# Best Practices in Browser Forensics

## Internet Browser Forensics Provide Crucial Artifacts

Both valid users and attackers use the Internet. Once they’ve compromised a machine, attacker’s activities consist of conducting online fraud, communicating with the needed command and control (C2) systems, downloading malware for pivoting throughout the network and exfiltrating sensitive data. Internet browser artifacts provide crucial evidence while investigating online activity in both civil and criminal matters.

While there are numerous examples that demonstrate the value of Internet browser artifacts in civil cases that do not make the news, there have been some criminal matters that have. For example, the online searches in the [**Casey Anthony case**](http://www.nytimes.com/2011/07/19/us/19casey.html?_r=1&) were arguably the best evidence available to the prosecution. What is not noted in the news is the value Internet browser forensics provides in determining the details of the advanced attacks conducted against our networks.

## The Challenges of Internet Browser Forensics

Leveraging Internet browser artifacts can be complex, but the value of the information available makes it worth the effort. The basics of Internet browser forensics revolve around artifacts such as Web sites visited, timestamps and counts of access, search histories, download activity, communications and the potential to rebuild Web pages viewed from cached files. However, locating and leveraging this information can be challenging without the needed prerequisite knowledge. The main challenges include:

* **Multiple browsers:** Investigators will likely encounter [**numerous mainstream browsers**](http://www.netmarketshare.com/). There may even be multiple browsers in use on the same machine.
* **Varied storage schemes:** Once investigators determine which browser(s) are being used, they must realize that each browser may store different types of artifacts, differently and in different locations. This is very important because different browsers often require different tools and approaches.
* **New/updated architectures:** Browser developers may even completely change the architecture between versions, as Mozilla Firefox and Internet Explorer (IE) have done in the past. For example, many tools that supported IE through Version 9 became useless with the release of IE 10 due to the significant changes made.
* **Non-standard browsers:** To further frustrate investigators, attackers may actually install a non-standard browser in an effort to obfuscate their activities.

In summary, to be successful in Internet browser forensics, we must identify the browser(s) being used, understand where the artifacts are stored and employ the correct tools for harvesting this data.

## An Internet Browser Forensics Workflow

With the proper approach, Internet browser forensics may be the difference between meeting your objective and scratching your head in dismay as to what occurred and how. The flow consists of:

* Determining the browser(s) being used
* Locating the needed artifacts
* Analyzing the available information for browsers on the Microsoft Windows operating systems

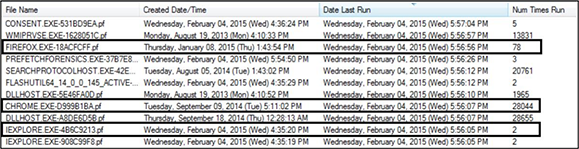
***Please note:*** To preserve the integrity of what could be evidence, it is strongly recommend that investigating this information be performed on a forensic image of the machine rather than the machine itself.

### Determining the Browser(s) Being Used

With Internet browser forensics, it can be easy to succumb to assumptions that may lead down the path of failure. For instance, an organization may have standardized on IE as its Internet browser. Therefore, investigators assume IE will always be the browser of focus. But what if the user has installed an additional browser, or what if an attacker did? Assuming everyone uses IE will cause them to overlook what could be crucial information.

Therefore, investigators must always confirm the browser(s) being used. This is a two-step process that involves more than determining the browser(s) installed; we must also know what is being used.

The first place to determine this information is Windows **[Prefetch](http://windows.microsoft.com/en-us/windows-vista/what-is-the-prefetch-folder" \t "_blank)**. While designed to increase the efficiency of the Windows operating system, the C:\Windows\Prefetch directory provides details of the browser(s) executing on the computer. By using a tool such as Accessdata's [**FTK Imager**](http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.3.0), the contents of Prefetch can be exported and analyzed with a tool such as **[PrefetchForensics](http://www.woanware.co.uk/forensics/prefetchforensics.html" \t "_blank)**from Woanware (see Figure 1).

