Forensic Analysis of Epic Privacy Browser on Windows Operating Systems

Alan Reed, Mark Scanlon, Nhien-An Le-Khac
School of Computer Science,
University College Dublin,
Belfield, Dublin 4, Ireland.

alan.reed@ucdconnect.ie, {mark.scanlon, an.lekhac}@ucd.ie

Abstract: Internet security can be compromised not only through the threat of malware, fraud, system intrusion or damage, but also via the tracking of internet activity. Criminals are using numerous methods to access data in the highly lucrative cybercrime business. Organized crime, as well as individual users, are benefiting from the protection of Virtual Private Networks (VPNs) and private browsers, such as Tor, Epic Privacy, to carry out illegal activity such as money laundering, drug dealing, the trade of child pornography, etc. News articles advising on internet privacy assisted in educating the public and a new era of private browsing arose. Although these measures were designed to protect legitimate browsing privacy, they also provided a means to conceal illegal activity. One such tool released for private browsing was Epic Privacy Browser. It is currently used in approximately 180 countries worldwide. Epic Privacy Browser is promoted as a chromium powered browser, specifically engineered to protect users' privacy. It operates solely in "private browser" mode and, after the close of the browsing session, it automatically deletes all browsing data. The developers of Epic Privacy Browser claim that all traces of user activity will be cleared upon close of the application. However, there is no forensic acquisition and analysis of Epic Privacy Browser in literature. In this paper, we contribute towards the goal of assisting forensic examiners with the location and type of evidence available through live and post-mortem state analysis of the Epic Privacy Browser on Windows 7 and Windows 10. This analysis identifies how the browser functions during use and where data can be recovered once the browser is closed, the necessary tools that will assist in the forensics discovery, and effective presentation of the recovered material.

Keywords: Web Browser Forensics, Epic Privacy Browser, Live Data Forensics, Post-Mortem Browser Forensics

1. Introduction

Internet security has been a major and increasing concern for many years. Internet security can be compromised not only through the threat of Malware, fraud, system intrusion or damage, but also via the tracking of internet activity. In order to combat these threats, encryption of data as a default setting is now commonplace. Firewalls (i.e. software that controls access to and from a network) and Anti-virus programs are essential tools in the fight against computer crime. Criminals are using numerous methods to access data in the highly lucrative Cybercrime business. Organized crime, as well as individual users, are benefiting from the protection of Virtual Private Networks (VPNs) and private browsers, such as Tor, Ice Dragon and Epic Privacy, to carry out illegal activity such as money laundering, drug dealing and the trade of child pornography. Weak security has been identified and exploited in several high-profile breaches in recent years. Most notably, in 2011, Sony PlayStation Network faced a major security breach (Connolly, 2011). Over 77 million PlayStation accounts were hacked, resulting in 12 million unencrypted credit card accounts compromised and the site closure for a month. In 2005, the IRS (Internal Revenue Service, USA) faced a data breach that resulted in a reported $50 million in fraudulent claims. As well, in 2015, Ashley Maddison (Fox-Brewster, 2015), a site for extra marital affairs, had 37 million account holders' details released. Breaches such as these illuminate the need for better online security and Internet privacy.

Following the Snowden breach (Toxen, 2014), there was public outrage at the lack of privacy leading to a rise in the number of browsers offering private browsing. News articles advising on internet privacy assisted in educating the public and a new era of private browsing arose. Although these measures were designed to protect legitimate browsing privacy, they also provided a means to conceal illegal activity. One such tool released for private browsing was Epic Privacy Browser (Rubenking, 2014). Epic Privacy Browser was first released in August 2013 by an India based company called Hidden Reflex. Epic Privacy Browser is based on the open-source web browser, Chromium. The Chromium project has resulted in a number of privacy-enhancing browsers being built upon its source code including Epic Privacy Browser, Comodo, Dooble (Gabet, 2016), Inox, and Project Maelstrom (Farina et al., 2015). Epic Privacy Browser was made available for Windows and OSX operating platforms. It gained over a quarter of a million downloads within a year of its release and is currently used in approximately 180 countries worldwide. Epic Privacy Browser is promoted as a browser specifically engineered to protect users' privacy. It only operates in private browser mode and, upon close of the browsing session, deletes all browsing data. Each tab functions as a separate process to increase security. In addition, it claims to remove address bar and URL (Uniform Resource Location) tracking, installation and error tracking, as well as offering a 'one-click' option to surf via the company's own encrypted proxy. The intention is to hide the user IP address as well as encrypt all browsing. Automatic proxy routing occurs when popular search engines are used to prevent searches being saved by IP addresses.

Information commonly stored on a device when using internet browsers include cache, temporary internet files, cookie information, search history, passwords, and registry changes. This paper aims to establish what, if any, data relating to the use of Epic Privacy Browser is produced during the installation and user interaction with the browser. Forensic tools such as Process monitor and Regshot (Regshot, 2016) will be run, capturing the live RAM data after use while the system is still running, and examining data acquired post-mortem once the system is shut down. Because of the privacy concerns surrounding Windows 10, it will be used as the main platform for analysis. We also compare artefacts found on Windows 10 with those available from Windows 7, both set up using default settings and the latest updates. This paper will also examine the Epic Privacy Browser claim that all traces of user activity will be cleared upon close of the application and will establish if the introduction of Windows 10 has had an adverse effect on this claim. The contribution of this paper consists of:

- The identification and analysis of Epic Privacy Browser artefact evidence left on Windows 10 compared with Windows 7 operating systems;
- The outlining of the amount of data recovered from live analysis compared with post-mortem analysis;
- Examine Epic Privacy Browser artefact evidence unique to Windows 10.
- Identify forensic tools available to provide effective analysis.

Our paper is set out as follows: Section 2 shows background on private browsing and related work on privacy browser forensics. We present our forensic techniques applied for Epic browser in Section 3. We describe case studies of forensic acquisition and analysis of Epic browser artefacts for both Windows 7 and Windows 10 in Section 4 and Section 5 respectively. We discuss on the experimental results in Section 6. Finally, we conclude and discuss on future work in Section 7.

2. Background

2.1 Private Browsing

Although private browsing has legitimate uses, such as activity on multiple user devices and political restrictions, many individuals are using the shield of anonymity to carry out illegal activity on the Internet. Private browsing is designed in some web browsers to disable browsing history and the web cache. This allows user to browse the Web without storing data on their system that could be retrieved by investigators. Privacy mode also disables the storage of data in cookies and browsing history databases. This protection is only available to the local device as it is still possible to identify websites visited by associating the IP (Internet Protocol) address at the website.

