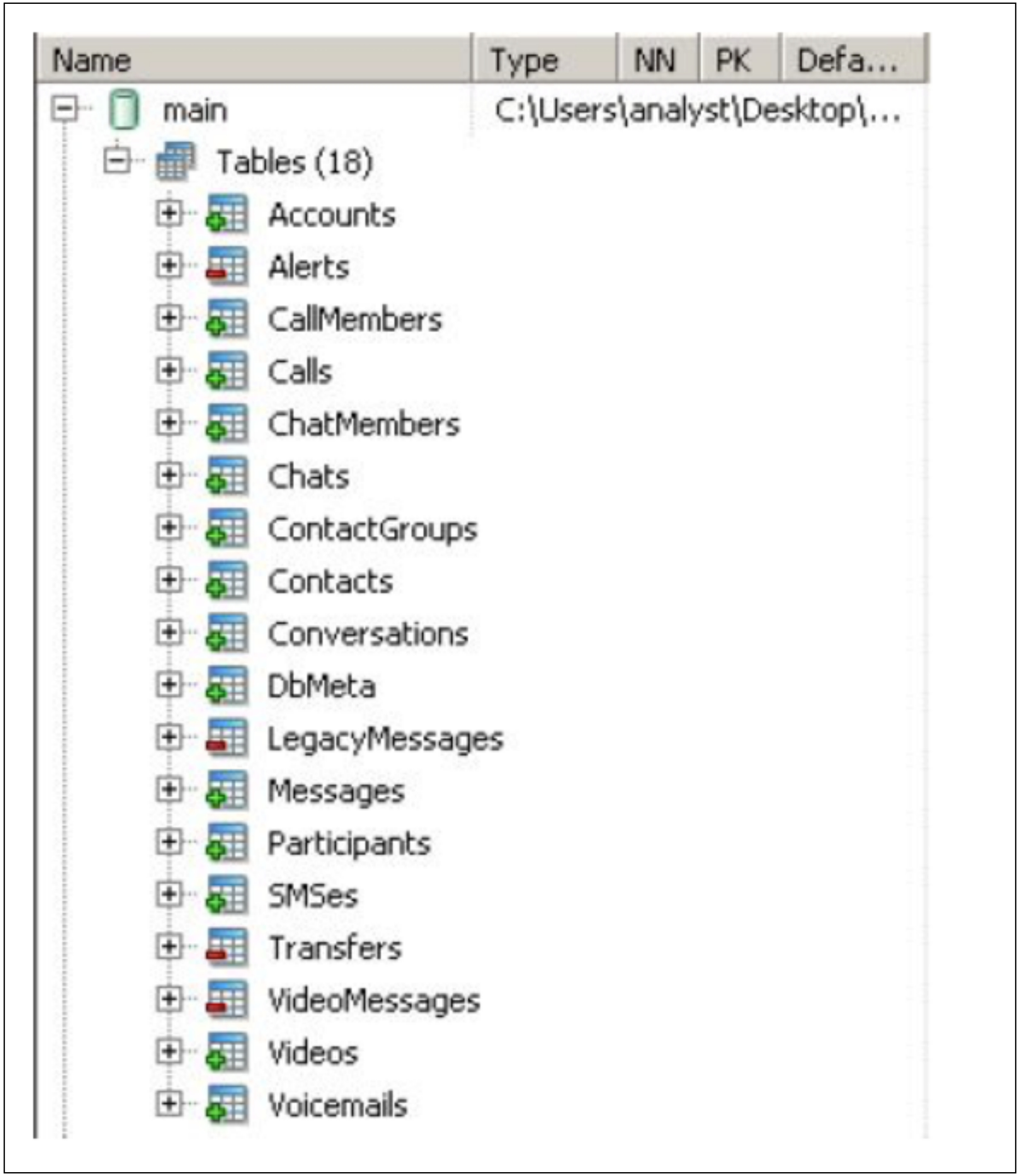
- **Now owned by Microsoft**
- **Logs retained "forever" by default**
- **SQLite3 format**



Operating System	Path
Windows Vista/7	C:\Users\{Windows_profile}\AppData\Roaming\Skype\{Skype_profile}\
Windows 2000/XP	C:\Documents and Settings\Application Data\Local\Skype\{Skype_profile}\
Linux	/home/{Linux_profile}/.Skype/{Skype_profile}/
OS X	/Users/{user}/Library/Application Support/Skype/{Skype_profile}/

Artifacts

- **Voicemails stored as audio files using a proprietary codec**
- **You can import them into another copy of Skype and play them there**



```
Name                          Type                         NN   PK   Defa...
⊟ main                        C:\Users\analyst\Desktop\...
   ⊟ Tables (18)
      ⊞ Accounts
      ⊞ Alerts
      ⊞ CallMembers
      ⊞ Calls
      ⊞ ChatMembers
      ⊞ Chats
      ⊞ ContactGroups
      ⊞ Contacts
      ⊞ Conversations
      ⊞ DbMeta
      ⊞ LegacyMessages
      ⊞ Messages
      ⊞ Participants
      ⊞ SMSes
      ⊞ Transfers
      ⊞ VideoMessages
      ⊞ Videos
      ⊞ Voicemails
```

Preferences

- **Stored in config.xml in each user's profile directory**
- **Contains contact names, chat history (if retained), dialed numbers, and avatar paths (images)**

Tools

- **SQLite browser**
- **Many Skype-specific tools**

Facebook Chat

- **All data stored on Facebook servers through the web-based client**
- **No locally installed software**
- **Logs are stored on Facebook's servers**
- **You need a search warrant or other legal process to get them**

Local Evidence

- **Some artifacts might be present in**
  - **RAM, page files, hibernation files**
  - **Unallocated space**
  - **Internet browser cache files**
- **All stored through indirect processes, not by design**
- **May be incomplete or inaccurate**

Tools

- **Internet Evidence Finder can analyze a memory image, carving it for Facebook items in JSON format**

AOL Instant Messenger (AIM)

- **Logs are not stored locally by default**
- **Must get them from AOL by a legal process**
- **User may configure "Save chats"**
  - **They they are stored in HTML format**

Tools

- **Any text viewer or Web browser can view the logs**
- **SQLite for preferences database**