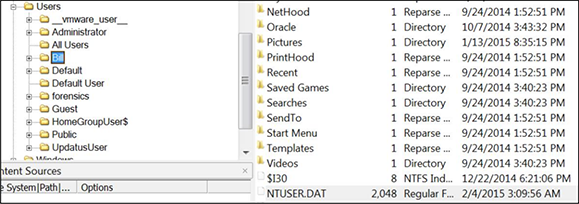


**Figure 1: Prefetch Results**  
Source: IANS, 2015

(***Analysis note:*** Starting with Windows 7, the C:\Windows\Prefetch folder is not populated on machines with SSD drives.)

As Figure 1 demonstrates, three browsers are being used on this machine. However, prefetch provides information related to the last 128 applications executed on the system as a whole. It does not distinguish the applications by the user; this is where analyzing the specific activities of each user will provide value.

User-specific information related to application execution can be found in the ntuser.dat file for each user profile. This file is located at \Users\‘username’\ntuser.dat and should be exported using a tool such as FTK Imager (see Figure 2).



**Figure 2: NTUSER.DAT Location**  
Source: IANS, 2015

Leveraging a tool such as **[UserAssist](http://blog.didierstevens.com/programs/userassist/" \t "_blank)**, the application execution for each user can be determined, with a specific focus on browser usage. Figure 3 demonstrates that the user in question only uses IE and Mozilla Firefox.



**Figure 3: User-Specific Browser Usage**  
Source: IANS, 2015

As Figure 3 demonstrates, no evidence of Google Chrome usage is found for this user. This indicates that another user on the machine uses Google Chrome. The same registry analysis for all users of the computer will determine who uses the Google Chrome browser.

At this point, the investigators must adjust their methods and tools for the specific browsers identified.

Locations of Internet Browser Artifacts

As we discussed earlier, each browser stores its [**artifacts**](http://www.magnetforensics.com/forensic-email-analysis-browser-artifacts-you-may-find/) in different locations. Below is a list of major browsers and the locations they use to store their information for the applicable operating systems.

* **IE (prior to version 10)**
  + **Windows XP:** %root%/Documents and Settings/%userprofile%/Local Settings /Temporary Internet Files/Content.IE5
  + **Windows Vista/7:** %root%/Users/%userprofile%/AppData/Local/Microsoft/Windows /Temporary Internet Files/Content.IE5
* **Internet Explorer 10**
  + **IE 10:** %root%/Users/%userprofile%/AppData/Local/Microsoft/Windows /History
* **Mozilla Firefox**
  + **Windows 7/8:** %root%/Users/%userprofile%/AppData/Local/Mozilla/Firefox/ Profiles/\*.default/Cache
  + **Linux:** /home/%userprofile%/.mozilla/firefox/$PROFILE.default/Cache
  + **Mac OS X:** /Users/%userprofile%/Library/Caches/Firefox/Profiles/ $PROFILE.default/Cache/
* **Google Chrome**
  + **Windows 7/8:** %root%/Users/%userprofile%/AppData/Local/Google/Chrome/User Data/Default/Cache
  + **Linux:** /home/%userprofile%/.config/google-chrome/Default/Application Cache/Cache/
  + **Mac OSX:** /Users/%userprofile%/Caches/Google/Chrome/Default/Cache/
* **Safari**
  + **Mac OSX:** /Users/$USERNAME/Library/Safari/\*
  + **Windows 7/8:** %root%/Users/%userprofile%/AppData/Roaming/Apple Computer/Safari/

### Tools

There are many open source, free and commercial tools to perform Internet browser forensics. While many have a concentration on a specific browser, most commercial applications support all mainstream browsers.