Aggarwal et al. (Aggarwal, 2013) examined private browsing features introduced by four popular browsers: Internet Explorer, Mozilla Firefox, Google Chrome and Apple Safari. The authors noted that private browsing modes have two goals: 1) to ensure sites visited while browsing in private leave no trace on the user's computer, and 2) to hide a user's identity from web sites they visit by, for example, making it difficult for web sites to link the user's activities in private mode to the user's activities in public mode. The research also identified the inconsistencies when using private mode with the popular browsers and revealed that, although all major browsers support private browsing, inconsistency in the type of privacy provided by each differs greatly. Firefox and Chrome attempt to protect against both web and local attacks while Safari only prevents local issues. In 2012, Marrington et al. examined the privacy benefits of the Chrome portable web browser (including private browsing mode) and discovered that browsing traces remained on the host machine after the session ended and the portable storage device has been disconnected.

As plug-ins and extensions are introduced to the browser, this can change the configuration, causing the privacy settings to no longer perform as intended, leaving the browser vulnerable to attack. Well known browsers such as Google Chrome, Internet Explorer, Safari and Mozilla Firefox rely on similar methods to ensure speed and popularity of their product. Web Cache is a popular way of storing data that can be easily and quickly accessed, thereby negating the necessity to find data that has already been used. History databases, thumbnails (small stored images), temporary files and cookies (user and site-specific data) all help to speed up the user experience and, in their path, leave a plethora of artefact evidence for examiners to feast on. Many studies have been carried out in this area and free tools, such as ChromeHistoryView, ChromeCacheView, IECacheView, as well as forensic software such as Internet Evidence Finder, are available to automate the examination process. All the above browsers have the option to operate in private mode.

Research by Khanikekar (2010) indicates that the use of Internet Explorer in 'Protected Mode' runs a 'Low Privilege' process, preventing the application writing to areas of the system that require higher privilege. Research literature by Hedberg (2013) states that Firefox browser history and search engine keywords are stored in the physical memory of the computer and can still be accessed after the browsing session by way of pagefile.sys or live memory dump. Of particular interest is Google Chrome's 'incognito' mode, as Epic Privacy Browser is part of the Chromium source code. Similar to Firefox, the history, cookies or download lists are not stored on the drive, but held in the physical memory. This still leaves the possibility of pagefile.sys artefact evidence remaining.

2.2 Epic Private Browser

Epic Browser prides itself on protecting the user's privacy by blocking tracking scripts, creating a new process every time a new tab is opened and removing installation information amongst other reported features. Forensic analysts have relied on the recovery of Internet artefacts to prove the type of Internet activity as well as to establish the identity of the user behind the keyboard. Epic Browser was released in August 2013, by a company called Hidden Reflex based in Bangalore, India and Washington DC. The browser was released in response to increased concerns of internet activity monitoring by both government and private company interests. It was the first browser built on Chromium that was engineered specifically to protect the privacy of the user. Epic lists among its many features, the ability to remove all Google tracking as well as blocking other companies' tracking attempts. It also offers the option of an encrypted proxy for added security. Rubenking (2014), a journalist with PC Magazine, published a review of the Epic Privacy Browser highlighting some of its main features. Although being powered by the world's leading search engines, Epic is able to prevent data being leaked. The author noted that the browser routes queries through Epic's proxy server automatically, blocking third party cookies and trackers. He also noted that some websites "simply didn't work with Epic."

3. Epic Privacy Browser Forensics

This paper will compare the Epic Privacy Browser performance on both the Windows 7 and Windows 10 operating systems. In addition, it will establish if the introduction of new data collection methods introduced in Windows 10 have provided an opportunity for forensic investigators to utilize any potential breaches in Epic's privacy settings. It will establish if tools currently used for the analysis of similar browsers built on the same source code, such as Google Chrome, can also be used to recover data from Epic and if live analysis, by the capture on Random Access Memory data, differs when using Windows 10 compared to Windows 7. A 320GB hard drive was used in an HP desktop computer, containing 4GB of RAM, for the analysis of Epic Privacy Browser on both the Windows 7 and Window 10 operating systems. The hard drive was wiped, using Wipemaster hardware, according to Department of Defence standards. Windows 7 Pro was then installed on the hard drive and all default settings were selected. The computer tower was then connected to the Internet via an Ethernet cable and all available software and security updates were carried out. Standard firewall and defender settings were applied. Once the Windows software was updated, Epic Privacy Browser, was installed. Installation of the browser was monitored using the following software to analyse activity on the system:

- Process Monitor – an advanced monitoring tool that shows real-time file system, registry and process thread activity;
- Regshot – an open-source utility that allows snapshots to be taken before and after software installation in order to record registry changed on the system;

- TCPView – Shows detailed listings of all TCP (Transmission control Protocol) and UDP (User Datagram Protocol) endpoints as well as network connection status;
- Registry viewer – software that allows analysis of the windows registry system;
- FTK Imager – Forensics software that is used to capture RAM dumps and protected files data on a live system.
- WireShark – Network protocol analyser. Identifies all network traffic.
- ChromeHistoryView – freeware that allows an examiner to view History database records
- ChromeCacheView – freeware that allows the examiner to view cache entries.

Following installation of Epic, a series of functions were carried out and recorded for the examination. These included Internet searches, viewing of photos, videos and galleries, as well as document and image downloads. Social networking sites such as Facebook, Twitter, Instagram and Youtube were visited. Any login details were entered and, when offered, the password was stored. Google Gmail was also visited and account sign in and log out completed. The computer was constantly connected to the internet for a period of 3 days with the Epic Privacy Browser displayed. On closure of the browser, but while the computer was still running, the Random Access Memory data was then acquired using FTK Imager, version 3.1.1.8. Protected files such as registry Sam, System, Security, Software and User files such as NTUSER.DAT was also acquired at different stages of the process using FTK Imager. Upon completion, the system was powered down using the Start>Power>Shutdown option. The same 320GB hard drive was then wiped, again to Department of Defence standards, and placed back into the HP tower and the process was repeated but this time using Windows 10 Pro operating system with the same browser and forensics software installed. The same queries that had been performed with Windows 7 were repeated. Random Access Memory data was captured before the Epic Browser was installed and on completion of the search queries, while the browser was still displayed. On completion, the browser was closed and the system shut down by the use of the Start – Power – Shut down method.

