CHAMPLAIN COLLEGE

LCDI

The Senator Patrick Leahy Center for Digital Investigation

PirateBrowser Artifacts

Written by
Chris Antonovich
Researched by
Olivia Hatalsky

175 Lakeside Ave, Room 300A
Phone: 802/865-5744
Fax: 802/865-6446
http://www.lcdi.champlin.edu

Published Date

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

Recently, governments have been trying to crack down on illegal file sharing on a global scale. Websites like BitSnoop, the Pirate Bay, ExtraTorrent, and IsoHunt have been blocked by the Belgian Anti-Piracy Federation. In the Netherlands, the Pirate Bay was black listed because of a court order brought by BREIN, a private foundation aimed at stopping Internet piracy. As more countries are imposing censorship mandates, new and creative solutions are being sought in order to access these sites. PirateBrowser was created to allow individuals access to pirating and torrenting sites.. Over the course of two months, TorrentFreak reported one million downloads on the site, yet only 0.5% of all Pirate Bay visitors use PirateBrowser. In our experiment, we wanted to test the difference between PirateBrowser's artifacts and its parents, Mozilla Firefox 23 and Firefox Portable. Additionally, we wanted to test was PirateBrowser's ability to connect to blocked torrent websites such as Torrentz, BitTorrent, and The Pirate Bay.

Background:

PirateBrowser was released in August 2013, on the 10th anniversary of notorious torrent site the Pirate Bay (Vincent 2013). The creators released PirateBrowser under the banner of the Pirate Bay and based it on Mozilla Firefox 23 and Firefox Portable, allowing it to be run from a thumb drive. The Firefox-based browser also had integrated FoxyProxy and Tor's Vidalia network, allowing it to connect to blocked sites. The creators do not claim that using the browser anonymizes or privatizes your connection. There has been previous research done on Mozilla Firefox 23 and Firefox Portable artifacts, though there has been none that we are aware of on the PirateBrowser itself. We believe that the reason for Firefox Portable being integrated into the PirateBrowser was because it gave the browser ability to be run on a flash drive. The browser was made with the intent of giving users the ability to connect to torrent sites in countries where they are blacklisted.

Purpose and Scope:

The purpose of this experiment was to examine PirateBrowser's artifacts and to note any differences when compared to its parent browsers, Mozilla Firefox 23 and Firefox Portable. Our research would be helpful to the forensic community, as we would be providing guidelines with which forensic examiners could gather data.

Research Questions:

1.) How are PirateBrowser artifacts different than artifacts from other browsers?
2.) Can PirateBrowser effectively connect to blocked websites?

Terminology:

Artifacts - Any user data retrieved from the browser is considered an artifact, including cookies, caches, geo-location, search history, etc.

BitTorrent – Peer-to-peer (P2P) file sharing protocol designed to reduce the bandwidth required to transfer files. P2P distributes file transfers across multiple systems, thereby lessening the average bandwidth used by each computer. For example, if a user begins downloading a movie file, the BitTorrent system will locate multiple computers with the same file and begin downloading the file from several computers at once (*TechTerms)*.

Bulk Extractor – Bulk Extractor is a computer forensics tool that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. The tool also creates histograms of features that it finds.

Internet Evidence Finder (IEF) –IEF is forensic software created by Magnet Forensics that is capable of recovering internet artifacts in areas such as: Cloud Artifacts, Instant Messenger Chats, Media, Mobile Backup Files, P2P File Sharing, Social Networking Sites, Webmail Applications, Web Related Activity, and Web Page Recovery.

Digital Evidence – Digital evidence is "information of probative value that is stored or transmitted in a binary form" (NCFS, 2012). Digital evidence not only includes computers in the traditional sense, but also includes digital audio, video, and pictures.

Digital Forensics – The identification, examination, collection, preservation, and analysis of computer data and information.

EnCase – EnCase is a suite of digital forensics tools created by Guidance Software. The software comes in several forms designed for forensic, cyber security, and e-discovery use. Data recovered by EnCase has been used successfully in various court systems around the world.

Firefox Portable - "Mozilla Firefox® Portable Edition is the popular Mozilla Firefox web browser bundled with a PortableApps.com Launcher as a portable app. It allows you to take your bookmarks, extensions and saved passwords with you (*PortableAppscom).*"

FoxyProxy – FoxyProxy is a Firefox extension which automatically switches an internet connection across one or more proxy servers based on URL patterns.

FTK – Forensic Toolkit, or FTK, is computer forensics software made by AccessData. It scans a hard drive looking for data and information. It can, for example, locate deleted e-mails and scan a disk for text strings to use them as a password dictionary to crack encryption. The toolkit also includes a standalone disk imaging program called FTK Imager. FTK Imager saves an image of a hard disk in one file or in segments that may be reconstructed later on. It calculates MD5 hash values and confirms the integrity of the data before closing the files.

PirateBrowser – PirateBrowser is a bundle package of the Tor client (Vidalia), Firefox Portable browser (with FoxyProxy add-on), and addtitional custom configurations that allows you to circumvent censorship that certain countries such as Iran, North Korea, United Kingdom, The Netherlands, Belgium, Finland, Denmark, Italy and Ireland impose onto their citizens.

The Pirate Bay – A website that provides magnet links to torrent files to make peer-to-peer sharing using the BitTorrent protocol possible. It is one of the most popular websites that offers this service.

Tor - Tor is short for "The Onion Router," free software that enables online anonymity by directing Internet traffic through a free worldwide volunteer network that consists of more than three thousand relays.

