A Journey into Litecoin Forensic Artifacts

Tor, Silk Road, and Litecoin. Bitcoin artifacts now appear in forensic tools such as Magnet Forensics Internet Evidence Finder (IEF). As the price of Bitcoins increases, it could potentially price out participants. Litecoin provides a cheaper alternative attempt at a peer-to-peer currency. Litecoin, like Bitcoin, also allows users to mine for profit. The paper will go beyond what is taught in class by attempting profiling of users. The first user will be browsing for, downloading and accessing Tor, and related sites. O...

A JOURNEY INTO LITECOIN FORENSIC ARTIFACTS

GIAC (GCFA) Gold Certification

Author: Daniel Piggott, piggott.daniel@gmail.com
Advisor: Richard Carbone

Accepted: 20th May 2014

Abstract

Tor, Silk Road, and Litecoin. Bitcoin artifacts now appear in forensic tools such as Magnet Forensics Internet Evidence Finder (IEF). As the price of Bitcoins increases, it could potentially price out participants. Litecoin provides a cheaper alternative attempt at a peer-to-peer currency. Litecoin, like Bitcoin, also allows users to mine for profit. The paper will go beyond what is taught in class by attempting profiling of users. The first user will be browsing for, downloading and accessing Tor, and related sites. Our second user mines for Litecoins and our third user has bought or sold Litecoins.

Table of Contents

List of Figures

1. Introduction to Virtual/Crypto Currencies

Litecoin is a virtual peer-to-peer currency. Introduced 7 October 2011 (Wikipedia 2014) it follows Bitcoin, first introduced 3 January 2009 (Wikipedia 2014). Virtual currencies offer the possibility of anonymity to those seeking to move currency between the physical and virtual worlds. Examples could be:

- Someone trying to hide money.
- Speculators.
- Someone trying to buy illicit goods on the internet.
- Someone trying to hide an exchange of goods or money.

Litecoin is, according to Kashmir (2014), one of the most lucrative in terms of speculations with respect to financial gains. Crypto currencies are not currently straight forward to purchase for the average user. Here is an example of Bitcoin/Litecoin:

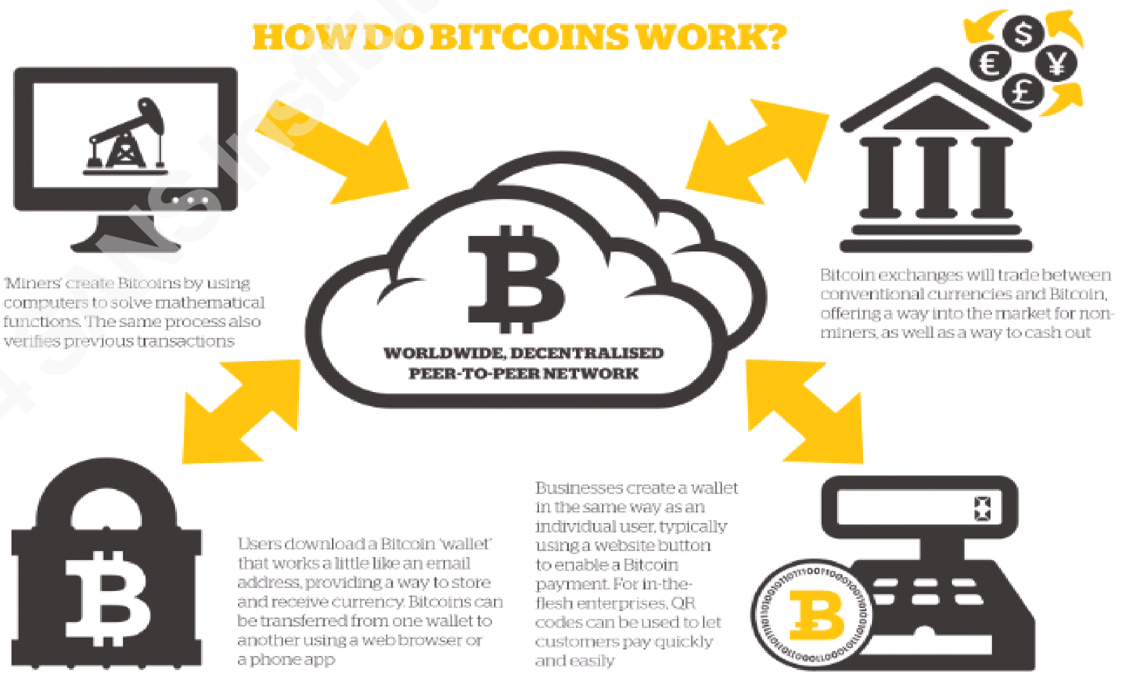

HOW DO BITCOINS WORK?
'Miners' create Bitcoins by using computers to solve mathematical functions. The same process also verifies previous transactions
WORLDWIDE, DECENTRALISED PEER-TO-PEER NETWORK
Bitcoin exchanges will trade between conventional currencies and Bitcoin, offering a way into the market for non-miners, as well as a way to cash out
Users download a Bitcoin 'wallet' that works a little like an email address, providing a way to store and receive currency. Bitcoins can be transferred from one wallet to another using a web browser or a phone app
Businesses create a wallet in the same way as an individual user, typically using a website button to enable a Bitcoin payment. For in-the-flesh enterprises, QR codes can be used to let customers pay quickly and easily

Figure AAT Comment, 2013 Bitcoin: what is it and how does it work?.

1.1. The Exchanges – Converting Physical Currency to Virtual Currency

First of all the user has to find a way of changing their currency in the real world into a virtual currency. For this they need the equivalent of a foreign exchange service. On the internet these exchanges are currently unregulated. They also sit in different geographical locations and are therefore covered by different legal jurisdictions.

To do the exchange some sites require identification which could lead to users giving away more personal information than they would normally do. Once you have converted the money into virtual currency the user then needs to decide where and how to store it electronically. Once in an electronic format the virtual currency needs to be adequately protected with encryption, password and backed up. Some users arrange to exchange at an agreed price on line on the various exchanges and then meet in person to exchange cash.

Indeed, Couts (2013) describes how users must first purchase Bitcoins to then be able to purchase Litecoins. However, this is not the case as exchanges exist to buy and sell the currency. One such site is https://litecoinlocal.org/ which will be examined in this paper with some example transactions.

1.2. The Peer-to-peer client

The peer-to-peer client (P2P) is the software which connects the user to the network to facilitate a transaction between two individuals without an exchange. All transactions are processed by each client. When you open your P2P program it updates itself from the network with all the transactions that make up the currency ledger. The client is also used to send and receive payments.

Haid (2013) discusses the use of Tor and virtual private networks for anonymity by those seeking to hide their identity. Virtual currencies have publicly available ledgers known to all the peer-to-peer participants. Therefore an audit trail of transactions should be possible to retrieve forensically from various sources. Anonymity will continue to be an issue until such time that physical identity can be tied to transactions.

Jules (2013) looks at anonymity and Bitcoins. This article confirms the issue around the audit trail of a transaction. Whilst it discusses using Tor for anonymity there are still points at which someone who wishes to remain anonymous has to trust another party.

1.3. Mining

Litecoin has distinct advantages over Bitcoin. Payments cannot only be processed quicker but mining is more efficient. Moreover, Litecoin can produce four times the quantity of a virtual currency compared with Bitcoin. Perhaps most importantly Litecoin can be mined by the average user whereas Bitcoin has now reached a stage where the average user is priced out of the mining market in terms of hardware, power and cooling required to mine for Bitcoins. (Wikipedia 2014)

As at 7 January 2014 Litecoin was trading at $25, and Bitcoin at $929. As Bitcoin increases in value, does it make Litecoin increasingly attractive and accessible to speculators?

Businesses and employers need to prepare for and be aware of the risk of malware and employees who could use company resources for mining for their own personal gain. Malware and organised criminals could also use corporation's resources and personal devices for mining. These resources might be in house, or cloud based such as Amazon web services. One example which was highlighted in 2013 was Chadwick (2013) whose Amazon cloud monthly spend went from $69 to $3493 after his account was hijacked by a hacker and utilized for mining.

Google has recently found applications in its play store which when installed on android devices, mine for crypto currencies. Smith (2014) found that of two applications one had been downloaded "*1 to 5 million times*". In the code there was mining going on in the background on the device. The phones that were infected with the mining malware were found in Kirk (2014) to overheat or suffer a battery drain.

1.4. Digital Wallet

Whichever crypto currency is being investigated one of the key files to identify is *wallet.dat* which is where the "*physical cryptographic private key file is stored*" (Heid, 2013). This file could be crucial to a forensic examiner and provide a quick way of identifying if other artifacts might exist. An examiner might also find a trail leading to a USB or other data storage device where the *wallet.dat* may be held offline to protect the data on it. With virtual currency applications being available for mobile devices as well this file could be located anywhere. A forensic examiner should consider all devices if trying to locate it. Malware may be of interest to forensic examiners as well with it being used by criminals to attempt to steal *wallet.dat* from user's devices (Barker, 2014). This malware could be general malware such as a phishing attempt to gain access to a user's machine. This could then call a further command and control server to pull down customised malware that looks for *wallet.dat*. It could be specifically built malware designed purely to look for virtual currency files. As well as personal wallets, businesses which accept digital payments may have a business wallet.

1.5. Example of the user process to do a transaction

Note this is after the user (Alice) having gone through the exchange. Alice has changed her cash from physical or virtual and downloaded her virtual coins to her wallet. So the user has already exchanged physical currency into virtual currency. Alice then downloads the Litecoin client and installs it on her device. Alice then exchanges her public address with Bob which in turn then allows Alice to receive 5 Litecoins from Bob. Finally, Alice places her Litecoins in her digital currency *wallet.dat* file:

1. Alice creates a new address in her P2P software. Here is a Litecoin example address (string of 33 characters) that gets created.
2. LVXXmgcVYBZAuiJM3V99uG48o3yG89h2Ph
3. Alice gives the address (string) to bob so he can make payment to it.
4. Bob opens his digital wallet on his machine, enters his encryption key and instructs the wallet to transfer 5 Litecoins to the address given him by Alice.
5. Bob then has the peer-to-peer client sign the transaction with the private key of the address from where he is transferring the Litecoins.
6. The transaction is broadcast to the peer-to-peer network and is verified and updated to the global ledger of transactions.

7. Alice receives her Litecoins.

As transactions are public, they can be searched using this site http://explorer.litecoin.net/.

Summary

Magnet Forensics has recently incorporated Bitcoin artifacts in their forensic product – Internet Evidence Finder (IEF). This paper will not look at mining. Instead, it is interested in looking for Litecoin artifacts or pointers to where evidence may be lurking when examining cases involving virtual currencies.

Sandvik (2013) looked at forensic artifacts left by Tor on OS X, Linux and Windows 7. The Tor version used was 2.3.25-6. The summary of the paper was to identify artifacts left behind by the installation, use and removal of a Tor package. Sandvik (2013) did not use a browser to install Tor but downloaded the program and installed it.

This paper seeks to investigate this evolving field and conduct research using three scenarios:

Scenario 1 – A user has a Windows 8 laptop, has installed Firefox, with no script add-on and Tor on the laptop. They have browsed for “Utopia” and browsed the site but have not made any purchases. They have browsed various Litecoin currency exchanges.

Scenario 2 – A user has a Windows 7 laptop, has installed the Litecoin application. This then connects on the peer-to-peer platform to assist in currency transactions. The Litecoin setup program is from https://litecoin.org/.

Scenario 3 – A user has used a Windows 7 laptop to buy Litecoins through a Litecoin currency website. The user does not have the peer-to-peer program installed and neither have they used any tool to hide their anonymity.

A record of the dates and times of the actions taken in the above scenarios can be found in (section 2.3). For scenario three a summary of the live trades, (appendix 6.1.7), breakdown of each trade, (appendix 6.1.8 – 6.1.12) and a full email trail (appendix 6.1.13) can be found. For example, when the Litecoins were purchased through a regular browser, there is an audit trail. This will allow forensic tool findings to be confirmed later when it becomes important to validate our tools results.

2. Test Schedule

For validation of the testing there is a record below of the equipment utilised along with the operating system and the scenario it relates to. The methodology covers the approach to setting up the artifacts in preparation for the forensic tool.

The actions taken will assist drawing conclusions from the test results through verification of artifacts and related timestamps.

2.1. Equipment utilised

The following equipment that was used for the analysis is as follows:

Scenario 1 - Clean Windows 8 SP1 Professional 64 bit laptop

Scenario 2 - Used Windows 7 SP1 Professional 64 bit laptop – running Litecoin but not mining

Scenario 3 - Used Windows 7 SP1 Professional 32 bit laptop – having already purchased Litecoins through P2P site https://litecoinlocal.org/.

2.2. Methodology

The methodology was to act as a normal user would do so that artifacts would be created to test the forensic tool. It is difficult to define a normal user as everyone is different. However, by using the three scenarios one would be able to obtain slightly different results.

Scenario 1 – The methodology was to test what results Tor would hide in terms of forensic analysis of a user's behaviour. The user would simply download and install the Tor browser. They would then activate the program and browse for virtual currency websites. Originally it was planned to use the Silk Road website but the site was subsequently taken down by law enforcement. Given the nature of Tor and the obvious interest of law enforcement in its use testing was limited to ensure just basic searches were performed.

Scenario 2 – The original methodology was to have a user who mined virtual currency. However, this was more involved and required greater processing power so the methodology was changed to a user who is partaking in the peer-to-peer network of a virtual currency.