3.1 Live Memory Acquisition

A 128GB Thumb drive was formatted (ExFAT) and used as storage for the RAM and protected file dumps. FTK Imager forensics software was installed on the examination computer on initial set up and was the software used to extract both the RAM and protected file data. The resulting data dump was then transferred to the forensics computer and labelled as either Windows 10 or Windows 7 RAM, pre or post examination, and protected file dumps.

3.2 Post-mortem Data Acquisition

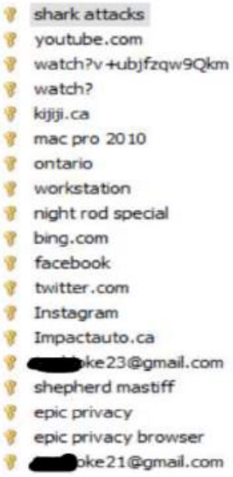
Once each hard drive was removed from the HP Tower, they were acquired individually using FTK Imager forensics software via Tableau write blocking hardware. This method is used in order to ensure an exact forensics image is obtained and verification by way of Cyclic Redundancy Check, an error detecting code that detects changes to raw data, and Hash MD5 algorithm on completion of the process. Tableau Write Blocking hardware is connected directly between the hard drive being acquired and the forensics computer running the acquisition software. Its function is to allow read only commands to be sent to the hard drive therefore preserving the original data. As the original hard drive is the best evidence in a case required for court, an exact forensic copy is produced as a ‘working copy’ for investigators to analyse to minimize the risk of damage or data loss to the original hard drive.

Both Windows 7 and Windows 10 E01’s were loaded into Encase, version 6.19.7, forensics software for analysis. A ‘lost folder’ recovery was then carried out followed by the inclusion of the live memory data. We then carried out a search on the following keywords (Figure 1).

4. Windows 7: Epic Privacy Browser forensic analysis

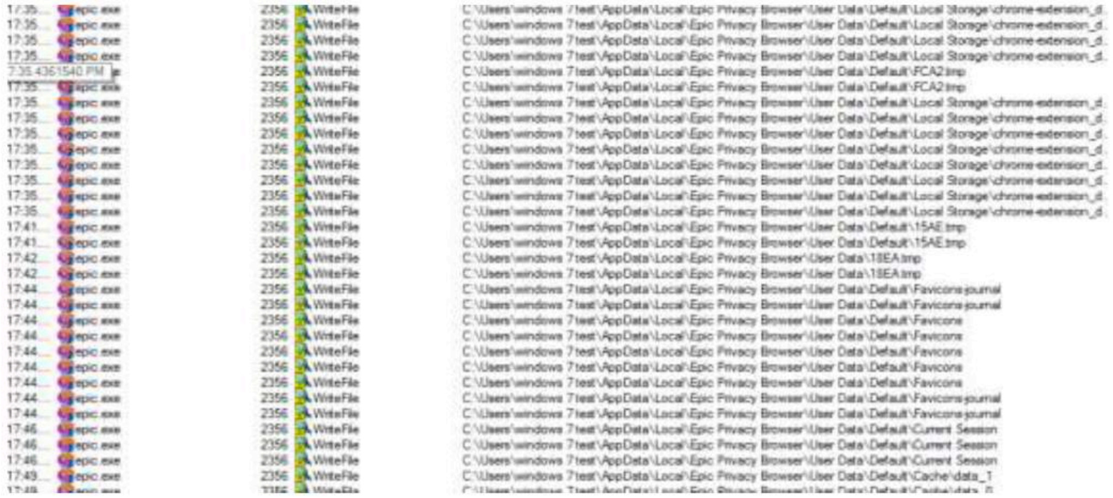
4.1 Post-Mortem Analysis

Initial analysis was carried out on Epic Privacy Browser installed on Windows 7 professional. The installation was monitored using Regshot freeware. A capture was taken pre- and post-install. The software then compares the before and after snapshots and provides a report of the changes recorded in the registry. On executing the browser, several other folders and files are created. The folder structure has a very similar look to that of Google Chrome. Process Monitor software was used to analyse the browser application launch (Figure 2). It shows the browser making use of a Cache folder and additional files that were not initially present on the browser install.



shark attacks
youtube.com
watch?v+ubjfzqw9Qkm
watch?
kijiji.ca
mac pro 2010
ontario
workstation
night rod special
bing.com
facebook
twitter.com
Instagram
Impactauto.ca
[redacted]ke23@gmail.com
shepherd mastiff
epic privacy
epic privacy browser
[redacted]ke21@gmail.com

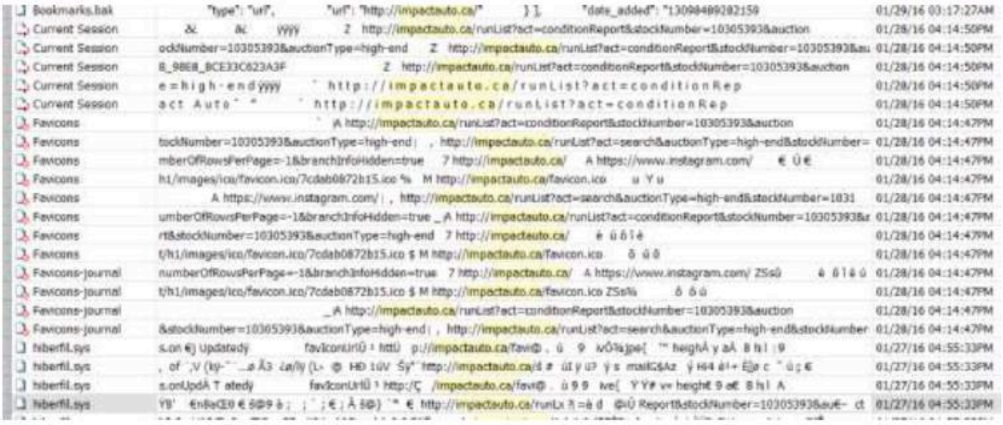
Figure 1: List of Keyword search terms



```
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
7:35.4361540 PM  e          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\FCA2.tmp
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\FCA2.tmp
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
17:35...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Local Storage\chrome-extension_d...
17:41...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\15AE.tmp
17:41...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\15AE.tmp
17:42...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\18EA.tmp
17:42...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\18EA.tmp
17:44...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Favicons-journal
17:44...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Favicons-journal
17:44...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Favicons
17:44...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Favicons
17:44...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Favicons
17:44...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Favicons
17:44...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Favicons
17:44...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Favicons-journal
17:44...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Favicons-journal
17:46...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Current Session
17:46...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Current Session
17:46...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Current Session
17:49...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Cache\data_1
17:49...  epic.exe          2356  WriteFile  C:\Users\windows 7test\AppData\Local\Epic Privacy Browser\User Data\Default\Cache\data_0
```