Torrent – A file that has the .torrent suffix and is available for download from websites using the BitTorrent protocol. They are different from regular downloads because they are usually downloaded from more than one

server at a time, which reduces the bandwidth used by each server, speeding up file transfers. Torrents are considered peer-to-peer (P2P) sharing.

Vidalia (Tor client) - Vidalia is a cross platform graphical controller for the Tor software. It lets a user start and stop Tor as well as see how much bandwidth they are consuming and how many circuits they have active.

Virtual Machine (VM) – A virtual machine is a software-based computer that executes and runs programs like a physical machine. A virtual machine supports the execution of a complete operating system. VMs usually emulate an existing architecture and are built with the purpose of either providing a platform to run programs where the real hardware is not available for use or for more efficient use of computing resources, both in terms of energy consumption and cost effectiveness (known as hardware virtualization, the key to a cloud computing environment).

VMware Workstation – Popular virtualization software used in desktops and laptop computers. VMware Workstation allows the creation and customization of virtual machines, supporting many types of Windows, Mac, and Linux Operating Systems.

Methodology and Methods

We chose to use three VMs each running Windows 7, allocating a different browser to be used on each VM. We then made a list of data generation steps for the user to follow on each of the VMs. After imaging the VMs and the thumb drive used to run Firefox Portable, we ran them through FTK, EnCase, Bulk Extractor, IEF, and MantaRay to compare results.

Table 1: Equipment

Item	Identifier	Size/Specification and/or Use
FTK 4.1	*FTK*	*Forensic tool for comparing acquired images*
FTK Imager	*FTK Imager*	*Imaging tool for acquiring forensic images*
EnCase 7	*EnCase 7*	*Forensic tool for comparing acquired images*
MantaRay	*MantaRay*	*Tool for automating processing forensic images with open source tools*
Bulk Extractor	*Bulk extractor*	*A tool that scans a disk image and extracts important information without parsing*
Internet Evidence Finder	*IEF*	*Software capable of recovering internet artifacts in many common areas*
Flash Drive	*Blue SanDisk*	
VMware 10.0	*VMware*	*Virtualization and cloud computing software provider for x86-compatible computers.*
SQLite Database Browser 2.0	*SQLite Browser*	*An open source tool meant for users that want to create databases, and search and edit data.*

Data Collection:

As the user followed the list of steps, he/she recorded each task on a data generation spreadsheet, recording the task and the time (see Appendix A, B, C).We then imaged the drives into different folders, so that our forensic

programs could run while still preserving evidence integrity. To recover artifacts from all three browsers, we first used IEF, then Bulk Extractor with MantaRay, and finally EnCase and FTK (to look for SQLite queries).

Analysis

We came into the project concerned that finding the artifacts for through IEF may prove to be less fruitful than using a program like EnCase because IEF may not be able to look in the same places. For example, with EnCase, we could directly access a file location to look for browser artifacts, while IEF has predetermined file signatures to look for. However, EnCase and FTK are the most reliable software to find artifacts for PirateBrowser. Since the PirateBrowser uses FoxyProxy and The Onion Network to connect to other blocked sites, we think that it will successfully connect to blocked torrent sites.

NOTE: It was suggested we add more screenshots to the Results sections, compare IEF report screenshots with OS forensics process tabs and screenshots, and explain our processes more. We are still working on processes explanation. We blocked www.ThePiratebay.sx through DNS blocking.

Results

1. IEF

1.1.1 Mozilla 23

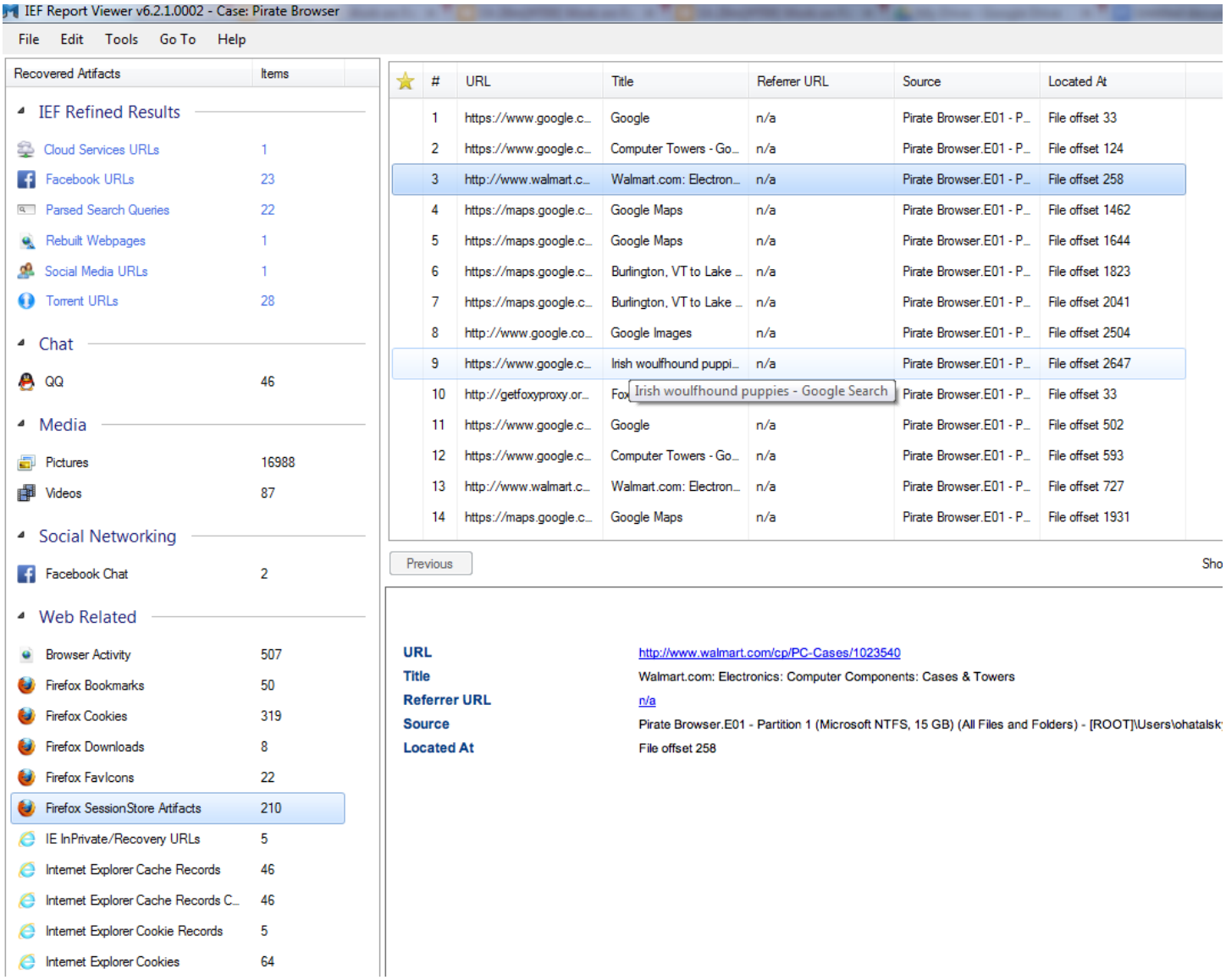
All of the data that was generated and recorded (Appendix A) appeared in the IEF timeline for Mozilla 23. By looking at the timeline, we were able to clearly see all of the user generated data, including the websites visited, email accounts logged into, the chats that were used, and the downloads from the browser. Along with our generated data, there was also a lot of advertisement information that was logged on the browser. Interestingly enough, a lot of it was from websites such as Twitter which the user never visited. This is similar to the information that we gathered from PirateBrowser, finding more background noise than usable data.