Scenario 3 – Our final user is our most active. One wanted to create the majority of "noise" in terms of forensic artifacts. To do this, real transactions were carried out on genuine sites on the internet. Physical currency was changed into virtual currency. The methodology being that the transactions would be identifiable forensically and allow a forensic investigator to trace transactions made.

2.3. Actions Taken

2.3.1 Scenario 1

2.3.1.1 Scenario 1 – Windows 8 laptop

The date and time were recorded - 5th February 2014 12:09.

Internet Explorer web browser that was part of the original installation of the new machine was opened.

Next, www.duckduckgo.com was entered as the website address in Internet Explorer. This was followed by entering a search for "Tor browser".

The Tor browser version 3.5.1 for Windows was downloaded.

Then, browsing to the downloaded Tor file a default installation is actioned taking all the default steps.

With the Tor browser installed, the following search term was entered: "*Litecoin*".

The website results were listed and "*litecoinrates.com"* was viewed. Time recorded at 12:21.

Next the following search terms were actioned one by one: "*buy Litecoin*", "*buy Litecoin UK*", "*buy Litecoin UK exchange", "Litecoin local*".

Interestingly, when "*litecoinlocal.org*" was next viewed, the default location was set to France. The default location (France) was being picked up from the random Internet Protocol (IP) address which Tor allocated to give anonymity. This is by design and was outside the scope of this paper to warranty further investigation.

The blog "*mainstreamlos.blogspot.de*" was viewed and time recorded at 12:33.

Then the search term "Utopia" was entered and viewed "*http://ggvow6fj3sehlm45.onion*".

Finally at 12:40 the Tor browser was closed.

2.3.1.2 Scenario 1 – Windows 8 laptop – Forensic Capture

The date and time were recorded - 16th March 2014 09:53.

Our forensic tool Internet Evidence Finder Triage runs from a USB stick. This was plugged into this machine. Magnet Forensics product was then run from the USB device and a full capture was actioned. This capture is not a bit by bit disk copy but a low-level sector scan by the tool that then builds its own database file.

2.3.2 Scenario 2

2.3.2.1 Scenario 2 – Windows 7 laptop – running Litecoin program

The date and time were recorded – 6th December 2013 20:01.

Internet Explorer was opened on the machine and a search for "*Litecoin*" was entered from the default Google search page.

Litecoin version 0.8.5.1 was downloaded and installed.

Litecoin was then run on the machine and left running so that it could download the transaction table for the peer-to-peer virtual currency network. Once the transactions had caught up the Litecoin program was closed and the machine was powered off.

The date and time were recorded – 13th January 2014 10:11.

Internet Explorer was opened on the machine and a search for "*Litecoin*" was entered from the default Google search page.

Litecoin version 0.8.6.2 was downloaded and installed. Hashes of this program version were taken and these can be found in Section 6.1.5. Screen dumps were also taken of all the files extracted for this installation and can be found in Section 6.1.4.

Litecoin was then run on the machine and left running so that it could download the transaction table for the peer-to-peer virtual currency network. Once the transactions had caught up the Litecoin program was closed and the machine was powered off.

2.3.2.2 Scenario 2 – Windows 7 laptop – Forensic Capture

The date and time were recorded - 16th March 2014 09:53.

Our forensic tool Internet Evidence Finder Triage runs from a USB stick. This was plugged into this machine. Magnet Forensics product was then run from the USB device and a full capture was actioned. This capture is not a bit-by-bit disk copy but a low-level sector scan by the tool that then builds its own database file.

2.3.3 Scenario 3

2.3.3.1 Scenario 3 – Windows 7 laptop – Purchasing Litecoins

The date was recorded – 6th December 2013.

The internet was browsed to the website litecoinlocal.org.

A purchase was made on litecoinlocal.org.

The date was recorded – 17th December 2013

The internet was browsed to the website litecoinlocal.org.

A purchase was made on litecoinlocal.org.

The date was recorded – 18th December 2013

The internet was browsed to the website litecoinlocal.org.

A purchase was made on litecoinlocal.org

2.3.3.2 Scenario 3 – Windows 7 laptop – Forensic Capture

The date and time were recorded – 4th April 2014 14:27.

Our forensic tool Internet Evidence Finder Triage runs from a USB stick. This was plugged into this machine. Magnet Forensics product was then run from the USB device and a full capture was actioned. This capture is not a bit by bit disk copy but a low-level sector scan by the tool that then builds its own database file.

2.4. Analysis

Now there is a forensic capture for each scenario. This is the evidence and artifacts being sought after from each scenario:

Scenario 1:

Our user downloaded and installed Tor as described in Methodology 3.2. Our search will be looking for web history artifacts relating to Tor.. We are also looking for search terms entered with the Tor browser. We are also looking for any virtual currency artifacts our forensic tool finds on the machine to see if our user has any traces of using virtual currency.

Scenario 2:

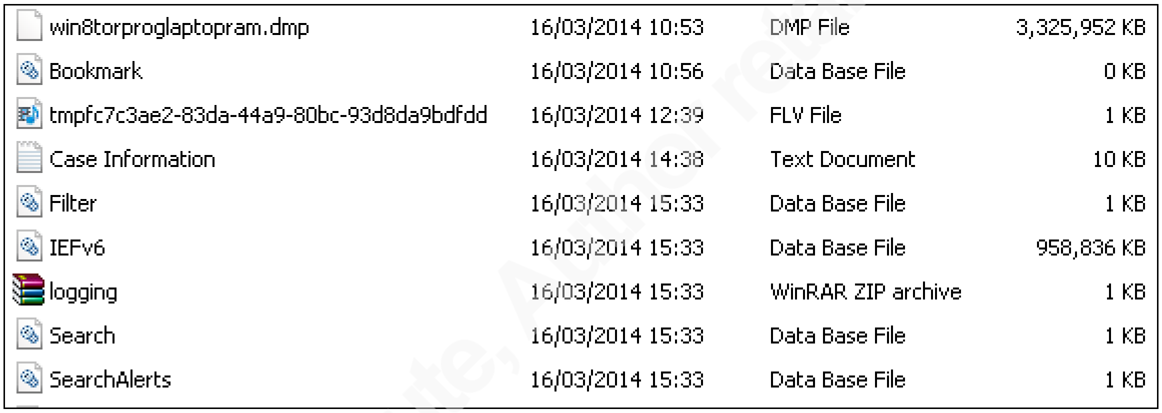
Our user downloaded and installed the Litecoin program as described in Methodology 3.2. We are looking for forensic artifacts that indicate use of a peer-to-peer virtual currency network. Looking for other artifacts such as websites visited in relation to virtual currencies will help differentiate between our third scenario. In our third scenario Litecoins have been purchased but not in this scenario. It will be good to compare.

Scenario 3:

Our user has purchased virtual currency in this scenario as described in Methodology 3.2 Therefore we will be looking for web artifacts, storage of the virtual currency. In particular we will be interested as to how the trades were made, when they were made and perhaps most importantly who with and where the forensic artifacts can be found.

2.4.1. Scenario 1 - Win 8 Laptop Analysis of Capture

Following the actions taken there is now a forensic capture by our forensic tool Internet Evidence Finder (IEF). The log file for this capture can be found in Section 6.1.14. This file simply details the partitions on the disk that were scanned, the options selected for the scan and the artifacts found, broken down by category. It should be noted that false positives exist. Below (event 1) are the files produced on our USB forensic capture which are created by the forensic tool. For completeness of capture for this machine, the memory capture (.dmp) file was manually added.



win8torproglaptopram.dmp	16/03/2014 10:53	DMP File	3,325,952 KB
Bookmark	16/03/2014 10:56	Data Base File	0 KB
tmpfc7c3ae2-83da-44a9-80bc-93d8da9bdfdd	16/03/2014 12:39	FLV File	1 KB
Case Information	16/03/2014 14:38	Text Document	10 KB
Filter	16/03/2014 15:33	Data Base File	1 KB
IEFv6	16/03/2014 15:33	Data Base File	958,836 KB
logging	16/03/2014 15:33	WinRAR ZIP archive	1 KB
Search	16/03/2014 15:33	Data Base File	1 KB
SearchAlerts	16/03/2014 15:33	Data Base File	1 KB

Figure 1 - Files created by IEF Triage (event 1).

Our next step to view the results was to launch the forensic programs report viewer. This was selected as below (event 2) from the standard Windows menu where our program was installed and selecting the IEF Report viewer.

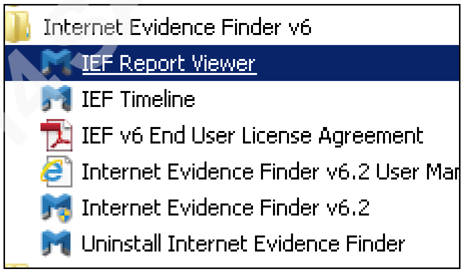

Internet Evidence Finder v6
IEF Report Viewer
IEF Timeline
IEF v6 End User License Agreement
Internet Evidence Finder v6.2 User Mar
Internet Evidence Finder v6.2
Uninstall Internet Evidence Finder

Figure 2 - Running IEF Report Viewer (event 2).

The report viewer as you can see from (event 3) then prompts for the forensic files you wish to examine by asking the user to click "here".

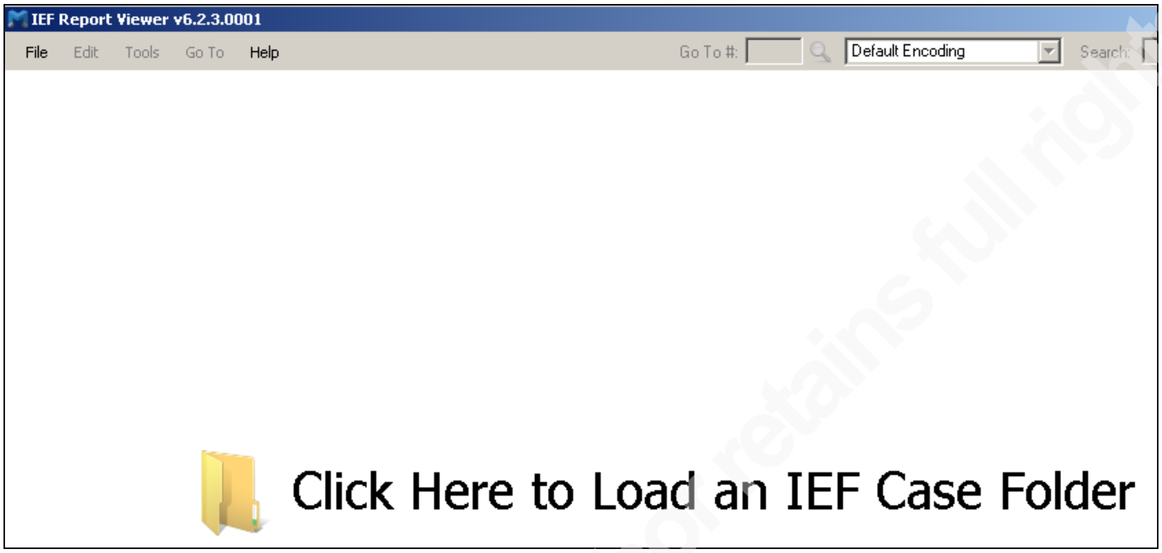

IEF Report Viewer v6.2.3.0001
File
Edit
Tools
Go To
Help
Go To #:
Default Encoding
Search:
Click Here to Load an IEF Case Folder

Figure 3 - Loading the IEF Triage file (event 3).

Next click on the word "here" in (event 3).

This loads the standard Windows interface to browse for files as shown in (event 4).

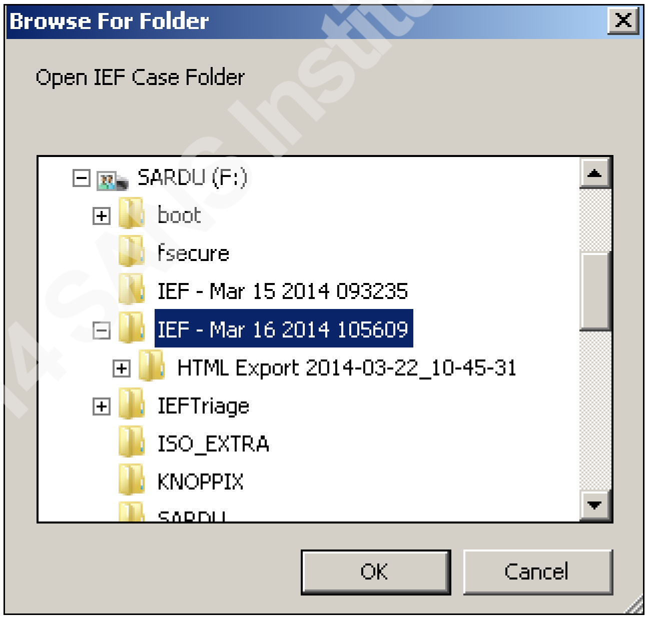
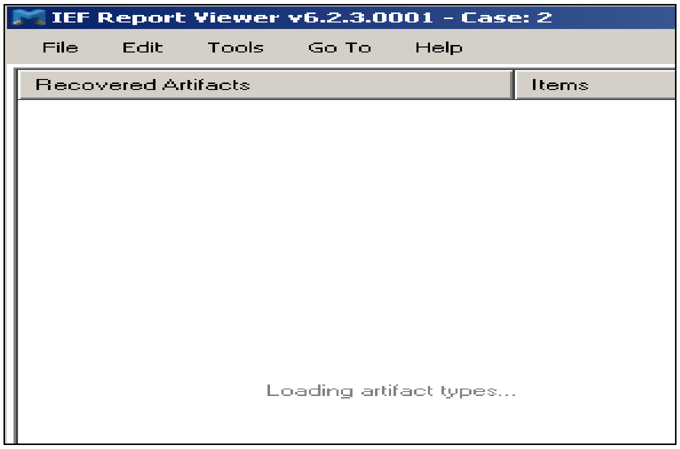


Figure 4 - Navigating to the IEF Triage file source (event 4).