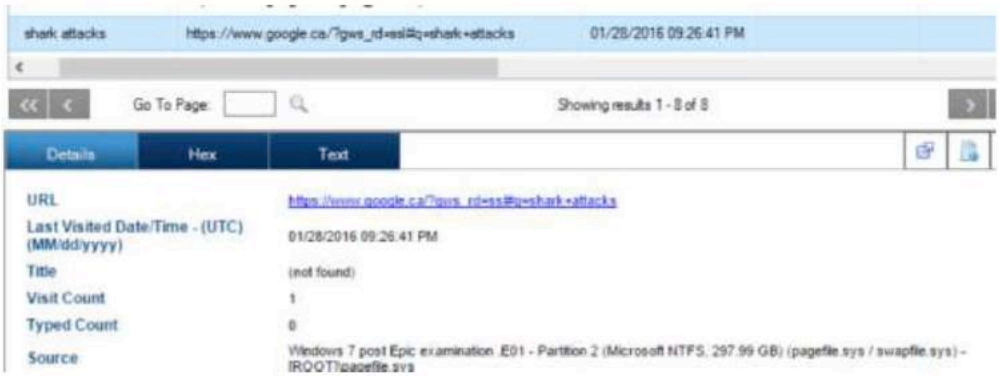
Figure 2: Procmon capture of Epic launch

The additional files and folders are populated with data while the browser is running and deleted when the browser is closed. The history.db file and cache folder appear to function in the same way as Google chrome, allowing data to be viewed using standard Chrome freeware tools. As well as offering a wealth of information through live capture, if the device was found running with the browser displayed, the browser also appears to lack the necessary ability to cover its tracks on closure. Although a large number of files are deleted from view when the browser is closed, a great deal of artefact evidence was either written to pagefile.sys, shown as deleted but recovered using standard forensics tools or recovered from unallocated space. Encase, as well as Internet Evidence Finder, was also able to recover created dates from Epic files shown as deleted (Figure 3). Further analysis was carried out using Internet Evidence finder, version 6.6.3.0740. The software allows for the Windows 7 image file to be loaded and specific category searches selected. IEF identified a large number of hits relating to queries carried out during the experiment. It appeared that data was regularly captured and transferred to the pagefile.sys. Following are just a small sample of those found (Figure 4). Windows 7 drive image (E01) returned 343,000 hits from keyword searches. The same keyword search terms were run on the Windows 10 drive image, resulting in only 52,000 hits.



```
Bookmarks.bak        "type": "url",     "url": "http://impactauto.ca/"      } ],     "date_added": "13098489282158      01/29/16 03:17:27AM
Current Session        &      &     yyyy       Z  http://impactauto.ca/runList?act=conditionReport&stockNumber=10305393&auction      01/28/16 04:14:50PM
Current Session      ockNumber=10305393&auctionType=high-end    Z  http://impactauto.ca/runList?act=conditionReport&stockNumber=10305393&au 01/28/16 04:14:50PM
Current Session      8_98E8_BCE33C623A3F                Z  http://impactauto.ca/runList?act=conditionReport&stockNumber=10305393&auction      01/28/16 04:14:50PM
Current Session      e=high-endyyyy     ' http://impactauto.ca/runList?act=conditionRep      01/28/16 04:14:50PM
Current Session      act Auto' "     ' http://impactauto.ca/runList?act=conditionRep      01/28/16 04:14:50PM
Favicons                         ' A http://impactauto.ca/runList?act=conditionReport&stockNumber=10305393&auction      01/28/16 04:14:47PM
Favicons             tockNumber=10305393&auctionType=high-end ;  , http://impactauto.ca/runList?act=search&auctionType=high-end&stockNumber= 01/28/16 04:14:47PM
Favicons             mberOfRowsPerPage=-1&branchInfoHidden=true   7 http://impactauto.ca/   A https://www.instagram.com/    € Û €      01/28/16 04:14:47PM
Favicons             h1/images/ico/favicon.ico/7cdab0872b15.ico %   M http://impactauto.ca/favicon.ico    u Y u      01/28/16 04:14:47PM
Favicons                   A https://www.instagram.com/ ; , http://impactauto.ca/runList?act=search&auctionType=high-end&stockNumber=1031      01/28/16 04:14:47PM
Favicons             umberOfRowsPerPage=-1&branchInfoHidden=true _A http://impactauto.ca/runList?act=conditionReport&stockNumber=10305393&z 01/28/16 04:14:47PM
Favicons             rt&stockNumber=10305393&auctionType=high-end  7 http://impactauto.ca/     è û ô Ì è      01/28/16 04:14:47PM
Favicons             t/h1/images/ico/favicon.ico/7cdab0872b15.ico $ M http://impactauto.ca/favicon.ico     ô û ô      01/28/16 04:14:47PM
Favicons-journal     numberOfRowsPerPage=-1&branchInfoHidden=true   7 http://impactauto.ca/   A https://www.instagram.com/ ZSsû     è ô Ì è û 01/28/16 04:14:47PM
Favicons-journal     t/h1/images/ico/favicon.ico/7cdab0872b15.ico $ M http://impactauto.ca/favicon.ico ZSs%     ô ô û      01/28/16 04:14:47PM
Favicons-journal                  _A http://impactauto.ca/runList?act=conditionReport&stockNumber=10305393&auction      01/28/16 04:14:47PM
Favicons-journal     &stockNumber=10305393&auctionType=high-end ; , http://impactauto.ca/runList?act=search&auctionType=high-end&stockNumber 01/28/16 04:14:47PM
hiberfil.sys         s.on €) Updatedy        faviconUrlÛ ¹ httÛ  p://impactauto.ca/favi© . û   9  ẃÔ¾jpe(  ™ heighÂ y aÂ  8 h l :9      01/27/16 04:55:33PM
hiberfil.sys         , of ¨,V (ky-¨¨_ø Ã3 ża/ly (L· ©  HÐ 1ûV  Šy" http://impactauto.ca/š #  ûI y û? ý s  mailG$Az  ý H4 é!+ Ëjø c  ¨ û; €      01/27/16 04:55:33PM
hiberfil.sys         s.onUpdÂ T atedy        faviconUrlÛ ¹ http:/Ç  /impactauto.ca/favi© . û 9 9  ẃe(  Ý Y# v« height 9 a€ 8 h l  A      01/27/16 04:55:33PM
hiberfil.sys         Y8'  €n8aŒ8 € 6@9 à ;  ; ¨ ; € ; Å 6@) ¨* € http://impactauto.ca/runLx ?\ =à d  ©iÛ Report&stockNumber=10305393&au€-  ct 01/27/16 04:55:33PM
```