1.1.2

1.1.3 PirateBrowser

After recording all of the steps taken, (Appendix B) we were able to successfully image the evidence using FTK Toolkit. When we opened IEF Report Viewer, we found that under the Firefox "SessionStore Facts" we were able to find most of the user's URL history. It is also important to note that after the FoxyProxy session the data repeats itself for an unknown reason. When we looked for chat artifacts, we could only find evidence that the user spent 13 minutes in Facebook chat and there was no evidence of Google talk chat at all. The PirateBrowser's preconfigured bookmarks for torrent websites could be seen on the IEF timeline. These bookmarks include: the Pirate Bay, Torrentz, 1337x, Fenopy, H33T, IsoHunt, KAT, BitSnoop, Movie4K, Monova, TorrentCrazy, and EZTV. There were 507 items under the "Browser Activity" tab, seemingly coming from the minimal use of Internet Explorer (Appendix B). While the user only went to IE's homepage and to the PirateBrowser website, there are 64 items under "Internet Explorer Cookies." The information that IEF did obtain included most of the browser history, including the FoxyProxy website, abcnews.com, and

nbcnews.com. Other than these websites, all of the other browser traffic appeared to be from advertisements. We could also see downloads by the user, including Skype, puppy.jpeg, narwhal.jpeg, iTunes, and Flash.