Select our case file from our USB forensic storage dated March 16 and click on ok as in (event 4).

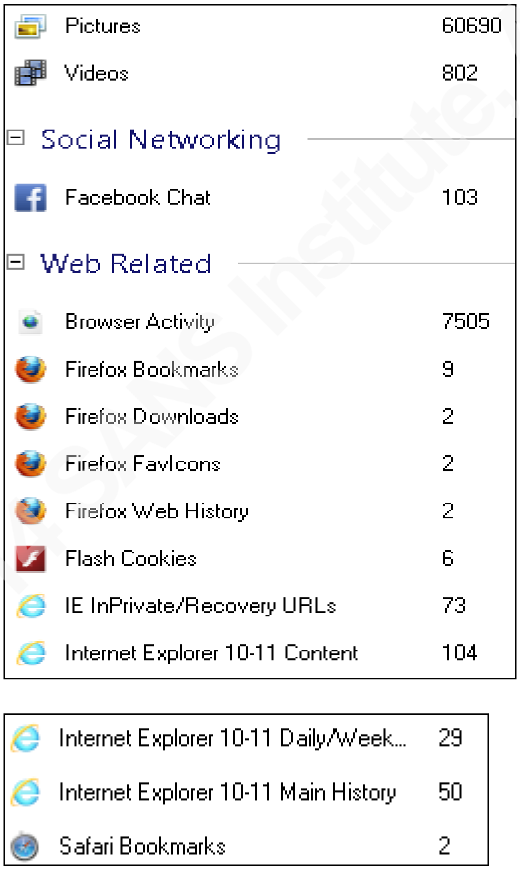
Then wait while the artifacts are loaded (event 5).



Loading artifact types...

Figure 5 - IEF Triage file loading the artifacts from the file source (event 5).

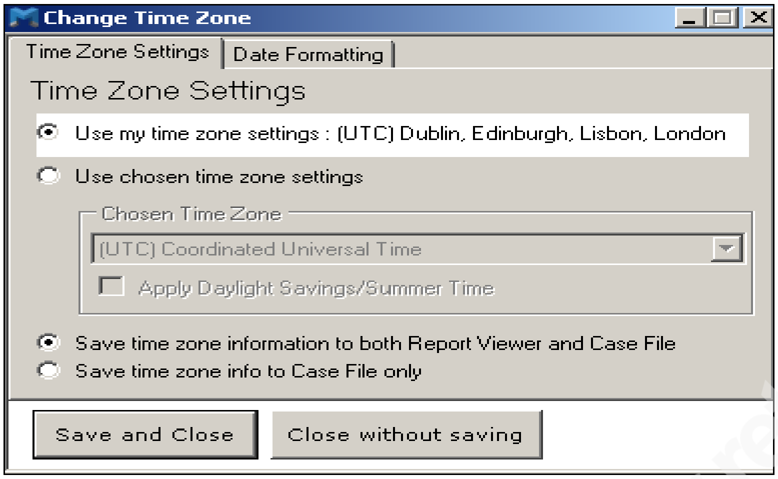
The tool presents a selection of artifacts sorted by this particular forensic tool's assessment heading (event 6).



Pictures	60690
Videos	802
⊟ Social Networking	
Facebook Chat	103
⊟ Web Related	
Browser Activity	7505
Firefox Bookmarks	9
Firefox Downloads	2
Firefox FavIcons	2
Firefox Web History	2
Flash Cookies	6
IE InPrivate/Recovery URLs	73
Internet Explorer 10-11 Content	104
Internet Explorer 10-11 Daily/Week...	29
Internet Explorer 10-11 Main History	50
Safari Bookmarks	2

Figure 6 - IEF Triage file listing of artifacts (event 6).

Next change the time zone to our geographic area where the image was taken from (event 7).:



Change Time Zone

Time Zone Settings | Date Formatting

Time Zone Settings

● Use my time zone settings : (UTC) Dublin, Edinburgh, Lisbon, London

○ Use chosen time zone settings

Chosen Time Zone

(UTC) Coordinated Universal Time

□ Apply Daylight Savings/Summer Time

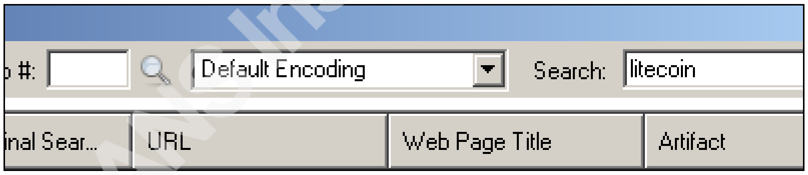
● Save time zone information to both Report Viewer and Case File

○ Save time zone info to Case File only

Figure 7 - Changing IEF Triage Time Zone to match our forensic source (event 7).

Changing the time settings is critical to any forensic examination to ensure timings are accurate.

Now we need to limit the artifacts to our particular investigation of Litecoin. You can limit the number of artifacts shown through the search facility. So a search term of “Litecoin” is entered in the search field (event 8).

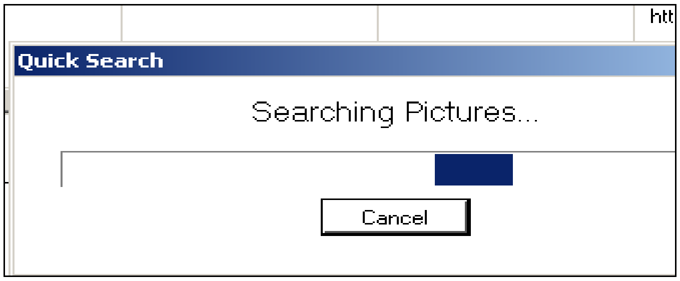


Default Encoding

Search: litecoin

Figure 8 - Searching IEF Triage file (event 8).

IEF then runs a search looking for Litecoin across the artifacts it has found (event 9).



Quick Search

Searching Pictures...

Figure 9 - IEF searching (event 9).

Our search returns no results for the term "Litecoin" (event 10).

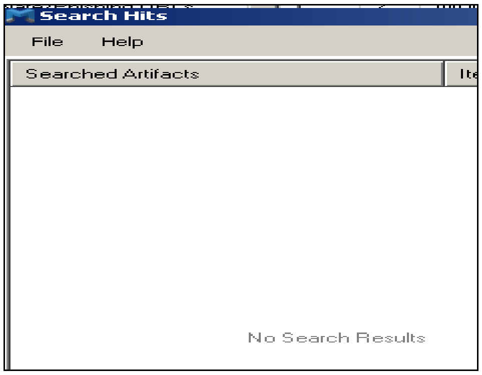


Figure 10 - No results from IEF Triage file search (event 10).

Next, run a timeline (event 11) of the artifacts found (event 2) to try and establish a pattern of use which should reflect our actions taken for Scenario 1.

Figure 11 - Running IEF Triage Timeline (event 11).

The tool then presents the timeline (event 12):

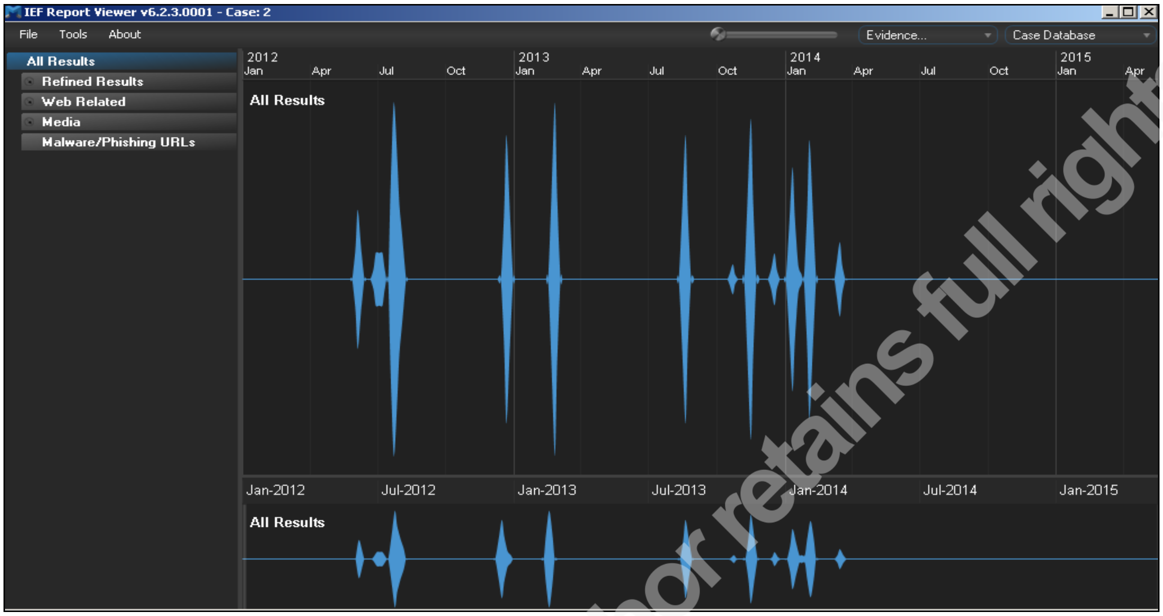
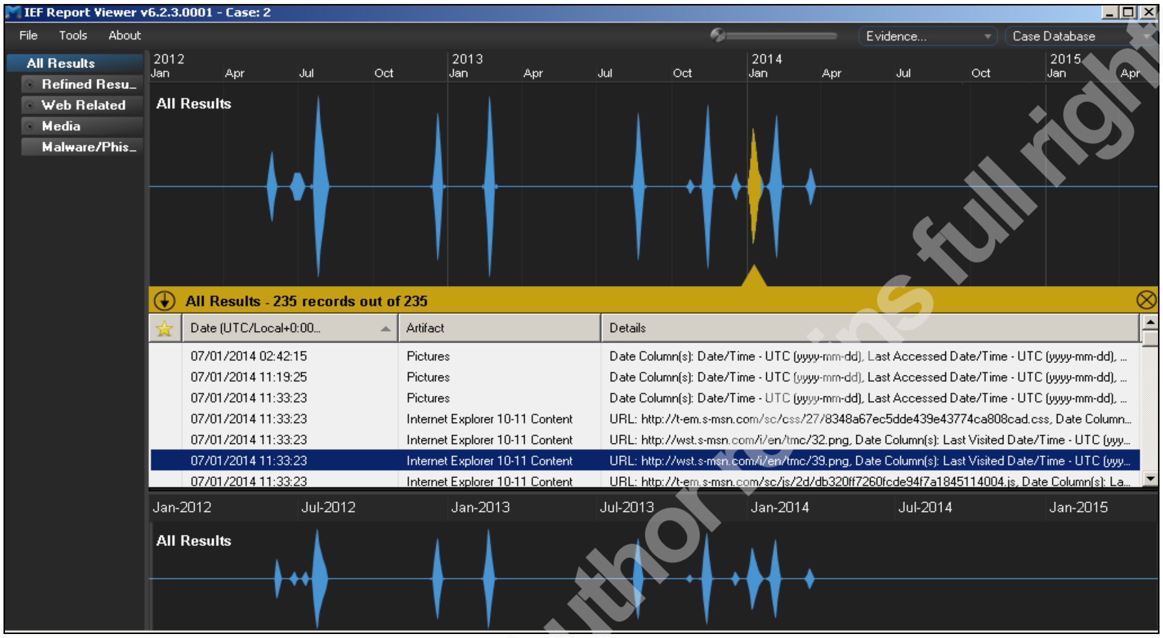


Figure 12 - IEF Triage Timeline file (event 12).

The timeline results look strange (event 12). The machine was purchased around 23 December 2013 but the timeline runs from 1st June 2012 to 16 March 2014?

This paper will not look further at this as there is a specific task to do, but it may warrant further investigation if evidence being sought is not found.

When clicking on a specific area of the timeline, it shows us the artifacts it has found and the period of these events (event 13).