Figure 3: Encase screenshot of recovered Epic artefacts including created dates



shark attacks | https://www.google.ca/?gws_rd=ssl#q=shark+attacks | 01/28/2016 09:26:41 PM

URL: https://www.google.ca/?gws_rd=ssl#q=shark+attacks

Last Visited Date/Time - (UTC) (MM/dd/yyyy): 01/28/2016 09:26:41 PM

Title: (not found)

Visit Count: 1

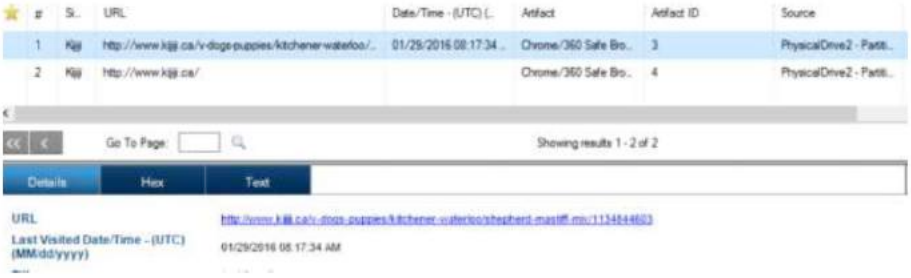
Typed Count: 0

Source: Windows 7 post Epic examination .E01 - Partition 2 (Microsoft NTFS, 297.99 GB) (pagefile.sys / swapfile.sys) - [ROOT]\pagefile.sys

Figure 4: Google search within Epic – 'shark attacks' date and time stamped

4.2 Live Analysis

On the completion of the internet queries, but before the Epic Privacy Browser was closed, the live memory capture was carried out using FTK Imager software. The system files were also captured at this time. The extracted data was then analysed in both Encase and Internet Evidence Finder. The benefit of live data capture was immediately evident although, in this case, post-mortem analysis had also bared significant fruit. It appeared that Epic Browser activity on Windows 7 was being captured in both RAM and written to pagefile.sys. Internet Evidence Finder was an excellent tool for parsing out and presenting the evidence found. Figure 5 shows the 'kijiji dogs' selection made during the browser query process. This was retrieved from both the RAM and post-mortem data dumps with the date and time of the search clearly visible.



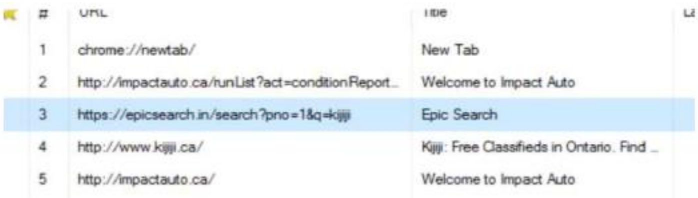
★	#	S..	URL	Date/Time - (UTC) (..	Artifact	Artifact ID	Source
	1	Kijiji	http://www.kijiji.ca/v-dogs-puppies/kitchener-waterloo/..	01/29/2016 08:17:34 ..	Chrome/360 Safe Bro..	3	PhysicalDrive2 - Partit..
	2	Kijiji	http://www.kijiji.ca/		Chrome/360 Safe Bro..	4	PhysicalDrive2 - Partit..

URL: http://www.kijiji.ca/v-dogs-puppies/kitchener-waterloo/shepherd-mastiff-mix/1134844603

Last Visited Date/Time - (UTC) (MM/dd/yyyy): 01/29/2016 08:17:34 AM

Figure 5: Kijiji search for dogs

Figure 6 shows a list of the URLs visited during the query stage. https://epicsearch.in/search?pno=1&q=kijiji showing not only the use of Epic, but that a Kijiji search was carried out by the user. IEF returned over 40 hits of interest from the Windows 7 RAM dump, cementing the requirement for investigators to capture live memory when possible.



#	URL	Title
1	chrome://newtab/	New Tab
2	http://impactauto.ca/runList?act=conditionReport...	Welcome to Impact Auto
3	https://epicsearch.in/search?pno=1&q=kijiji	Epic Search
4	http://www.kijiji.ca/	Kijiji: Free Classifieds in Ontario. Find ...
5	http://impactauto.ca/	Welcome to Impact Auto

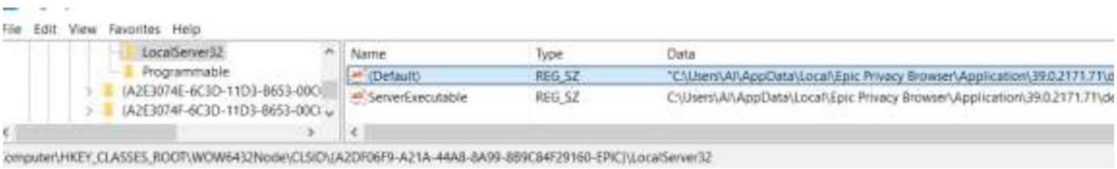
Figure 6: URL's visited

52,000 hits were recorded from the combined Keyword searches entered in Encase, against the live memory dumps of Epic queries on both Windows 7 and Windows 10 operating systems. Of the 52,000 hits, only 12,000 were recorded from the Windows 7 operating system, even though the same experimental process was carried out on each OS.

5. Windows 10: Epic Privacy Browser forensic analysis

5.1 Post-Mortem Analysis

As with Windows 7, Epic Privacy Browser installation on Windows 10 professional was monitored using Regshot and Process Monitor tools. A snapshot was also taken immediately before, and after, the installation process to identify changes to both the file system, and Windows registry. There were a number of registry entries of interest that hadn't been present in the Windows 7 install (Figure 7). Further entries were discovered specific to the users Security Identifier (SID) that would assist the examiner in identifying the user account associated with the application. The SID is a device and account identifier. It is variable in length and encapsulates the hierarchical notion of issuer and identifier. It consists of a 6-byte identifier authority field that is followed by 1-14, 32-bit sub-authority value. It ends in a single 32-bit Relative Identifier (RID). This not only makes it unique to the user but also to the device. The SID is assigned during the installation of the operating system and is unique to each computer. All user accounts are based on the computers SID and contain the relative identifier for each user account. Although this is randomly generated, it is theoretically impossible for the same SID to appear on 2 devices and is therefore extremely useful to a forensic examiner (Figure 8).