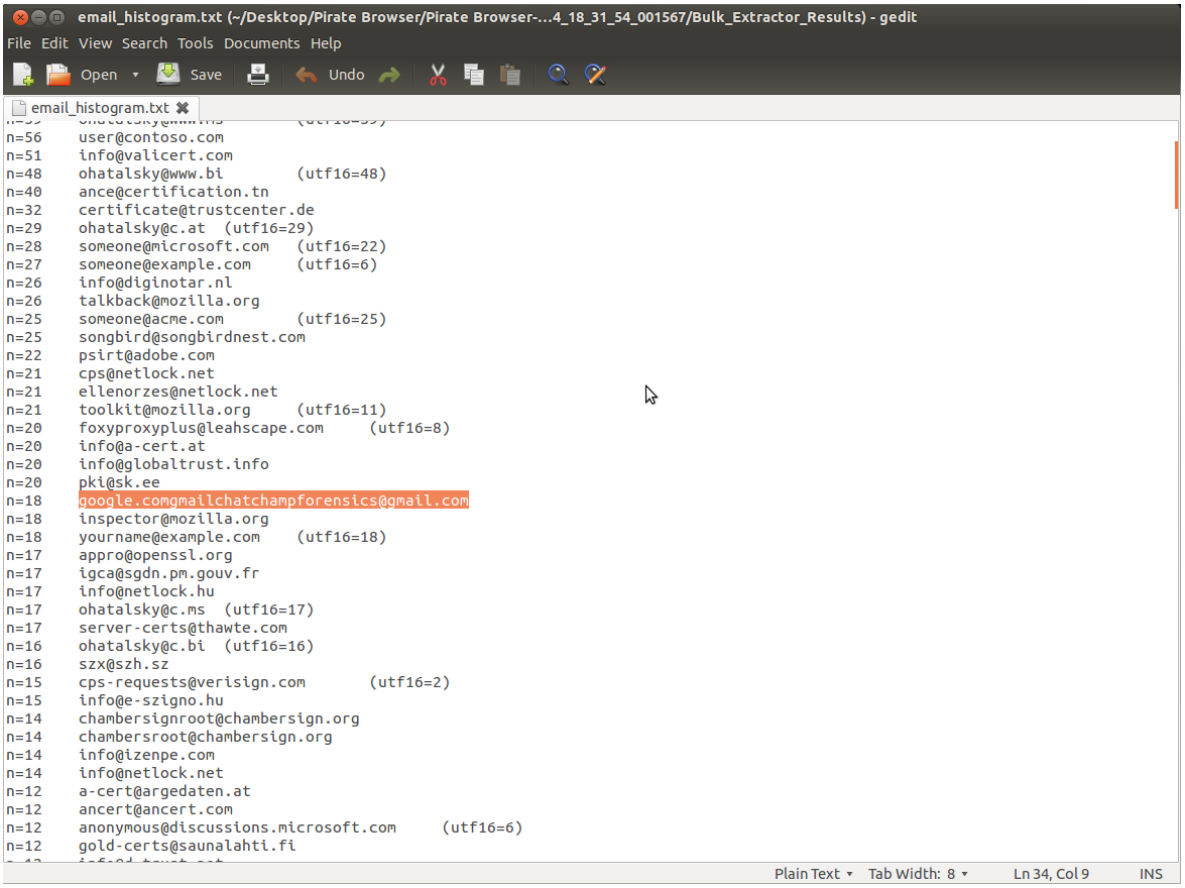
1.1.4 Firefox Portable

We found that the Virtual Machine that was used to run Firefox Portable had no traceable data of any kind on it, as the browser history was saved directly to the flash drive. This is interesting to note because it shows computers that run Firefox Portable from a flash drive will retain no information of the searches conducted or any downloads made. Using IEF to look at the image of the flash drive itself, all of the websites visited could be accessed. We were able to find most actions (Appendix C) in IEF, not including chat logs from Google. Unlike Mozilla 23, there was minimal advertisement chatter from third parties recorded, but Firefox Portable did have more cookies than Mozilla 23.

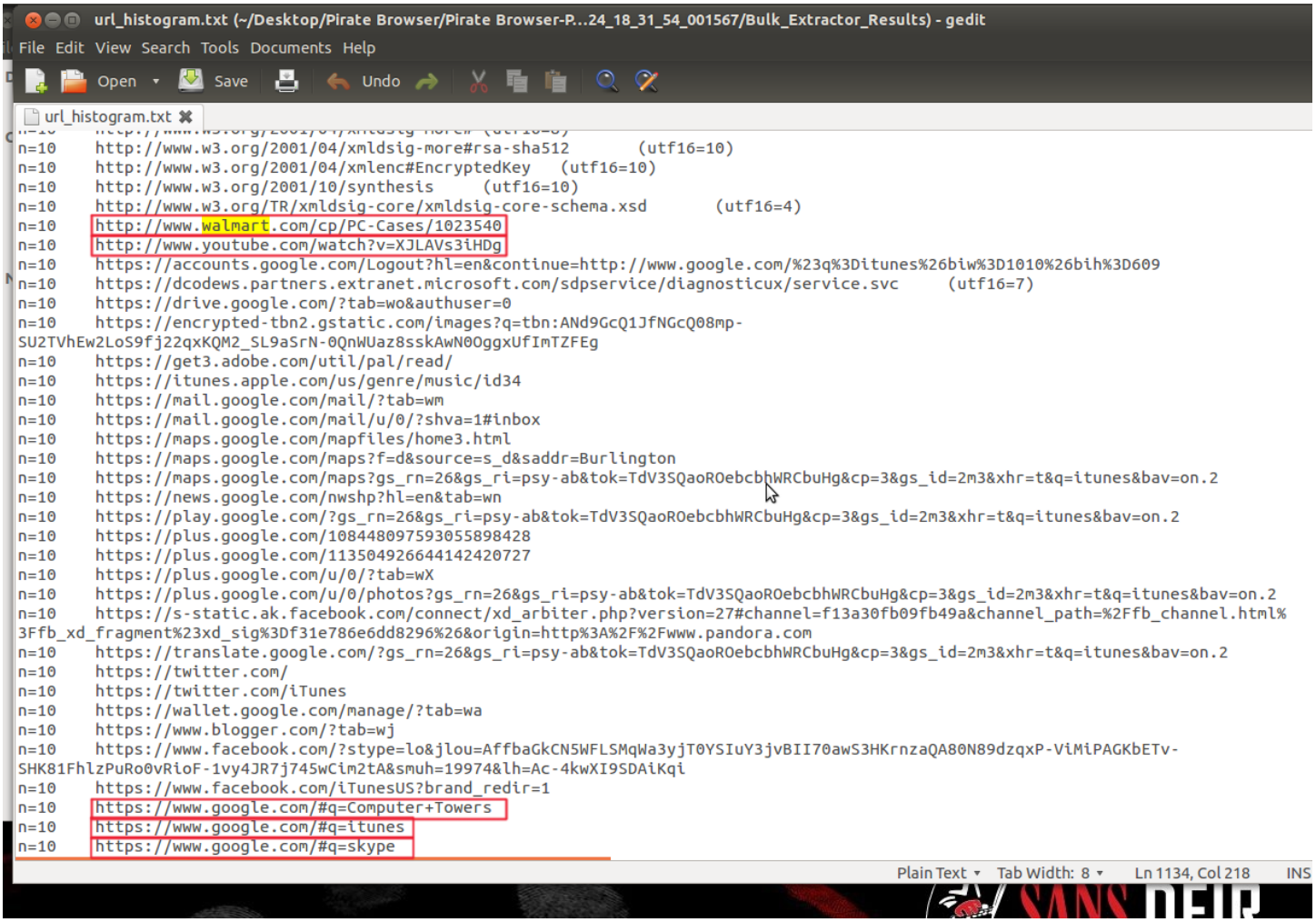
2. Bulk Extractor/MantaRay

MantaRay is a forensic suite created by ManTech that can automate the use of open source tools in processing forensic images, directories, and individual files. The open source tool utilized for this research was Bulk

Extractor. The files supplied by Bulk Extractor that were most useful in our comparison of the browsers were: “domain.txt,” “domain_histogram.txt,” and email.txt.” These files provided information on browser history, chat logs, and download data for each of the browsers tested. For example, the results for “email_histogram” in the PirateBrowser VM turned up google.comgmailchatchampforensics@gmail.com. This service is the only evidence we found for Gmail chat (Appendix B).