All Results - 235 records out of 235

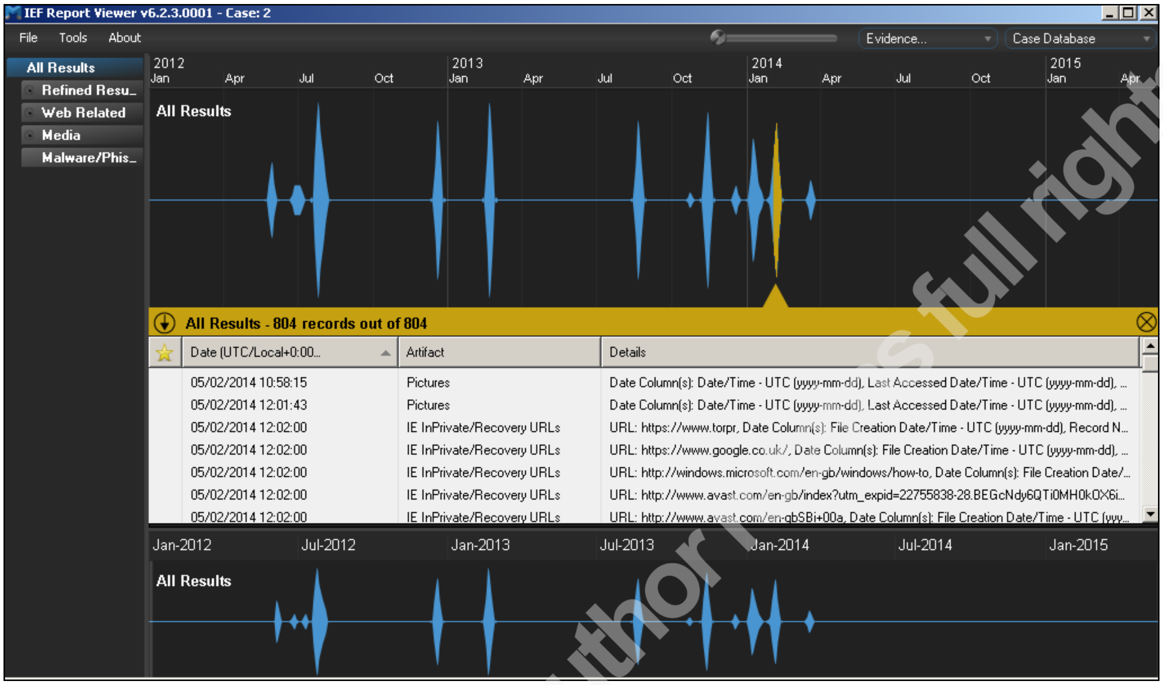
Date (UTC/Local+0:00...	Artifact	Details
07/01/2014 02:42:15	Pictures	Date Column(s): Date/Time - UTC (yyyy-mm-dd), Last Accessed Date/Time - UTC (yyyy-mm-dd), ...
07/01/2014 11:19:25	Pictures	Date Column(s): Date/Time - UTC (yyyy-mm-dd), Last Accessed Date/Time - UTC (yyyy-mm-dd), ...
07/01/2014 11:33:23	Pictures	Date Column(s): Date/Time - UTC (yyyy-mm-dd), Last Accessed Date/Time - UTC (yyyy-mm-dd), ...
07/01/2014 11:33:23	Internet Explorer 10-11 Content	URL: http://t-em.s-msn.com/sc/css/27/8348a67ec5dde439e43774ca808cad.css, Date Column...
07/01/2014 11:33:23	Internet Explorer 10-11 Content	URL: http://wst.s-msn.com/i/en/tmc/32.png, Date Column(s): Last Visited Date/Time - UTC (yyy...
07/01/2014 11:33:23	Internet Explorer 10-11 Content	URL: http://wst.s-msn.com/i/en/tmc/39.png, Date Column(s): Last Visited Date/Time - UTC (yyy...
07/01/2014 11:33:23	Internet Explorer 10-11 Content	URL: http://t-em.s-msn.com/sc/js/2d/db320ff7260fcde94f7a1845114004.js, Date Column(s): La...

Figure 13 - Viewing correlated artifacts on the IEF Timeline (event 13).

In the example above there are 235 events with the majority on the 7 January 2014 but two on the 13 January 2014 (event 13).

The next largest group of artifacts moving forwards in time is represented by the tool with a large blue indicator.

Click on it to see a snapshot of the artifacts it represents (event 14).

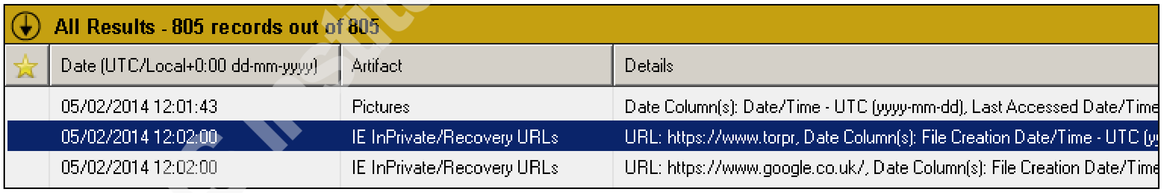


All Results - 804 records out of 804

☆	Date (UTC/Local+0:00...	Artifact	Details
	05/02/2014 10:58:15	Pictures	Date Column(s): Date/Time - UTC (yyyy-mm-dd), Last Accessed Date/Time - UTC (yyyy-mm-dd), ...
	05/02/2014 12:01:43	Pictures	Date Column(s): Date/Time - UTC (yyyy-mm-dd), Last Accessed Date/Time - UTC (yyyy-mm-dd), ...
	05/02/2014 12:02:00	IE InPrivate/Recovery URLs	URL: https://www.torpr, Date Column(s): File Creation Date/Time - UTC (yyyy-mm-dd), Record N...
	05/02/2014 12:02:00	IE InPrivate/Recovery URLs	URL: https://www.google.co.uk/, Date Column(s): File Creation Date/Time - UTC (yyyy-mm-dd), ...
	05/02/2014 12:02:00	IE InPrivate/Recovery URLs	URL: http://windows.microsoft.com/en-gb/windows/how-to, Date Column(s): File Creation Date/...
	05/02/2014 12:02:00	IE InPrivate/Recovery URLs	URL: http://www.avast.com/en-gb/index?utm_expid=22755838-28.BEGcNdy6QTi0MH0kOX6i...
	05/02/2014 12:02:00	IE InPrivate/Recovery URLs	URL: http://www.avast.com/en-gbSBi+00a, Date Column(s): File Creation Date/Time - UTC (yyy...

Figure 14 - Viewing correlated artifacts on the IEF Timeline from our actions (event 14).

There are 804 artifacts in the timeline period above (event 14).

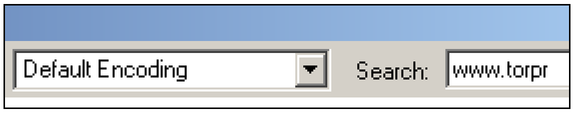


All Results - 805 records out of 805

☆	Date (UTC/Local+0:00 dd-mm-yyyy)	Artifact	Details
	05/02/2014 12:01:43	Pictures	Date Column(s): Date/Time - UTC (yyyy-mm-dd), Last Accessed Date/Time
	05/02/2014 12:02:00	IE InPrivate/Recovery URLs	URL: https://www.torpr, Date Column(s): File Creation Date/Time - UTC (yy
	05/02/2014 12:02:00	IE InPrivate/Recovery URLs	URL: https://www.google.co.uk/, Date Column(s): File Creation Date/Time

Figure 15 - Viewing Tor artifacts on the IEF Timeline from our actions (event 15).

In the timeline (event 15) one can see the first possible reference to Tor use on the machine. To validate this, a search for www.torpr is entered back on the main IEF screen (event 16).

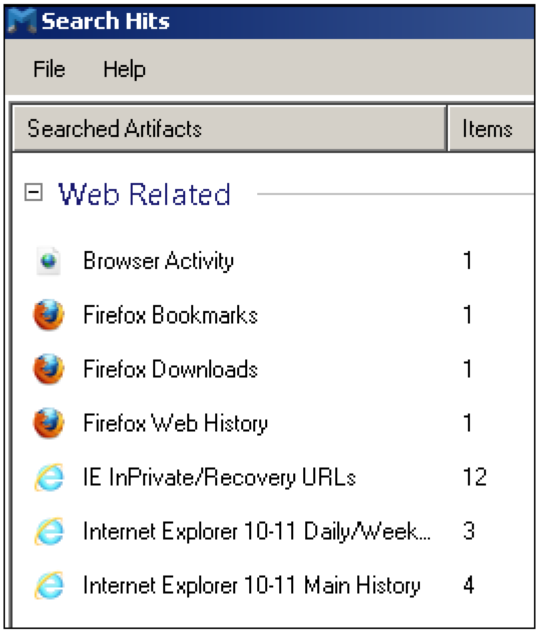


Default Encoding ▾ Search: www.torpr

Figure 16 - Searching for Tor artifacts (event 16).

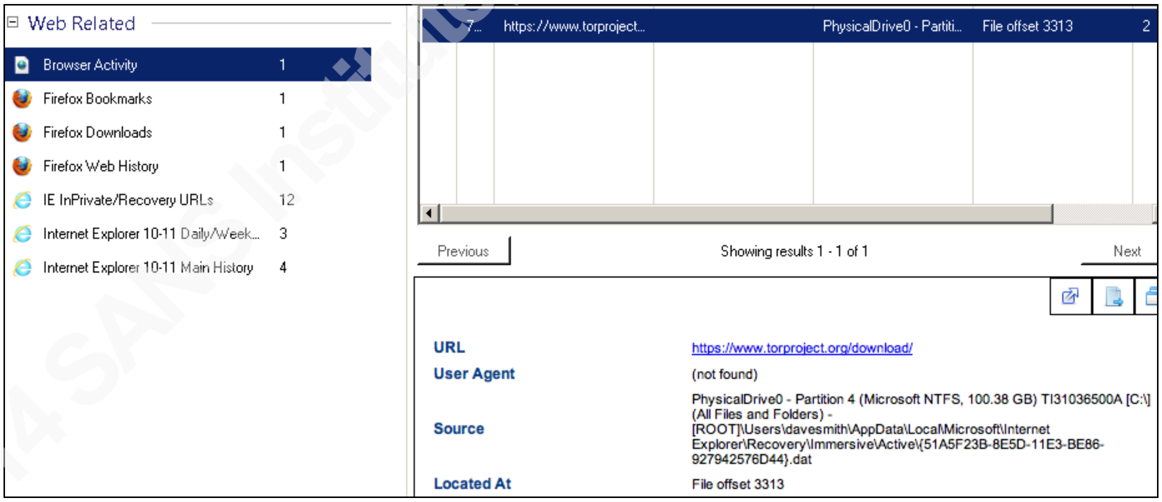
Daniel Piggott, Piggott.daniel@gmail.com

When the search is complete, IEF presents a list of 23 hits in our artifacts that can be investigated further (event 17).



Searched Artifacts	Items
Web Related	
Browser Activity	1
Firefox Bookmarks	1
Firefox Downloads	1
Firefox Web History	1
IE InPrivate/Recovery URLs	12
Internet Explorer 10-11 Daily/Week...	3
Internet Explorer 10-11 Main History	4

Figure 17 - Hits found from a search for Tor (event 17).



Web Related	
Browser Activity	1
Firefox Bookmarks	1
Firefox Downloads	1
Firefox Web History	1
IE InPrivate/Recovery URLs	12
Internet Explorer 10-11 Daily/Week...	3
Internet Explorer 10-11 Main History	4

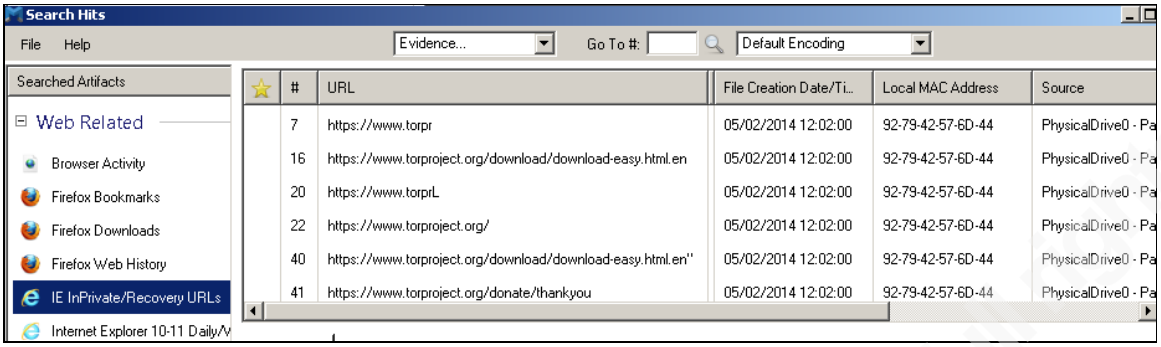
7...	https://www.torproject...	PhysicalDrive0 - Partiti...	File offset 3313	2

URL https://www.torproject.org/download/
User Agent (not found)
Source PhysicalDrive0 - Partition 4 (Microsoft NTFS, 100.38 GB) TI31036500A [C:\] (All Files and Folders) - [ROOT]\Users\davesmith\AppData\Local\Microsoft\Internet Explorer\Recovery\Immersive\Active\{51A5F23B-8E5D-11E3-BE86-927942576D44}.dat
Located At File offset 3313

Figure 18 - First hit confirms an Internet Explorer artifact for the URL (event 18).

Clicking on the first artifact in the list "Browser Action", you now see a URL for the TOR download (https://www.torproject.org/download/) (event 18).