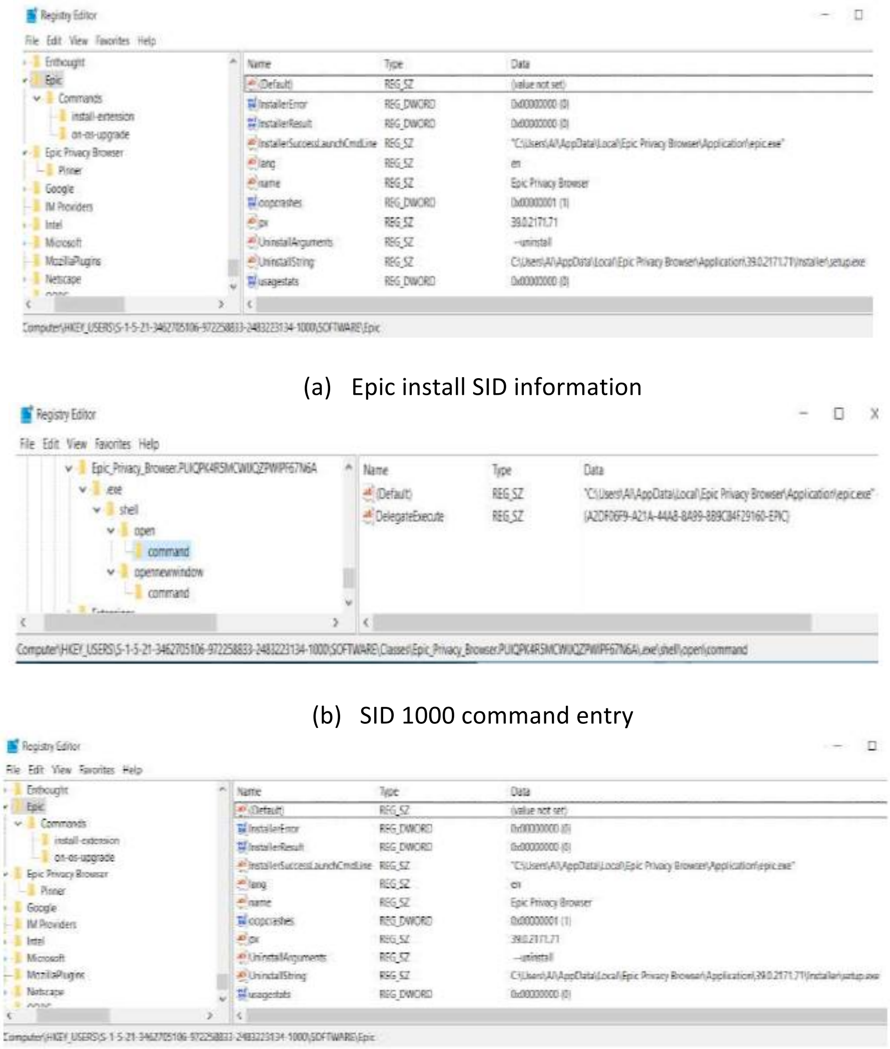


Name	Type	Data
(Default)	REG_SZ	"C:\Users\Al\AppData\Local\Epic Privacy Browser\Application\39.0.2171.71\d
ServerExecutable	REG_SZ	C:\Users\Al\AppData\Local\Epic Privacy Browser\Application\39.0.2171.71\de

omputer\HKEY_CLASSES_ROOT\WOW6432Node\CLSID\{A2DF06F9-A21A-44A8-8A99-889C84F29160-EPIC}\LocalServer32

Figure 7: Epic WOW6432 Node version #

The installation of Epic Privacy Browser on Windows 10 appears to differ slightly to that of Windows 7 with the addition of a 'Bookmarks.bak' file. This appears to be a backup of the bookmarks file and remains, even when the browser is closed. All other files appear to behave in the same way as in Windows 7 in that the additional cache folder and files are generated on the launch of the browser and then are deleted immediately on its conclusion. A running system with browser displayed offers the best opportunity to capture the default folder and, therefore the complete history and cache but all is not lost if the system is powered off. Although many of the files display in Encase as deleted, the data, and often the metadata, appears to be present (Figure 9). Stored in Windows\ServiceProfiles\NetworkService\ is a file named NTUSER.DAT.LOG2 (Figure 10). The file logged search queries carried out during the experiment, including the site contacted to carry out the search. https://epicsearch.in. Windows 10 drive image (E01) returned 52,000 hits from keyword searches. The same search terms resulted in 343,000 hits on the Windows 7. It appears that live capture for Epic artefact evidence in Windows 10 is far more beneficial when dealing with evidence from this operating system compared to Windows 7.



Name	Type	Data
(Default)	REG_SZ	(value not set)
InstallerError	REG_DWORD	0x00000000 (0)
InstallerResult	REG_DWORD	0x00000000 (0)
InstallerSuccessLaunchCmdLine	REG_SZ	"C:\Users\Al\AppData\Local\Epic Privacy Browser\Application\epic.exe"
lang	REG_SZ	en
name	REG_SZ	Epic Privacy Browser
oopcrashes	REG_DWORD	0x00000001 (1)
px	REG_SZ	39.0.2171.71
UninstallArguments	REG_SZ	--uninstall
UninstallString	REG_SZ	C:\Users\Al\AppData\Local\Epic Privacy Browser\Application\39.0.2171.71\Installer\setup.exe
usagestats	REG_DWORD	0x00000000 (0)

Computer\HKEY_USERS\S-1-5-21-3462705106-972258833-2483223134-1000\SOFTWARE\Epic

(a) Epic install SID information

Registry Editor
File Edit View Favorites Help
Epic_Privacy_Browser.PUIQPK4R5MCWIXQZPWIPF67N6A
.exe
shell
open
command
opennewwindow
command

Name	Type	Data
(Default)	REG_SZ	"C:\Users\Al\AppData\Local\Epic Privacy Browser\Application\epic.exe"
DelegateExecute	REG_SZ	{A2DF06F9-A21A-44A8-8A99-8B9C84F29160-EPIC}

Computer\HKEY_USERS\S-1-5-21-3462705106-972258833-2483223134-1000\SOFTWARE\Classes\Epic_Privacy_Browser.PUIQPK4R5MCWIXQZPWIPF67N6A\.exe\shell\open\command