Bulk Extractor pulls any data that has the variable “xxx@yyyy.zz,” explaining the numerous emails from programmers, certificates, and so on.

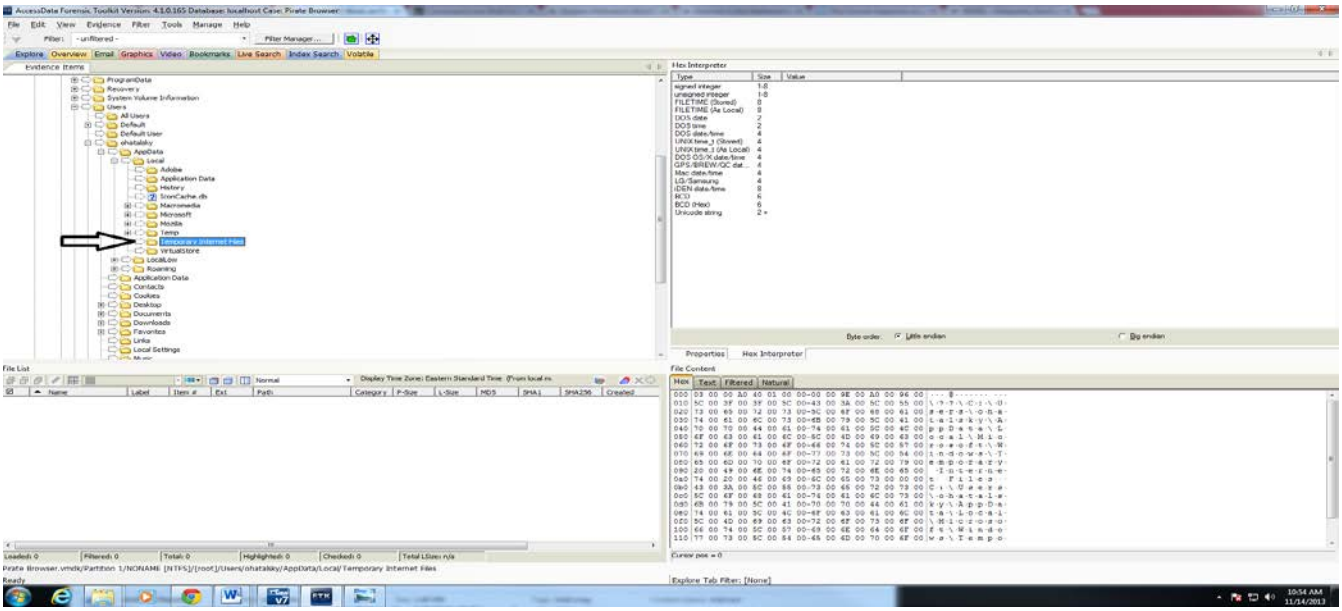


Bulk Extractor pulls up any web address accessed from the VM, from the user's actual browser history to background chatter. These results are helpful to investigators because we can discern that the user was using foxy-proxy, as well as that specific Gmail account to chat with another user.

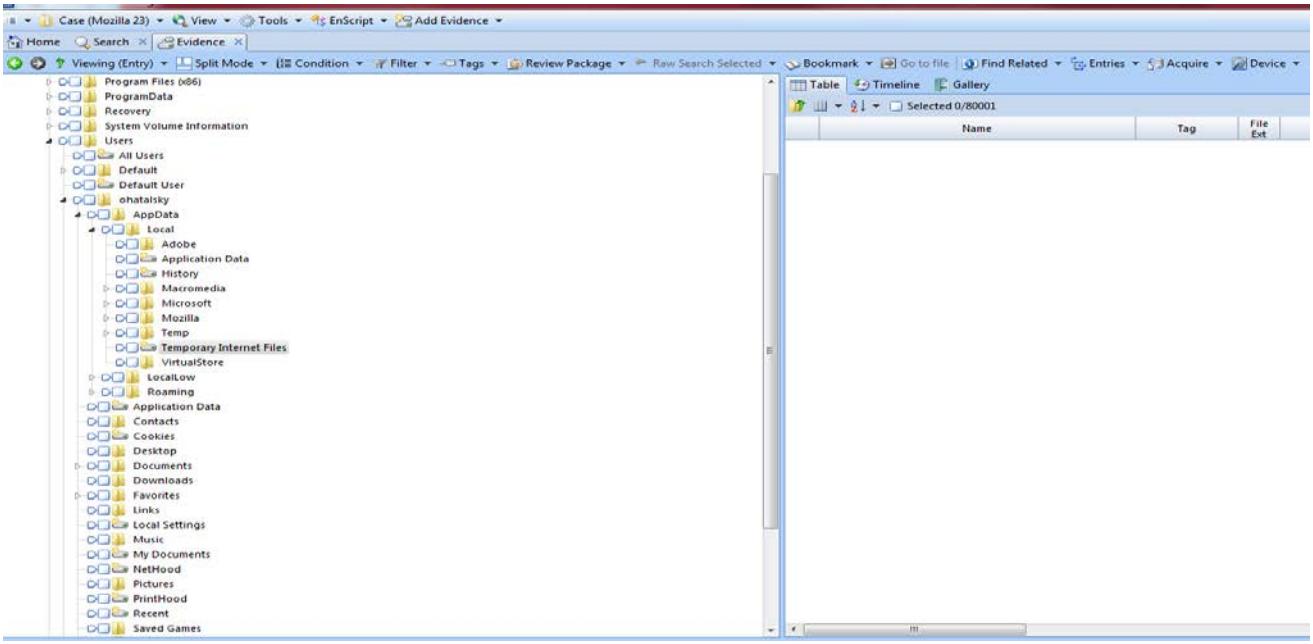
Of all the tools used to search for browser artifacts, specifically on the PirateBrowser, Bulk Extractor turned up some of the most useful and clear results.