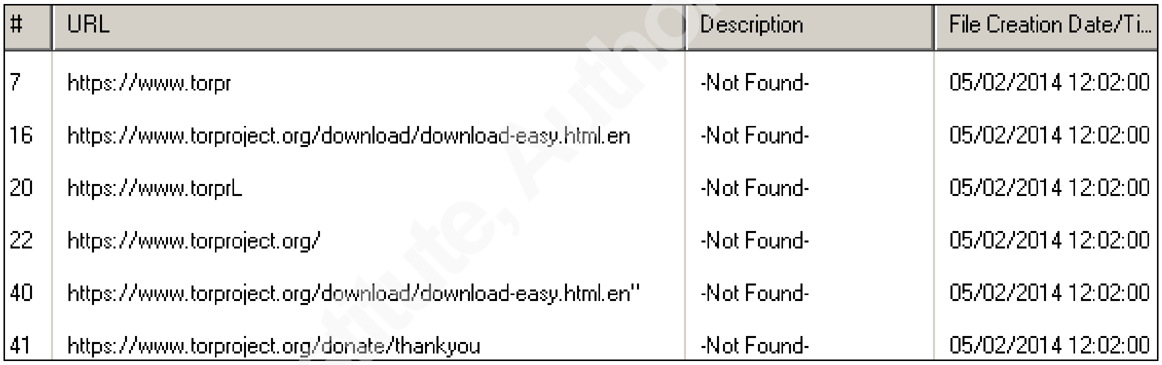
Also we have a user profile from our Windows machine – Dave Smith. (Event 18)



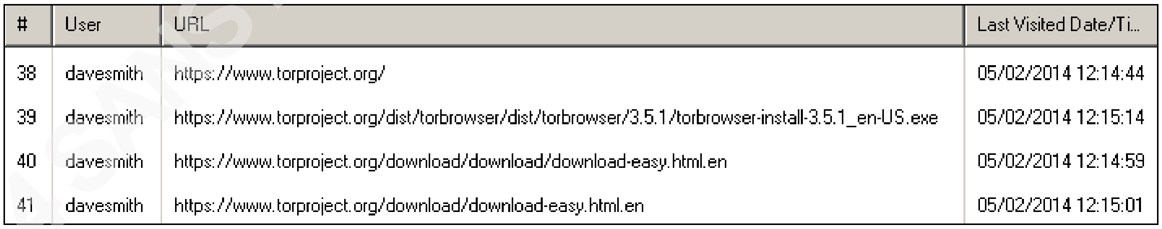
#	URL	File Creation Date/Ti...	Local MAC Address	Source
7	https://www.torpr	05/02/2014 12:02:00	92-79-42-57-6D-44	PhysicalDrive0 - Pa
16	https://www.torproject.org/download/download-easy.html.en	05/02/2014 12:02:00	92-79-42-57-6D-44	PhysicalDrive0 - Pa
20	https://www.torprL	05/02/2014 12:02:00	92-79-42-57-6D-44	PhysicalDrive0 - Pa
22	https://www.torproject.org/	05/02/2014 12:02:00	92-79-42-57-6D-44	PhysicalDrive0 - Pa
40	https://www.torproject.org/download/download-easy.html.en"	05/02/2014 12:02:00	92-79-42-57-6D-44	PhysicalDrive0 - Pa
41	https://www.torproject.org/donate/thankyou	05/02/2014 12:02:00	92-79-42-57-6D-44	PhysicalDrive0 - Pa

Figure 19 - Further hits confirming Internet Explorer artifacts for Tor (event 19).

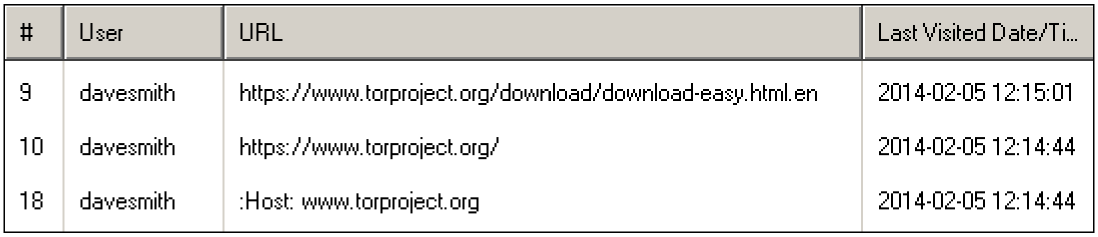
Using the menu on the left hand side you can browse the different artifacts found (event 19). The forensic tool adds a sequence number to the overall list of artifacts. These can be viewed, particularly our Tor artifacts, in time order (event 20).



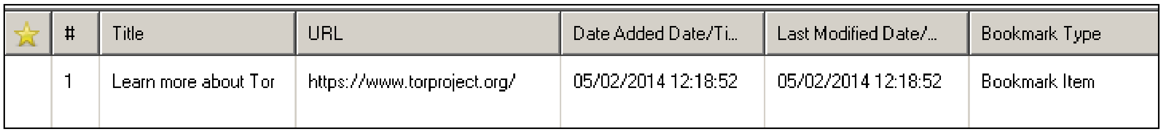
#	URL	Description	File Creation Date/Ti...
7	https://www.torpr	-Not Found-	05/02/2014 12:02:00
16	https://www.torproject.org/download/download-easy.html.en	-Not Found-	05/02/2014 12:02:00
20	https://www.torprL	-Not Found-	05/02/2014 12:02:00
22	https://www.torproject.org/	-Not Found-	05/02/2014 12:02:00
40	https://www.torproject.org/download/download-easy.html.en"	-Not Found-	05/02/2014 12:02:00
41	https://www.torproject.org/donate/thankyou	-Not Found-	05/02/2014 12:02:00



#	User	URL	Last Visited Date/Ti...
38	davesmith	https://www.torproject.org/	05/02/2014 12:14:44
39	davesmith	https://www.torproject.org/dist/torbrowser/dist/torbrowser/3.5.1/torbrowser-install-3.5.1_en-US.exe	05/02/2014 12:15:14
40	davesmith	https://www.torproject.org/download/download/download-easy.html.en	05/02/2014 12:14:59
41	davesmith	https://www.torproject.org/download/download-easy.html.en	05/02/2014 12:15:01



#	User	URL	Last Visited Date/Ti...
9	davesmith	https://www.torproject.org/download/download-easy.html.en	2014-02-05 12:15:01
10	davesmith	https://www.torproject.org/	2014-02-05 12:14:44
18	davesmith	:Host: www.torproject.org	2014-02-05 12:14:44



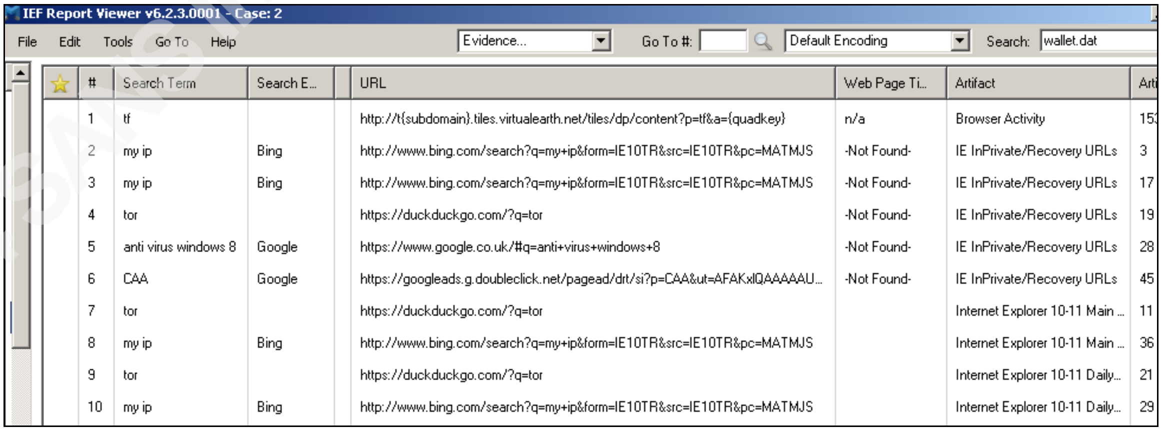
★	#	Title	URL	Date Added Date/Ti...	Last Modified Date/...	Bookmark Type
	1	Learn more about Tor	https://www.torproject.org/	05/02/2014 12:18:52	05/02/2014 12:18:52	Bookmark Item

Figure 20 - Tor related artifacts in time order (event 20).

The timeline (event 14) so far shows us related activity between 5/2/14 12:01:43 and 5/2/14 12:40:25.

In Scenario 1 search terms were entered into the Tor web browser in an attempt to create artifacts. These search terms were then entered in our forensic tool to search for artifacts (event 21):

- Litecoin
- Buy
- UK
- Exchange
- Local
- Mainstreamlos.blogspot.de
- http://ggvow6fj3sehlm45.onion



★	#	Search Term	Search E...	URL	Web Page Ti...	Artifact	Arti
	1	tf		http://t{subdomain}.tiles.virtualearth.net/tiles/dp/content?p=tf&a={quadkey}	n/a	Browser Activity	153
	2	my ip	Bing	http://www.bing.com/search?q=my+ip&form=IE10TR&src=IE10TR&pc=MATMJS	-Not Found-	IE InPrivate/Recovery URLs	3
	3	my ip	Bing	http://www.bing.com/search?q=my+ip&form=IE10TR&src=IE10TR&pc=MATMJS	-Not Found-	IE InPrivate/Recovery URLs	17
	4	tor		https://duckduckgo.com/?q=tor	-Not Found-	IE InPrivate/Recovery URLs	19
	5	anti virus windows 8	Google	https://www.google.co.uk/#q=anti+virus+windows+8	-Not Found-	IE InPrivate/Recovery URLs	28
	6	CAA	Google	https://googleads.g.doubleclick.net/pagead/drt/si?p=CAA&ut=AFAKxlQAAAAAU...	-Not Found-	IE InPrivate/Recovery URLs	45
	7	tor		https://duckduckgo.com/?q=tor		Internet Explorer 10-11 Main ...	11
	8	my ip	Bing	http://www.bing.com/search?q=my+ip&form=IE10TR&src=IE10TR&pc=MATMJS		Internet Explorer 10-11 Main ...	36
	9	tor		https://duckduckgo.com/?q=tor		Internet Explorer 10-11 Daily...	21
	10	my ip	Bing	http://www.bing.com/search?q=my+ip&form=IE10TR&src=IE10TR&pc=MATMJS		Internet Explorer 10-11 Daily...	29

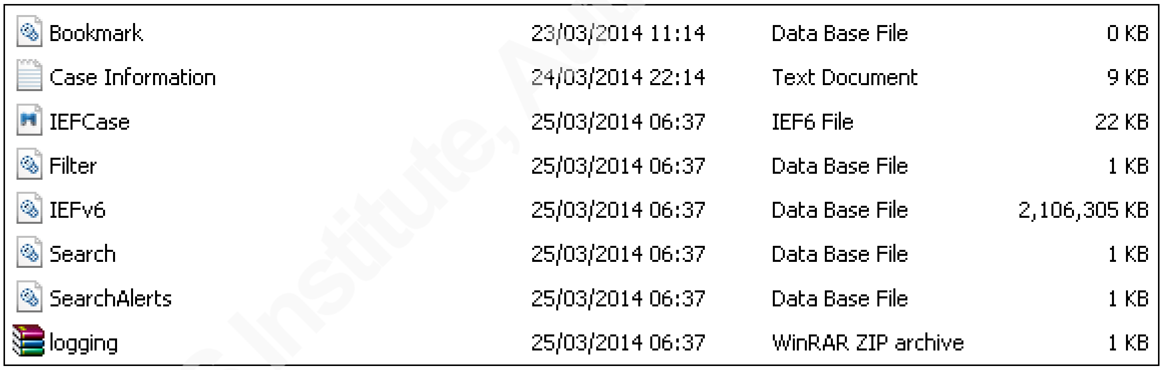
Figure 21 - Search query validation of actions taken (event 21).

All our test searches return a negative response and show no artifacts. Finally a search for *wallet.dat* is entered as we are looking for virtual currency activity on this machine. This also returns a negative response and shows no artifacts found.

2.4.2. Scenario 2 - Win 7 Laptop (running Litecoin) Analysis of Capture

Following our actions taken we now have a forensic capture by our forensic tool Internet Evidence Finder (IEF). The log file for this capture can be found in Section 6.1.15. This file simply details the partitions on the disk that were scanned, the options selected for the scan and the artifacts found, broken down by category. It should be noted that false positives exist. Below (event 1) are the files produced on our USB forensic capture which are created by the forensic. For completeness of capture for this machine, the memory capture (.dmp) file was added manually.

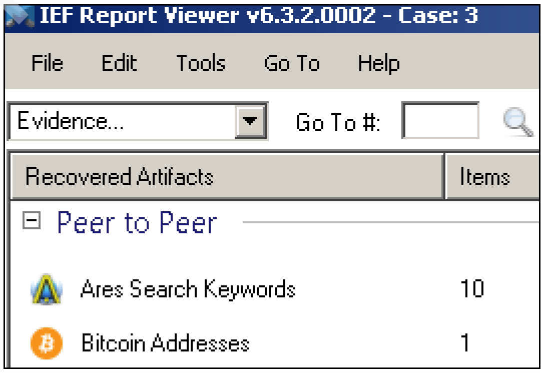
After IEF Triage has completed these are the capture files (event 22):



Bookmark	23/03/2014 11:14	Data Base File	0 KB
Case Information	24/03/2014 22:14	Text Document	9 KB
IEFCase	25/03/2014 06:37	IEF6 File	22 KB
Filter	25/03/2014 06:37	Data Base File	1 KB
IEFv6	25/03/2014 06:37	Data Base File	2,106,305 KB
Search	25/03/2014 06:37	Data Base File	1 KB
SearchAlerts	25/03/2014 06:37	Data Base File	1 KB
logging	25/03/2014 06:37	WinRAR ZIP archive	1 KB

Figure 22 - Files created by IEF Triage (event 22).

The report viewer is then run (event 2) and the case folder loaded (event 3) above (event 22) is selected. IEF then loads the artifacts (event 6).