(b) SID 1000 command entry

Name	Type	Data
(Default)	REG_SZ	(value not set)
InstallerError	REG_DWORD	0x00000000 (0)
InstallerResult	REG_DWORD	0x00000000 (0)
InstallerSuccessLaunchCmdLine	REG_SZ	"C:\Users\Al\AppData\Local\Epic Privacy Browser\Application\epic.exe"
lang	REG_SZ	en
name	REG_SZ	Epic Privacy Browser
oopcrashes	REG_DWORD	0x00000001 (1)
px	REG_SZ	39.0.2171.71
UninstallArguments	REG_SZ	--uninstall
UninstallString	REG_SZ	C:\Users\Al\AppData\Local\Epic Privacy Browser\Application\39.0.2171.71\Installer\setup.exe
usagestats	REG_DWORD	0x00000000 (0)

Computer\HKEY_USERS\S-1-5-21-3462705106-972258833-2483223134-1000\SOFTWARE\Epic

(c) Epic software entry in 1000 SID

Figure 8: SID information

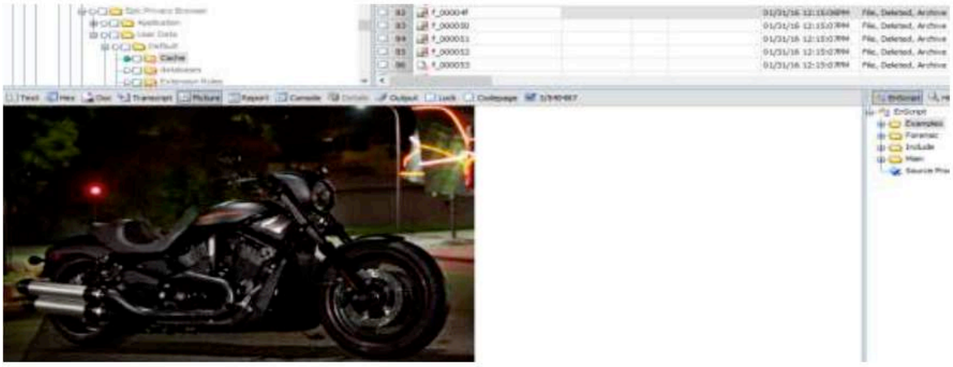
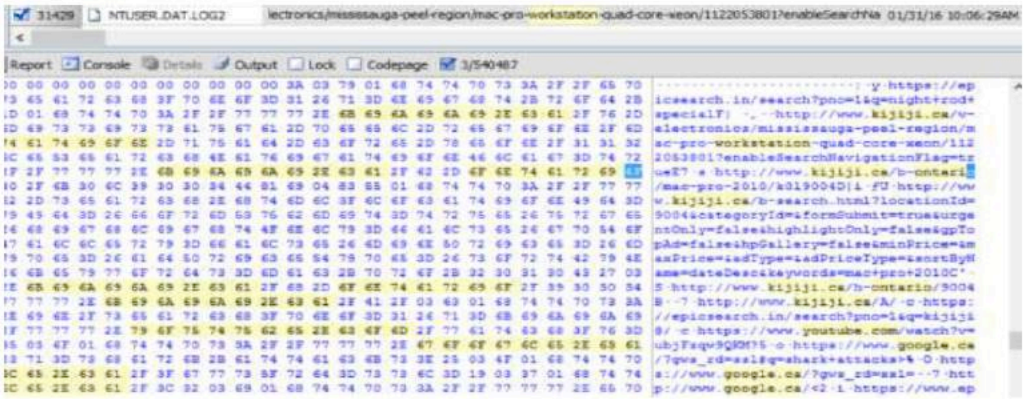


Figure 9: Night rod special cache - shown as deleted data

5.2 Live Analysis

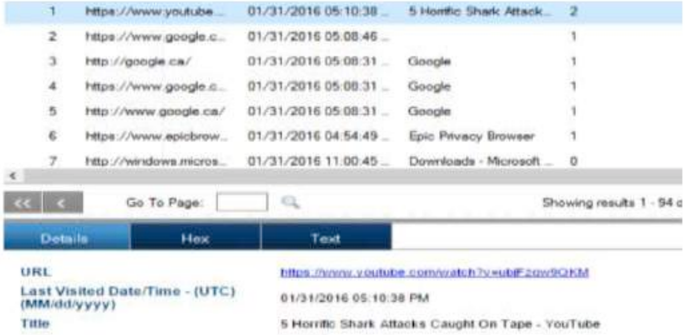
Windows 10 relied heavily on live memory storage during the use of Epic Privacy Browser with the analysis reporting that the newest offering from Microsoft was responsible for approximately 80% of the live captured data compared with the same tests on Windows 7, again enforcing the importance of live data capture. Encase and IEF was used to analyse and present the data. IEF results of note are as follows (Figure 11).



☑ 31429 NTUSER.DAT.LOG2 lectronics/mississauga-peel-region/mac-pro-workstation-quad-core-xeon/1122053801?enableSearchNa 01/31/16 10:06:29AM

```
··························y·https://ep
icsearch.in/search?pno=1&q=night+rod+
specialF) ·,··http://www.kijiji.ca/v-
electronics/mississauga-peel-region/m
ac-pro-workstation-quad-core-xeon/112
2053801?enableSearchNavigationFlag=tr
ueE7·s·http://www.kijiji.ca/b-ontari
/mac-pro-2010/k0l9004D|i·fU·http://ww
w.kijiji.ca/b-search.html?locationId=
9004&categoryId=&formSubmit=true&urge
ntOnly=false&highlightOnly=false&gpTo
pAd=false&hpGallery=false&minPrice=&m
axPrice=&adType=&adPriceType=&sortByN
ame=dateDesc&keywords=mac+pro+2010C*
5·http://www.kijiji.ca/b-ontario/9004
B··7·http://www.kijiji.ca/A/·c·https:
//epicsearch.in/search?pno=1&q=kijiji
8/·c·https://www.youtube.com/watch?v=
ubjFzqw9QKM?5·o·https://www.google.ca
/?gws_rd=ssl#q=shark+attacks>%·O·http
s://www.google.ca/?gws_rd=ssl=··7·htt
p://www.google.ca/<2·i·https://www.ep
```

Figure 10: NTUSER.DAT.LOG2 file information



1	https://www.youtube...	01/31/2016 05:10:38 ...	5 Horrific Shark Attack...	2
2	https://www.google.c...	01/31/2016 05:08:46 ...		1
3	http://google.ca/	01/31/2016 05:08:31 ...	Google	1
4	https://www.google.c...	01/31/2016 05:08:31 ...	Google	1
5	http://www.google.ca/	01/31/2016 05:08:31 ...	Google	1
6	https://www.epicbrow...	01/31/2016 04:54:49 ...	Epic Privacy Browser	1
7	http://windows.micros...	01/31/2016 11:00:45 ...	Downloads - Microsoft ...	0

URL: https://www.youtube.com/watch?v=ubjFzqw9QKM

Last Visited Date/Time - (UTC) (MM/dd/yyyy): 01/31/2016 05:10:38 PM

Title: 5 Horrific Shark Attacks Caught On Tape - YouTube

Figure 11: Search results captured in live memory

Data within the Gmail account, that was displayed but not directly accessed, was also captured in memory and parsed by IEF. Information of this nature if invaluable to any forensic investigator as it's often difficult to place a user behind the keyboard. The live memory capture shows not only the browser install location, but also the user account that it was installed in. 52,000 hits were recorded from the combined Keyword searches entered in Encase, against the live memory dumps of Epic queries on both Windows 7 and Windows 10 operating systems. Of the 52,000 hits, approximately 38,000 were recorded from the Windows 10 operating system.