EnCase/FTK

While installing PirateBrowser, we accepted the automatic download path without realizing how difficult it would be to retrieve data from the folder "Users\ohatalsky\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\92E716H3." When we tried to view the OS in FTK 4.1, we could not access the folder's contents.



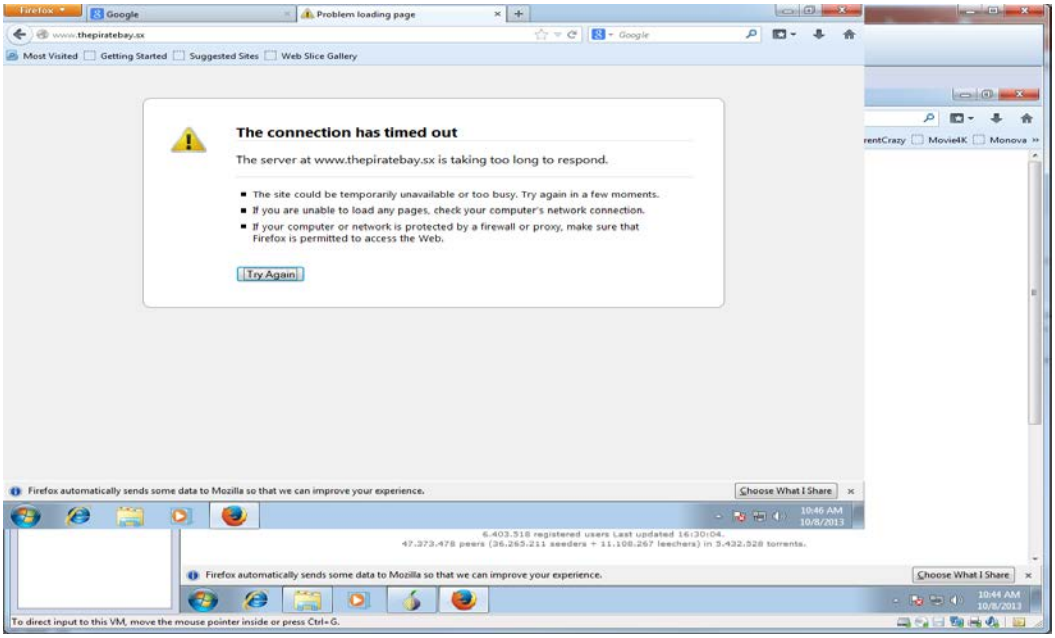
After several attempts, we could not find a way to access the files through FTK 4.1, at which point we used EnCase 7. We tried using EnCase 7 search utility for the file contents using the string "piratebrowser." At this point, we found a number of SQLite tables, only one of which to us found helpful (the download path of narwhal.jpg). Upon finding the .sqlite files, we exported them to view under SQLite Database Browser.



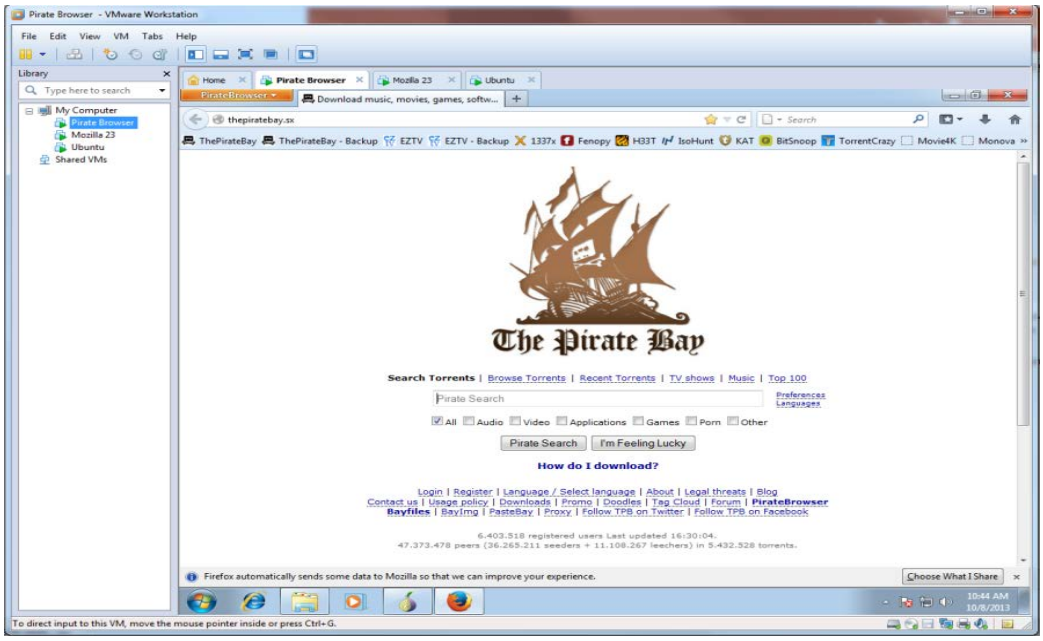
PirateBrowser Censorship Circumvention

For our tests, we blacklisted the DNS of www.ThePirateBay.sx in our network and then attempted to access it with all of our web browsers. The images below show that Firefox was not able to connect to the blocked website while PirateBrowser was.