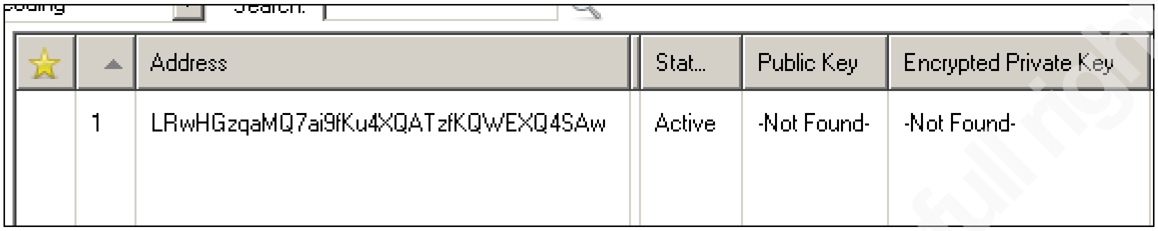
IEF Report Viewer v6.3.2.0002 - Case: 3

Recovered Artifacts	Items
⊟ Peer to Peer	
Ares Search Keywords	10
Bitcoin Addresses	1

Daniel Piggott, Piggott.daniel@gmail.com

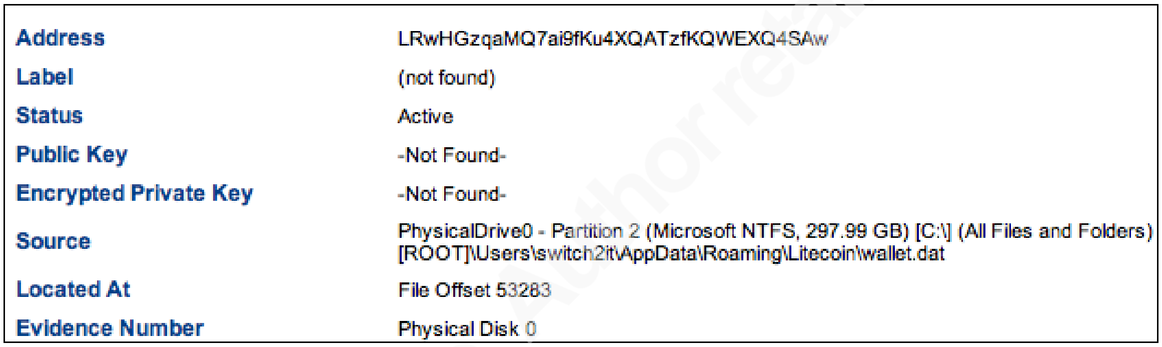
Figure 23 - Bitcoin artifact hit (event 23).

IEF has found what it thinks is a Bitcoin artifact (event 23).



☆	▲	Address	Stat...	Public Key	Encrypted Private Key
	1	LRwHGzqaMQ7ai9fKu4XQATzfKQWEXQ4SAw	Active	-Not Found-	-Not Found-

Figure 24 - Bitcoin artifact hit (event 24).

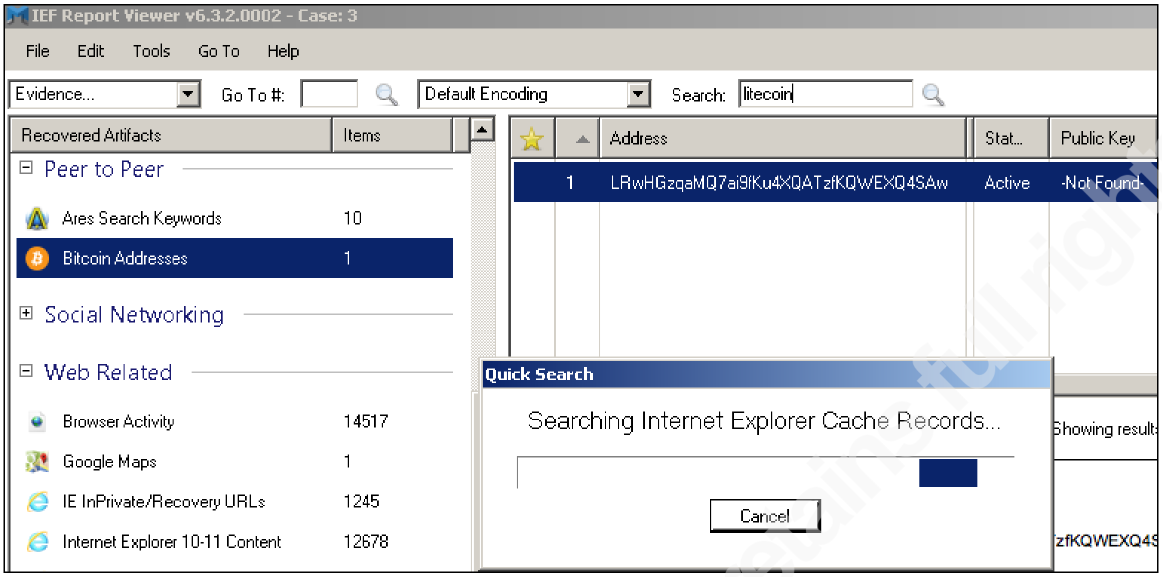


Address	LRwHGzqaMQ7ai9fKu4XQATzfKQWEXQ4SAw
Label	(not found)
Status	Active
Public Key	-Not Found-
Encrypted Private Key	-Not Found-
Source	PhysicalDrive0 - Partition 2 (Microsoft NTFS, 297.99 GB) [C:\] (All Files and Folders) [ROOT]\Users\switch2it\AppData\Roaming\Litecoin\wallet.dat
Located At	File Offset 53283
Evidence Number	Physical Disk 0

Figure 25 - Bitcoin artifact hit (event 25).

IEF has located one virtual currency Litecoin artifact (event 24,25). This is the *wallet.dat* file commonly associated with peer-to-peer currencies.

Next doing a search of “Litecoin” across all the artifacts IEF has found on our disk (event 26).



IEF Report Viewer v6.3.2.0002 - Case: 3

Evidence... Go To #: Default Encoding Search: litecoin

Recovered Artifacts	Items
Peer to Peer	
Ares Search Keywords	10
Bitcoin Addresses	1
Social Networking	
Web Related	
Browser Activity	14517
Google Maps	1
IE InPrivate/Recovery URLs	1245
Internet Explorer 10-11 Content	12678

	Address	Stat...	Public Key
1	LRwHGzqaMQ7ai9fKu4XQATzfKQWEXQ4SAw	Active	-Not Found-

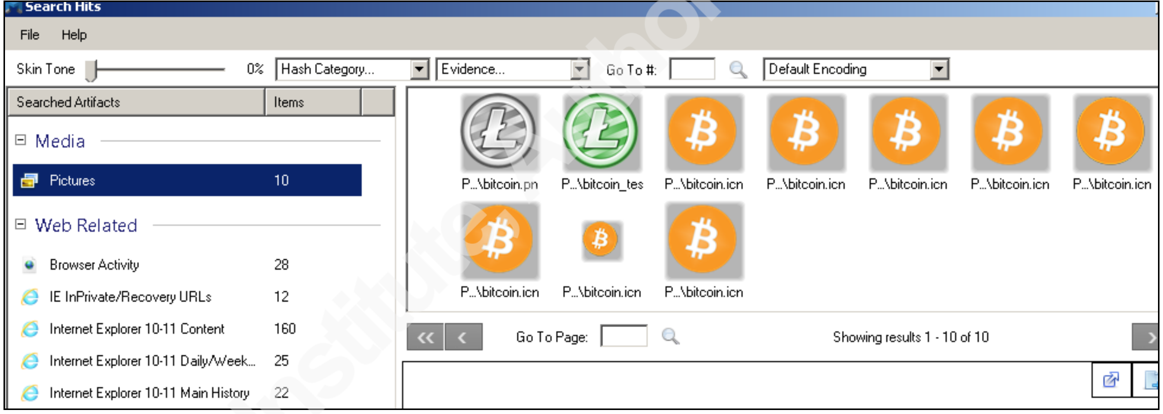
Quick Search

Searching Internet Explorer Cache Records...

Showing result

zfKQWEXQ4S

Figure 26 - Search for Litecoin artifacts (event 26).



Search Hits

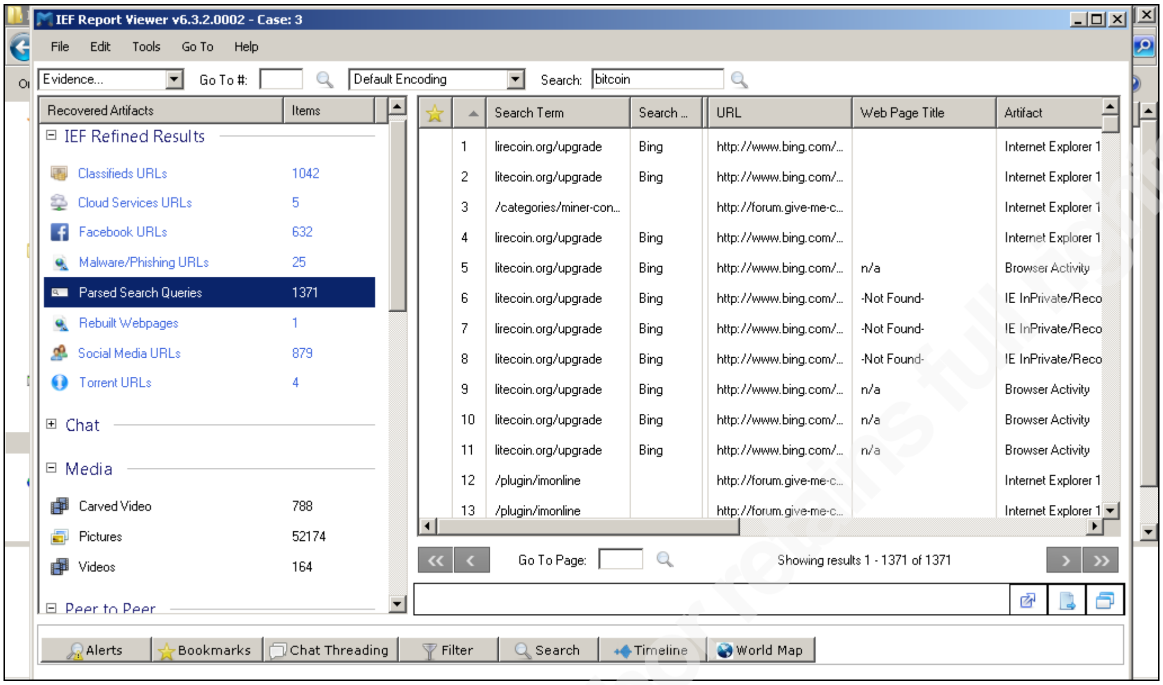
Skin Tone 0% Hash Category... Evidence... Go To #: Default Encoding

Searched Artifacts	Items
Media	
Pictures	10
Web Related	
Browser Activity	28
IE InPrivate/Recovery URLs	12
Internet Explorer 10-11 Content	160
Internet Explorer 10-11 Daily/Week...	25
Internet Explorer 10-11 Main History	22

P...\bitcoin.pn P...\bitcoin_tes P...\bitcoin.icn P...\bitcoin.icn P...\bitcoin.icn P...\bitcoin.icn P...\bitcoin.icn P...\bitcoin.icn P...\bitcoin.icn P...\bitcoin.icn

Go To Page: Showing results 1 - 10 of 10

Figure 27 - Results of a Bitcoin search parameter in IEF (event 27).



Search: bitcoin

Recovered Artifacts	Items
⊟ IEF Refined Results	
Classifieds URLs	1042
Cloud Services URLs	5
Facebook URLs	632
Malware/Phishing URLs	25
Parsed Search Queries	1371
Rebuilt Webpages	1
Social Media URLs	879
Torrent URLs	4
⊞ Chat	
⊟ Media	
Carved Video	788
Pictures	52174
Videos	164
⊟ Peer to Peer	