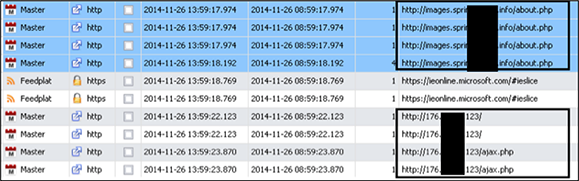
* **Free/open source**
  + [**Pasco**](http://www.mcafee.com/us/downloads/free-tools/pasco.aspx): Free application for IE (pre IE 10)
  + [**Web Historian**](https://www.mandiant.com/resources/download/web-historian): Supports all major browsers (pre IE 10)
  + [**Nirsoft**](http://www.nirsoft.net/web_browser_tools.html): Provides numerous applications for most major browsers
  + [**Nirsoft**](http://www.nirsoft.net/password_recovery_tools.html): Provides applications to extract saved passwords from browsers
  + [**Total Recall**](http://totalrecall.win7dwnld.com/): Free application for IE (pre IE 10)
  + [**Browser Forensic Tool**](http://darkcodersc.blogspot.com/2012/05/browser-forensic-tool-v20-updated.html): Locates and extracts keyword searches
  + [**Browser History Viewer**](http://forensic-software.co.uk/browser-history-viewer/): Free application for IE, Chrome and Firefox
* **Commercial**
  + [**NetAnalysis**](http://www.digital-detective.net/digital-forensic-software/netanalysis/): Supports all major browsers and recovers deleted Internet histories
  + [**Cacheback**](http://www.siquest.com/index.php): Supports all major browsers and reconstructs Web pages
  + [**Magnet Forensics**](http://www.magnetforensics.com/mfsoftware/internet-evidence-finder/): Supports all major browsers and provides additional forensic artifacts

## Internet Browser Forensics in Use

Let’s walk through a couple of case studies where the success of Internet browser forensics made the difference. The first case study involved a cleared defense contractor that fell prey to a spear-phishing email that compromised one of its systems. Armed with the information of the C2 systems used by the attackers, the key question we as investigators wanted to determine was how long the system had been communicating with the C2.

We followed our normal methodology to identify that IE was the only browser being used on the system. After recovering and parsing all artifacts, the Internet activity did not extend beyond Nov. 1, 2014. Our initial assumption was that the attackers must have cleaned up their tracks; this was not the case. We fell prey to a poor assumption.

After scratching our heads for a couple of hours, we discovered that IE was upgraded from Version 9 to 10. Due to the architecture change with this upgrade, the forensics software we were using provided no value. Once we employed the correct software, we were able to determine the extent of the communications with the C2s involved on the date of infection. We were also able to determine that there was only one other day the infected system communicated with the hostile C2s (see Figure 4).



**Figure 4: C2 Communications**  
Source: IANS, 2015

Our second case study involved a server that was being used to commit financial fraud. After determining the attackers’ method for obtaining stolen credentials, we were able to see their fraudulent Internet activities while they were using the “backup” account (see Figure 5).



**Figure 5: Fraudulent Activity**  
Source: IANS, 2015

What made this investigation interesting was evidence indicating that the attackers were using different browsers on this system to commit the fraud and obfuscate their activities. Figure 6 below demonstrates the UserAssist value of the backup account from the ntuser.dat file.

figure6-use-of-firefox-browser

**Figure 6: Usage of Firefox Browser**  
Source: IANS, 2015

Additional analysis also demonstrated that a non-standard browser called SeaMonkey was also being used (see Figure 7).

figure7-use-of-seamonkey-browser

**Figure 7: Usage of SeaMonkey Browser**  
Source: IANS, 2015

Without the determination of each and every browser being used, we would have overlooked crucial artifacts in this investigation.

## Always Employ Browser Forensics in Incident Response

Internet browser forensics has always been a staple in civil and criminal matters to detail the nefarious activities of users on computers and mobile devices. However, Internet browser forensics can also play a critical role in responding to computer security incidents. Overlooking this information may cause you to miss the answers you seek.

To gain the most benefit in incident response investigations, organizations should:

* **Always determine the browser(s) being used:** Failing to identify each browser being used on the machine may cause you to overlook crucial information. Do not rely on assumptions.
* **Research the browsers being used and the artifacts available:** The mainstream browsers typically store similar artifacts. However, each browser type stores the information differently and in different locations. This information is needed for your success.
* **Use the appropriate tools:** As with most forensic applications, the commercial products meet many of your needs. However, specialized free and open source tools can add additional value.

## Related IANS Insights

The IANS Insight [**Techniques for Detecting Compromised Systems**](http://www.iansresearch.com/ResearchDetail.aspx?id=4975) provides several methods for determining compromised machines that need this additional analysis. Others related insights that may be of interest include:

* [**Getting a Handle on Browser Data Collection**](http://iansresearch.com/ResearchDetail.aspx?id=15382), Jan. 12, 2015
* [**Establishing Security Baselines for Firefox, Safari and Chrome Browsers**](http://iansresearch.com/ResearchDetail.aspx?id=10435), May 30, 2014