Firefox Connection Attempt:



PirateBrowser Connection Attempt:



Conclusion

PirateBrowser is most useful when you are using it to torrent in countries, or situations, where torrent sites are blocked; if you are trying to access blocked sites other than those for torrents, you are better off using something like Tor. PirateBrowser only allowed censorship circumvention for torrents sites. When we tried to

look for artifacts pertaining to the PirateBrowser in EnCase or FTK, we had difficulty finding data. The reason we believe it was hard to find any artifacts for PirateBrowser was due to its location in "\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\92E716H3." It was difficult for us to do anything that required us to look into that folder. After realizing that we wouldn't be able to access the file through browsing through folders, we used search queries to look for the file location and access all of the folder's contents. We found that the folder held important evidence. Looking through what we could, we found SQLite tables that shed little light on the artifacts from the PirateBrowser. IEF proved to be very helpful in finding artifacts related to user history and downloads, while bulk extractor provided information pertaining to login information and added more in-depth browser history. We believe this was because the most useful artifacts were not stored in SQLite tables. They were stored in ".js" and ".bak" files where all of the browser history was found. When doing forensic research, we found that using the programs concurrently is the best way to accurately make conclusions based on the evidence.

Further Work

In order to more accurately research this browser, we feel that we should have been torrenting additional files to have a full understanding of this browser's ability. Another aspect of PirateBrowser we would be interesting in testing would be its ability to run from removable media, documenting its ability to run without leaving breadcrumbs in the OS.

Appendix A

Mozilla Firefox 23

Time	Action / Variable	User Interface / Software	Comments
10:28	Logged into VM		
10:29	Opened IE	Internet Explorer	
10:31	Went to www.google.com		
10:32	Clicked Link to Firefox page		
10:32	Went to Firefox's Download page		
10:34	Downloaded Firefox 23 and ran it	Firefox 23	
10:35	Went to www.google.com		
10:36	Searched: Computer Towers		
10:37	Went to www.walmart.com/cp/PC-Cases/1023540		
10:38	Clicked and Added Antec Nine Hundred Case, Black Finish to cart		
10:39	Went to www.google.com		

10:40	Clicked “Maps”		
10:40	Clicked “get directions”		
10:41	Clicked “get directions” –From Burlington, VT to Lake George, NY		
10:42	Clicked Images		
10:42	Searched “Irish wolfhound puppies”		
10:43	Clicked on specified image		
10:44	Saved Image as “puppy” downloads folder		
10:45	Went to www.nbcnews.com		
10:49	Clicked On Article: Obama faces showdown with Putin at G-20 over summit		
10:50	Went to abcnews.go.com		
10:50	Clicked on World		
10:50	Clicked on “Obama, Putin Set for G-20 Showdown over Syria”		
10:52	Went to www.google.com		
10:53	Searched “skype”		
10:53	Clicked on “www.skype.com		
10:54	Clicked on “Downloads”		
10:54	Clicked on “get skype for windows for Windows Desktop”		
10:55	Ran Skype Install		
10:57	Idle		
11:35	Went to “www.facebook.com		
11:36	Opened Chat		
11:37	Sent Chat Message “Olivia” to Olivia Hatalsky		
11:37-11:44	Chatted with facebook account user “Olivia Hatalsky” on Facebook		
11:45	Went to “www.gmail.com” and logged into account		
11:47-11:55	Chatted with Olivia via gmail chat		
11:56	Went to youtube.com		
11:56	Signed out the champ forensics account		

11:57	Searched 10 years chasing the rapture		
11:57	Clicked on First link		www.youtube.com/watch?v=f8yiyvqzkQ8
11:58	Clicked on 10 Years the Wicked ones		www.youtube.com/watch?v=XJLAVs3iHDg
12:00	Went to www.google.com		
12:01	Searched for Itunes and clicked apple.com/itunes link		
12:02	Clicked link and Downloaded Itunes		
12:04	Went to Pandora.com		
12:04	Went to install flash		
12:05	Installed Flash		
12:06	Went back to pandora		
12:06	Made Evans Blue Radio		
12:07	In a new tab, went to “www.bing.com”		
12:08	Clicked first link		www.narwhal.org/NarwhalFacts.html
12:09	Clicked back button and went to “Narwhal Pictures” under “also try”		
12:10	Clicked on Narwhal Picture		
12:55	Saved to Desktop as Narwhal.jpg		

Appendix B

Pirate Browser

Time	Action / Variable	User Interface / Software	Comments
11:01	Opened IE		
11:02	Went to www.piratebrowser.com		
11:04	Downloaded and ran piratebrowser, self-extracting archive		
11:08	Extracted file		C:\Users\ohatalsky\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\92E716H3
11:08	Started Pirate Browser	PirateBrowser	Connecting to Tor Network
11:12	Went to “www.google.com		
11:13	Searched “computer towers”		
11:13	Clicked On www.walmart.com/cp/PC-		