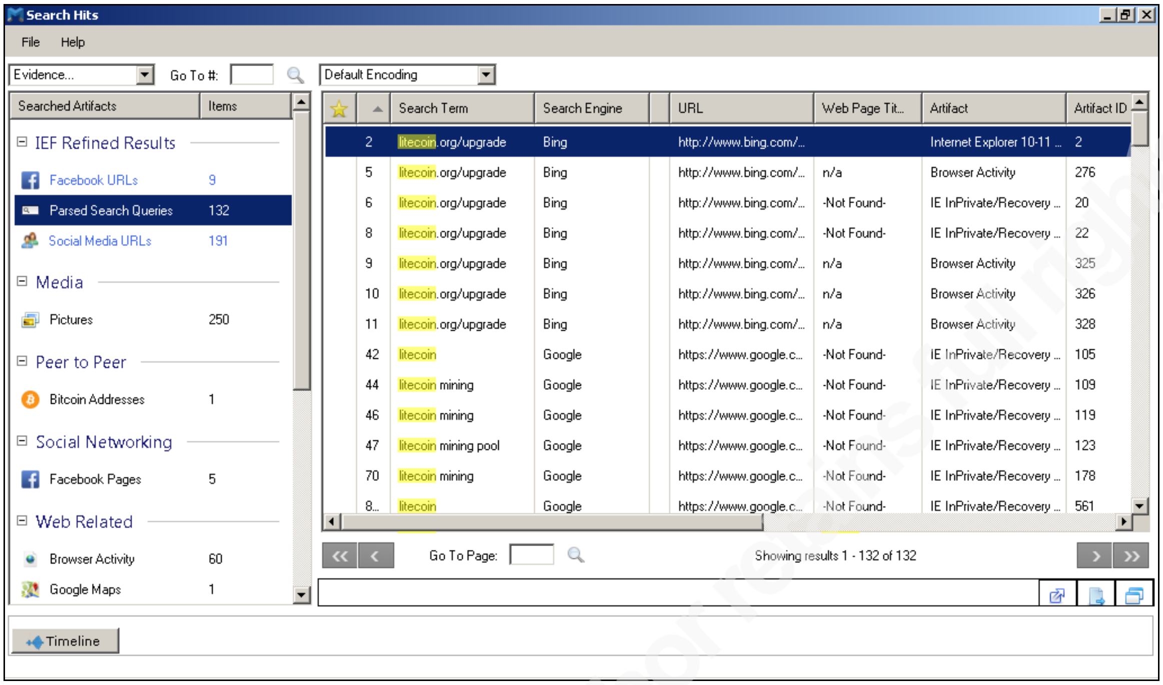
	Search Term	Search ...	URL	Web Page Title	Artifact
1	lirecoin.org/upgrade	Bing	http://www.bing.com/...		Internet Explorer 1
2	litecoin.org/upgrade	Bing	http://www.bing.com/...		Internet Explorer 1
3	/categories/miner-con...		http://forum.give-me-c...		Internet Explorer 1
4	lirecoin.org/upgrade	Bing	http://www.bing.com/...		Internet Explorer 1
5	litecoin.org/upgrade	Bing	http://www.bing.com/...	n/a	Browser Activity
6	litecoin.org/upgrade	Bing	http://www.bing.com/...	-Not Found-	IE InPrivate/Reco
7	lirecoin.org/upgrade	Bing	http://www.bing.com/...	-Not Found-	IE InPrivate/Reco
8	litecoin.org/upgrade	Bing	http://www.bing.com/...	-Not Found-	IE InPrivate/Reco
9	litecoin.org/upgrade	Bing	http://www.bing.com/...	n/a	Browser Activity
10	litecoin.org/upgrade	Bing	http://www.bing.com/...	n/a	Browser Activity
11	litecoin.org/upgrade	Bing	http://www.bing.com/...	n/a	Browser Activity
12	/plugin/imonline		http://forum.give-me-c...		Internet Explorer 1
13	/plugin/imonline		http://forum.give-me-c...		Internet Explorer 1

Go To Page:

Showing results 1 - 1371 of 1371

Figure 28 - Results of a Bitcoin search parameter in IEF (event 28).

We can see from entering Bitcoin as a search parameter that the forensic tool still gives us other virtual currency artifacts (event27/28). The Litecoin and Bitcoin images could suggest a peer-to-peer currency program has been installed at some point (event 27). Furthermore, we can see "Litecoin.org/upgrade" URL entries suggesting a user has been looking at the upgrade page for the Litecoin client on the Litecoin website www.litecoin.org (event 28).



Searched Artifacts	Items
IEF Refined Results	
Facebook URLs	9
Parsed Search Queries	132
Social Media URLs	191
Media	
Pictures	250
Peer to Peer	
Bitcoin Addresses	1
Social Networking	
Facebook Pages	5
Web Related	
Browser Activity	60
Google Maps	1

	Search Term	Search Engine	URL	Web Page Tit...	Artifact	Artifact ID
2	litecoin.org/upgrade	Bing	http://www.bing.com/...		Internet Explorer 10-11 ...	2
5	litecoin.org/upgrade	Bing	http://www.bing.com/...	n/a	Browser Activity	276
6	litecoin.org/upgrade	Bing	http://www.bing.com/...	-Not Found-	IE InPrivate/Recovery ...	20
8	litecoin.org/upgrade	Bing	http://www.bing.com/...	-Not Found-	IE InPrivate/Recovery ...	22
9	litecoin.org/upgrade	Bing	http://www.bing.com/...	n/a	Browser Activity	325
10	litecoin.org/upgrade	Bing	http://www.bing.com/...	n/a	Browser Activity	326
11	litecoin.org/upgrade	Bing	http://www.bing.com/...	n/a	Browser Activity	328
42	litecoin	Google	https://www.google.c...	-Not Found-	IE InPrivate/Recovery ...	105
44	litecoin mining	Google	https://www.google.c...	-Not Found-	IE InPrivate/Recovery ...	109
46	litecoin mining	Google	https://www.google.c...	-Not Found-	IE InPrivate/Recovery ...	119
47	litecoin mining pool	Google	https://www.google.c...	-Not Found-	IE InPrivate/Recovery ...	123
70	litecoin mining	Google	https://www.google.c...	-Not Found-	IE InPrivate/Recovery ...	178
8...	litecoin	Google	https://www.google.c...	-Not Found-	IE InPrivate/Recovery ...	561

Showing results 1 - 132 of 132

Figure 29 - Results of a Litecoin search parameter in IEF (event 29).

Looking at the search queries that have been entered one can see artifacts found by , the forensic tool. These entries have been entered into Internet Explorer. One can identify *"Litecoin", "Litecoin mining", Litecoin mining pool"*. (Event 29).

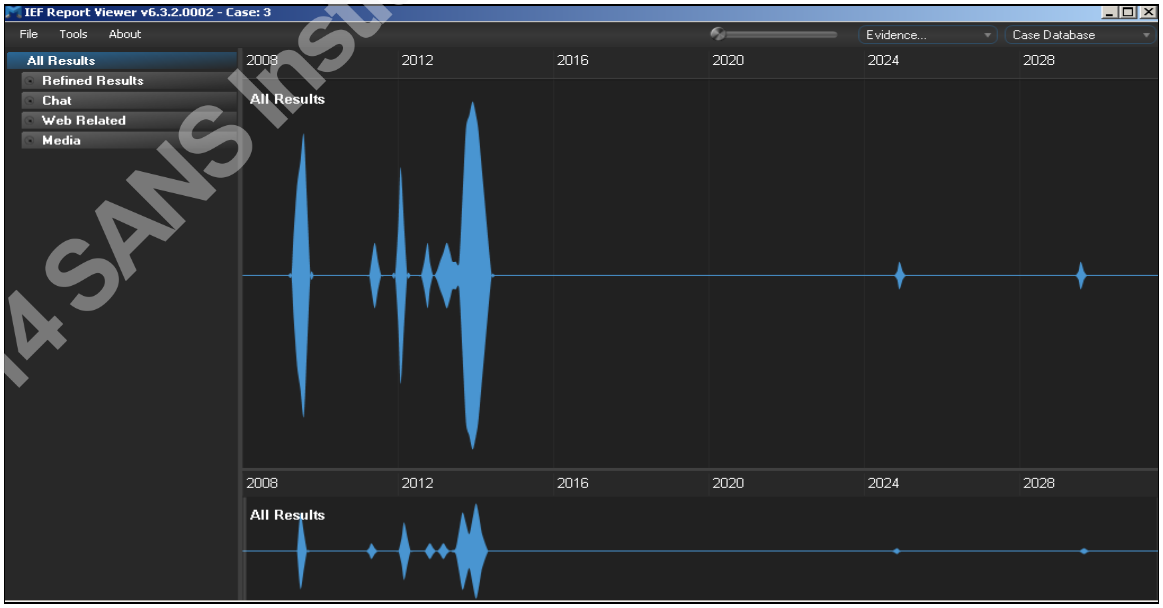


Figure 30 - Results of Timeline for this machine (event 30).

The timeline shows the testing activity with a large blue oval on this machine (event 30):

Daniel Piggott, Piggott.daniel@gmail.com

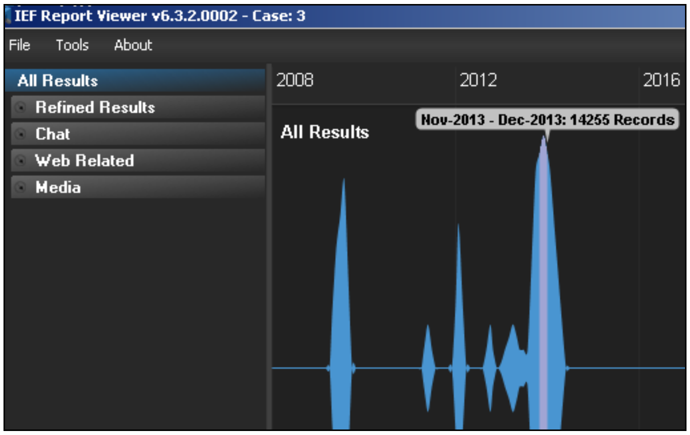


Figure 31 - Results of Timeline records for this machine (event 31).

Comparing our actions taken: Scenario 2 on the 6th December 2013 (event 31).

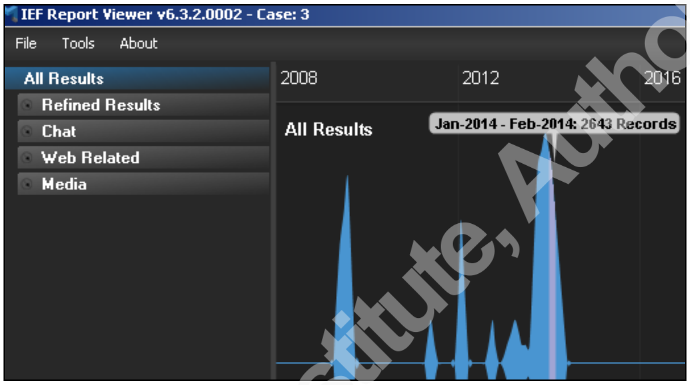
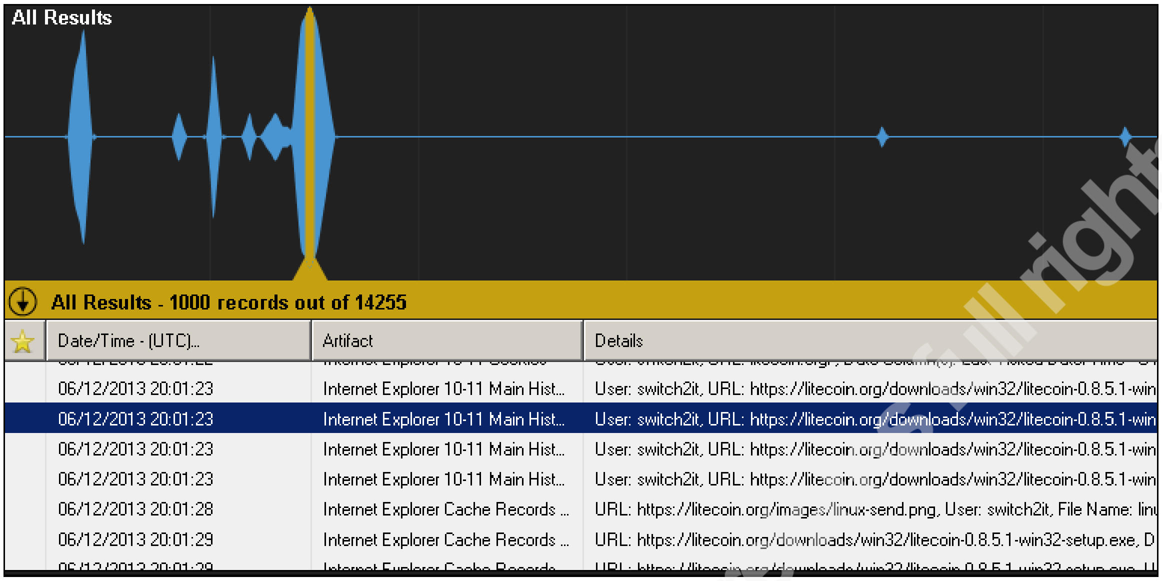


Figure 32 - Results of Timeline records for this machine (event 32).

Then comparing our actions taken: Scenario 2 on the 13th January (event 32).

Our testing activity was actioned on the 6th December 2013 and 13 January 2014. Our timeline is consistent in that it shows many artifacts around this period. Now to investigate the detail.



All Results - 1000 records out of 14255

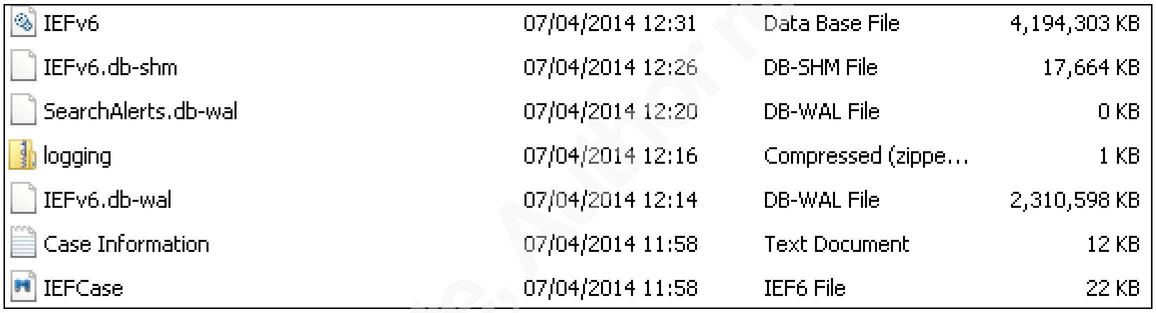
☆	Date/Time - (UTC)...	Artifact	Details
	06/12/2013 20:01:23	Internet Explorer 10-11 Main Hist...	User: switch2it, URL: https://litecoin.org/downloads/win32/litecoin-0.8.5.1-win
	06/12/2013 20:01:23	Internet Explorer 10-11 Main Hist...	User: switch2it, URL: https://litecoin.org/downloads/win32/litecoin-0.8.5.1-win
	06/12/2013 20:01:23	Internet Explorer 10-11 Main Hist...	User: switch2it, URL: https://litecoin.org/downloads/win32/litecoin-0.8.5.1-win
	06/12/2013 20:01:23	Internet Explorer 10-11 Main Hist...	User: switch2it, URL: https://litecoin.org/downloads/win32/litecoin-0.8.5.1-win
	06/12/2013 20:01:28	Internet Explorer Cache Records ...	URL: https://litecoin.org/images/linux-send.png, User: switch2it, File Name: lin
	06/12/2013 20:01:29	Internet Explorer Cache Records ...	URL: https://litecoin.org/downloads/win32/litecoin-0.8.5.1-win32-setup.exe, D
	06/12/2013 20:01:29	Internet Explorer Cache Records ...	URL: https://litecoin.org/downloads/win32/litecoin-0.8.5.1-win32-setup.exe, U

Figure 33 - Download of Litecoin-0.8.5.1 for Windows platform (event 33).