6. Discussion

So what artefact evidence is produced when Epic Privacy Browser is installed on the Windows 10 operating system platform? On installation the application creates a number of documents in the C:\Users\User\AppData\Local\Epic Privacy Browser folder. A default folder is also created that houses data on installation and temporary files and folders used only when the browser is launched. Even though the temporary files are deleted on closure, a great deal of information can be retrieved from both live and post-mortem examination. Registry entries, specific to the user account (SID) are populated and recovered using software such as Registry Viewer. Comparing to Windows 10, on Windows 7, Epic choses the same location for application installation and, by default, installs the same files and folders as with Windows 10 (with the exception of the *bookmarks.bak* included in Windows 10). Artefact evidence is written to areas such as the pagefile.sys and little effort is made to delete and overwrite private browsing data. Another important question is that whether all Internet artefact evidence cleared when Epic Privacy Browser is closed? Although temporary files and folders within the default folder of the Epic Browser are cleared when the application is closed, the data appears readily available to the forensic examiner, using the standard tools. Besides, live memory capture is beneficial for many reasons and the acquisition of Epic artefact evidence is no exception. Finding a computer running with the application displayed or minimised on screen would afford the examiner the opportunity to extract the browser 'default' folder in its entirety, thereby capturing all the temporary files and data within. Live memory dump would also glean a wealth of information, as demonstrated in this dissertation. Acquisition and analysis of the imaged drive has shown to be of benefit from both the Windows 7 and Windows 10 operating systems. Important artefact evidence was found in deleted data files, *pagefile.sys, hiberfil.sys, Ntuser.dat* log files and unallocated space. It appears that the browser does very little to, either overwrite the information, or prevent the data being written to the drive. So looking at the differences between the artefact evidence when using Epic Privacy Browser on Windows 10 compared to Windows 7 Operating systems. It appears that Windows 7 is far more RAM dependent than its successor and so far, more evidence was found on the drive. Windows 10 RAM dump produced 80% for the live memory data from keyword searches. Besides, both *ChromeHistoryView* and *ChromeCacheView* were successful in presenting data acquired from the Epic browser default folder. This was expected and both Google Chrome and Epic Privacy Browser hail from the Chromium source code.

7. Conclusion and Future work

In this paper, we present the forensic acquisition and analysis of Epic privacy browser on Windows 7 and Windows 10. Epic Privacy Browser prides itself on protecting the user's privacy when online and reports to clear all traces of browsing history on closure. The files and folders created on a temporary basis do get deleted at the end of a browsing session, but the information was still readily available to any forensic examiner using the standard tools. Windows 10 live memory data produced the bulk of Epic artefact evidence in this operating system, although data was also written to the drive in the areas listed above. The results of this research are useful to, and may be referenced by, forensic experts involved in investigations concerning web activity and also for seeking advanced techniques and methods for recovering, parsing and analysing web browser specific data. Some topics for further scientific and practical research is coming up. First of all, investigators can use forensic method proposed in this chapter to examine other privacy Internet browsers such as Browzar (Warren et al. 2017). Experimental results described in this paper can assist the researchers who are studying for new methods of preserving the privacy in the next generation of web browser or even in triage process for front-line forensic personnel (Hitchcock et al. 2016).

References

Connolly M. et al. (2011), Limiting the impact of data breach & the case of the Sony PlayStation Network, Booz & Company in 2011

Fox-Brewster (2015), The NSA and Snowden: Securing the All-Seeing Eye, *Communications of the ACM*, Vol. 57 (5), p.44-51, 2015.

Toxen, B. (2014), How Snowden Breached the NSA from the Inside, Infosecurity Magazine, Nov 13th 2013, Available online: https://www.infosecurity-magazine.com/news/how-snowden-breached-the-nsa-from-the-inside/, Accessed January 2017

Regshot (2016), https://sourceforge.net/projects/regshot/

Gabet, R.M., (2016). A comparative forensic analysis of privacy enhanced web browsers, Purdue Universit.

Farina, J., Kechadi, M-T., and Scanlon, M. (2015), Project Maelstrom: Forensic Analysis of the BitTorrent-Powered Browser *Journal of Digital Forensics, Security and Law*, 10 (4), p. 115-124.

Aggarwal G., et al. (2013) An Analysis of Private Browsing Modes in Modern Browsers, In Proceedings of the 19th USENIX Security Symposium, Wardman Park Marriott Hotel, Washington, D.C. 11-13 Aug. 2013.

Marrington, A., Baggili, I., Al Ismail, T., & Al Kaf, A. (2012). Portable web browser forensics: A forensic examination of the privacy benefits of portable web browsers. In Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on (pp. 1-6). IEEE.

Khanikekar . S. K. (2010). Web Forensics. Graduate Thesis, A&M University, Texas, USA

Hedberg A. (2013), The Privacy of Private Browsing, Technical Report, Tufts University, MA, USA

Rubenking, N. (2014), Epic Privacy Browser, PC Magazine, May 2014, Available online: http://in.pcmag.com/epic-privacy-browser/70902/review/epic-privacy-browser

Warren, C., El-Sheikh, E., Le-Khac, N-A. (2017) Privacy Preserving Internet Browsers – Forensic Analysis of Browzar, In K. Daimi (Ed.), *Computer and Network Security Essentials*, Springer Verlag, Chapter 21, p.117-136, 2017 (In press)

Hitchcock, B., Le-Khac, N-A. and Scanlon, (2016) Tiered Forensic Methodology Model for Digital Field Triage by Non-Digital Evidence Specialists, *Digital Investigation* Vol. 16(13S), p.S75-S85, 2016