	Cases/1023540		
11:14	Clicked on and added to cart “antec Nine hundred case black finish		`
11:15	Went to www.google.com		
11:16	Clicked on “Maps”		
11:16	Clicked on Get directions		
11:17	Clicked Get Directions-A: Burlington, VT B: Lake George, NY		
11:18	Clicked Images		
11:18	Searched Irish wolf hound puppies		
11:18	Clicked on Image		
11:19	Downloaded image as puppy to downloads folder		
11:21	Went to ww.nbcnews.com		
11:24	Clicked on article Obama faces showdown with Putin at G-20 Summit over Syria		
11:25	Went to abcnews.go.com		
11:25	Went to “World”		
11:27	Clicked on “Obama , Put Set for G-20 Showdown over Syria”		
11:28	Went to www.google.com		
11:28	Searched skype		
11:29	Clicked on www.skype.com		
11:29	Clicked on Downloads		
11:29	Clicked get skype for windows desktop and saved file		
11:31	Ran Skye setup		
11:32	Idle		
12:12	Went to facebook.com		
12:13	Logged into facebook and went to chat		
12:14	Clicked Home		
12:14	Clicked on Digital Forensics Group Page		
12:22	Open chat with Olivia		
12:31	Logged into facebook		

12:32	Went to gmail.com		
12:34	Logged into gmail.com		
12:38	Went to youtube.com		Signed out for me
12:39	Searched 10 Years chasing the rapture and clicked first link		
12:41	Clicked on video, went back ,Clicked on 10 Years the wicked ones		
12:43	Went to google.com		
12:43	Searched iTunes		
12: 44	Clicked On Download ITunes		
12:45	Downloaded ITunes		
12:45	Went to Pandora, Went to install flash		
12:46	Installed Flash		
12:47	Went back to Pandora		
12:47	Repeated last 3 steps (pirate browser did not recognize I installed flash)		
12:48	Went Back to Pandora tab		
12:49	Started Evans Blue Station		
12:49	Open New tab		
12:50	Went to bing.com		
12:50	Searched narwhal facts		
12:50	Clicked First link www.narwhal.org/NarwhalFacts.html		
12:51	Clicked Backwards, returned to search page		
12:51	Clicked on Also Try: Narwhal Pictures		
12:52	Clicked on a Narwhal Picture		

Appendix C

Firefox Portable

Time	Action / Variable	User Interface / Software	Comments

9:59	Opened FirefoxPortable Browser from thumbdrive	FirefoxPortable	
10:00	Went to www.google.com		
10:00	Clicked on Walmart.com link		
10:01	Clicked on Antec Nine Hundred		
10:01	Added to Cart		
10:01	Went to www.google.com		
10:02	Clicked on “Maps” Link		
10:02	Clicked on “Get Directions”		
10:03	Entered data into A and B as specified and got directions		
10:06	Clicked on Images		
10:07	Searched Irish Wolf hound puppies		
10:07	Saved as puppy		
10:08	Went to nbcnews.com		
10:09	Clicked on World		
10:12	Clicked on Top Stories Article “Peaceful Solution: Syria accepts Russia deal to hand over chemical weapons		
10:13	Went abcnews.go.com		
10:14	Clicked on World		
10:14	Clicked on top story Syria Vows to Accept Russian Plan as Way to Stave Off American Aggression		
10:15	Went to www.skype.com		
10:16	Went to downloads		
10:17	Clicked Get Skype for Windows Desktop and downloaded into downloads folder		
10:18	Installed Skype		
10:19	Went to facebook.com		
10:20	Logged in and chatted		
10:35	Went to gmail.com and logged in		
10:42	Went to youtube.com		
10:46	Searched for 10 years chasing the rapture and clicked first link		
10:48	Clicked video and then went back to original video after seeing it needed flash		

	was able to watch “10 years feeding the wolves(2010)(Full Album)HD”		
10:49	Went to www.google.com		
10:49	Searched in google’s search bar Itunes		
10:50	Clicked on specified link, apple.com/itunes		
10:50	Clicked Download Itunes		
10:51	Saved iTunes to downloads folder and installed		
10:52	www.pandora.com		
10:52	Went to flash download page		
10:53	Downloaded flash		
10:56	Installed flash		Error with flash being recognized
10:59	Closed Mozilla to install flash		
11:00	Went to Pandora.com again		
11:00	Went to bing.com in tab		
11:01	Searched for narwhal facts		
11:01	Clicked Back Button		
11:02	Clicked narwhal Pictures		
11:03	Saved narwhal picture to desktop		

References

* All numbers on this page are for demonstration purposes only; any resemblance to reality is purely coincidental

"BitTorrent." *TechTerms*. N.p., n.d. Web. 7 Nov. 2013. <http://www.techterms.com/definition/bittorrent>.

Digital evidence. (2012). *NCFS*. Retrieved from http://www.ncfs.org/digital_evd.html

Ernesto. (2013, October 19). TorrentFreak. TorrentFreak RSS. Retrieved from http://torrentfreak.com/pirate-bays-anti-censorship-browser-clocks-1-million-downloads-131019/

"Frequently Asked Questions." *FoxyProxy*. N.p., n.d. Web. 7 Nov. 2013. <http://getfoxyproxy.org/mozilla/faq.html>

"Mozilla Firefox, Portable Edition." *PortableAppscom News*. N.p., n.d. Web. 7 Nov. 2013. <http://portableapps.com/apps/internet/firefox_portable>.

Vincent, J. (2013, August 12). The Pirate Bay launches its own 'Pirate Browser' to dodge filters. *The Independent*. Retrieved October 24, 2013, from <http://www.independent.co.uk/life-style/gadgets-and-tech/news/the-pirate-bay-launches-its-own-pirate-browser-to-dodge-filters-8757257.html>