Looking in more depth (event 33) one can see the time matches the actions taken where Litecoin version 0.8.5.1 was downloaded. One can also see the executable file that was downloaded as Litecoin-0.8.5.1-win32-setup.exe.

2.4.3. Scenario 3 - Win 7 Laptop (Purchase Litecoins) Analysis of Capture

Following our actions taken there is now a forensic capture by our forensic tool Internet Evidence Finder (IEF). The log file for this capture can be found in Section 6.1.16. This file simply details the partitions on the disk that were scanned, the options selected for the scan and the artifacts found, broken down by category. It should be noted that false positives exist. Below (event 34) are the files produced on our USB forensic capture which are created by the forensic. For completeness of capture for this machine, the memory capture (.dmp) file was added manually. This machine is where it is expected to find the most activity from our actions taken.

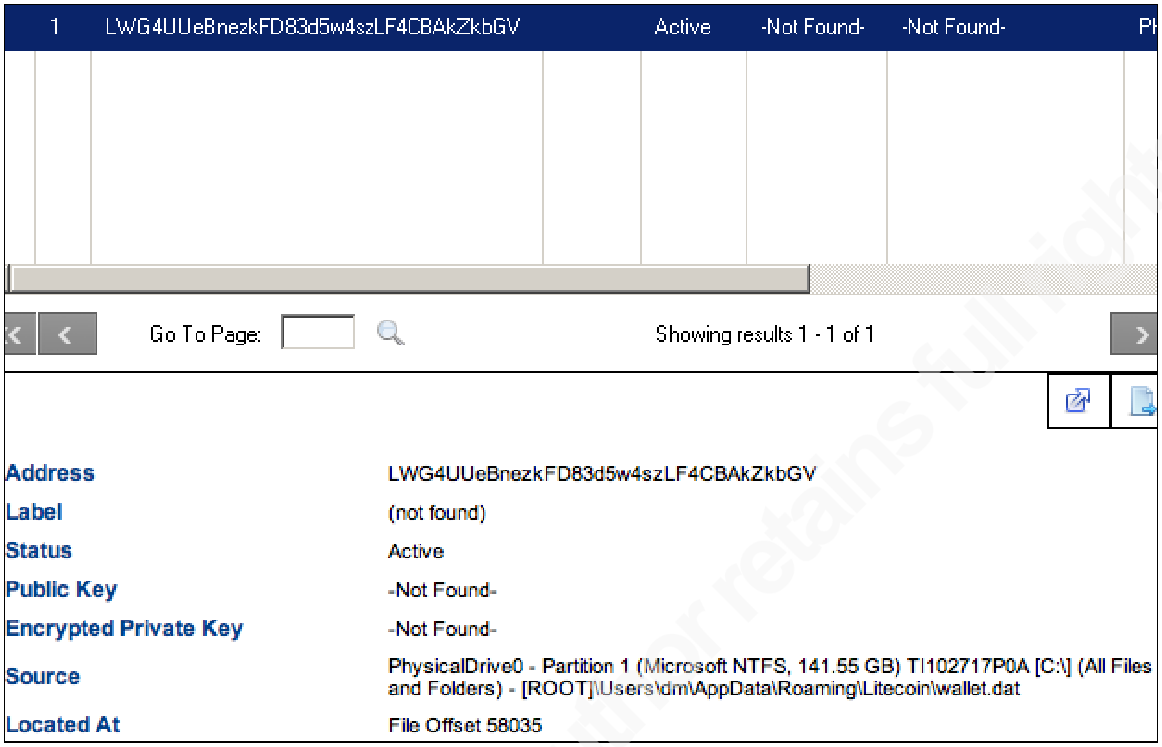


IEFv6	07/04/2014 12:31	Data Base File	4,194,303 KB
IEFv6.db-shm	07/04/2014 12:26	DB-SHM File	17,664 KB
SearchAlerts.db-wal	07/04/2014 12:20	DB-WAL File	0 KB
logging	07/04/2014 12:16	Compressed (zippe...	1 KB
IEFv6.db-wal	07/04/2014 12:14	DB-WAL File	2,310,598 KB
Case Information	07/04/2014 11:58	Text Document	12 KB
IEFCase	07/04/2014 11:58	IEF6 File	22 KB

Figure 34 - Files created by IEF Triage (event 34).

The report viewer is then run (event 2), the case folder loaded (event 3), IEF then loads the artifacts (event 6) and Timezone changed (event 7).

On loading the artifacts, there is an immediate Bitcoin artifact "hit" on this machine as well (event 35):

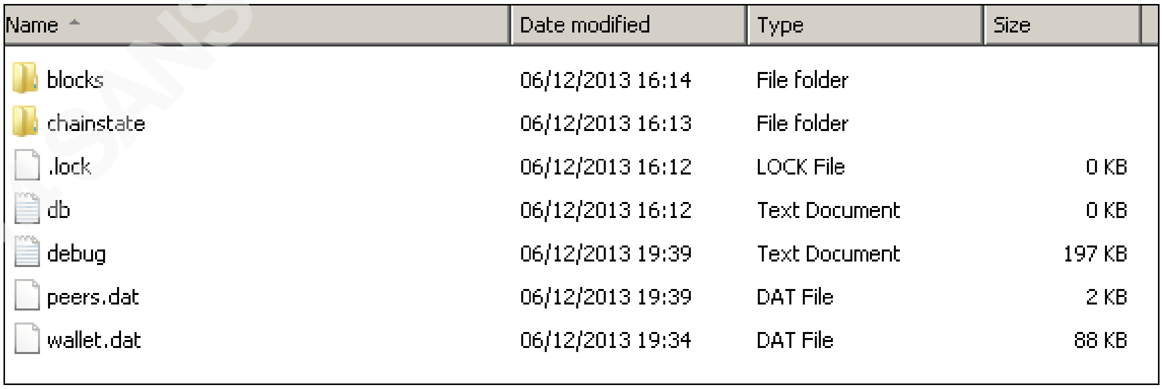


1	LWG4UUeBnezkFD83d5w4szLF4CBAkZkbGV	Active	-Not Found-	-Not Found-	Pl

Address	LWG4UUeBnezkFD83d5w4szLF4CBAkZkbGV
Label	(not found)
Status	Active
Public Key	-Not Found-
Encrypted Private Key	-Not Found-
Source	PhysicalDrive0 - Partition 1 (Microsoft NTFS, 141.55 GB) TI102717P0A [C:\] (All Files and Folders) - [ROOT]\Users\dm\AppData\Roaming\Litecoin\wallet.dat
Located At	File Offset 58035

Figure 35 - Files created by IEF Triage (event 35).

On our test machine the file structure that is left by the install of the Litecoin client (event 36) is then investigated further. Here one can clearly see the *wallet.dat* file. There is also a *peers.dat* file that holds a list of IP addresses that the program connects to through the peer-to-peer virtual currency network.



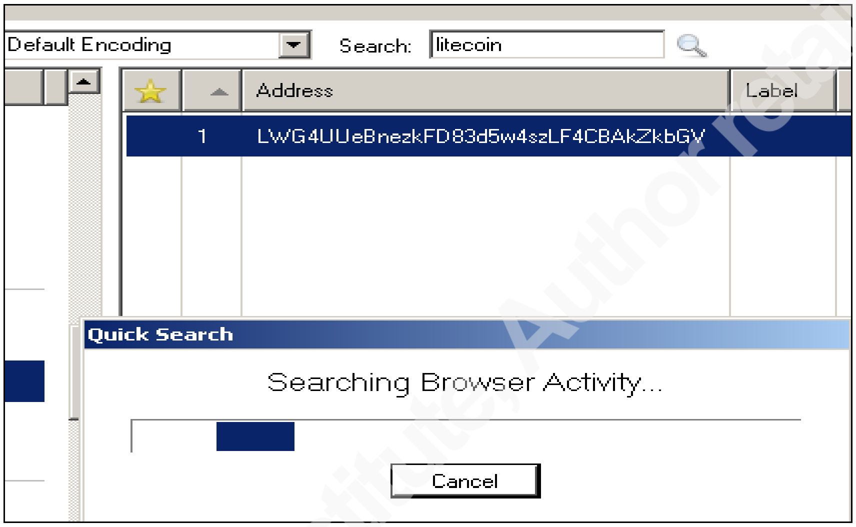
Name	Date modified	Type	Size
blocks	06/12/2013 16:14	File folder	
chainstate	06/12/2013 16:13	File folder	
.lock	06/12/2013 16:12	LOCK File	0 KB
db	06/12/2013 16:12	Text Document	0 KB
debug	06/12/2013 19:39	Text Document	197 KB
peers.dat	06/12/2013 19:39	DAT File	2 KB
wallet.dat	06/12/2013 19:34	DAT File	88 KB

Figure 36 - Files created by Litecoin install (event 36).

For the purpose of this project the hashes of the *peers.dat* and *wallet.dat* files were taken.

MD5 Hash of *wallet.dat*	3c928c5f6cf53338fde30b563c98ccbf
SHA1 Hash of *wallet.dat*	dc798f70c9694a8ccdad1b3dfffc087ff91c740b
MD5 Hash of peers.dat	fbe71c09d316f156d924cbed662104ea
SHA1 Hash of peers.dat	71ed864680383e05c22ccd4cbee2f7fd4ba01359

Next another search is then actioned for "Litecoin" across the artifacts:



Default Encoding

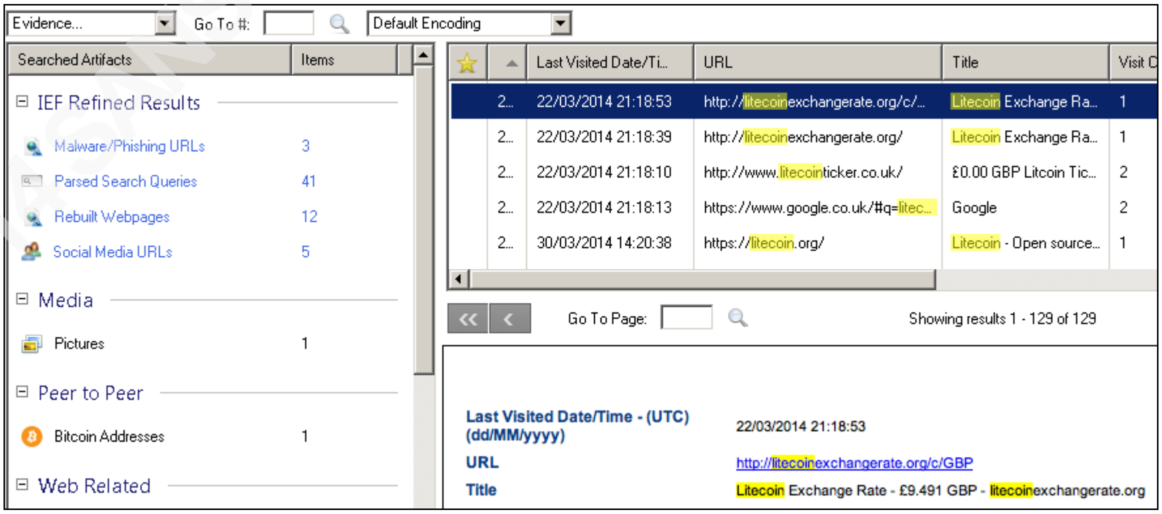
Search: litecoin

☆	▲	Address	Label
	1	LWG4UUeBnezkFD83d5w4szLF4CBAkZkbGV	

Quick Search

Searching Browser Activity...

Figure 37 - Artifact search for "Litecoin" (event 37).



Evidence...

Go To #:

Default Encoding

Searched Artifacts	Items
⊟ IEF Refined Results	
Malware/Phishing URLs	3
Parsed Search Queries	41
Rebuilt Webpages	12
Social Media URLs	5
⊟ Media	
Pictures	1
⊟ Peer to Peer	
Bitcoin Addresses	1
⊟ Web Related	

☆	▲	Last Visited Date/Ti...	URL	Title	Visit C
	2...	22/03/2014 21:18:53	http://litecoinexchangerate.org/c/...	Litecoin Exchange Ra...	1
	2...	22/03/2014 21:18:39	http://litecoinexchangerate.org/	Litecoin Exchange Ra...	1
	2...	22/03/2014 21:18:10	http://www.litecointicker.co.uk/	£0.00 GBP Litcoin Tic...	2
	2...	22/03/2014 21:18:13	https://www.google.co.uk/#q=litec...	Google	2
	2...	30/03/2014 14:20:38	https://litecoin.org/	Litecoin - Open source...	1

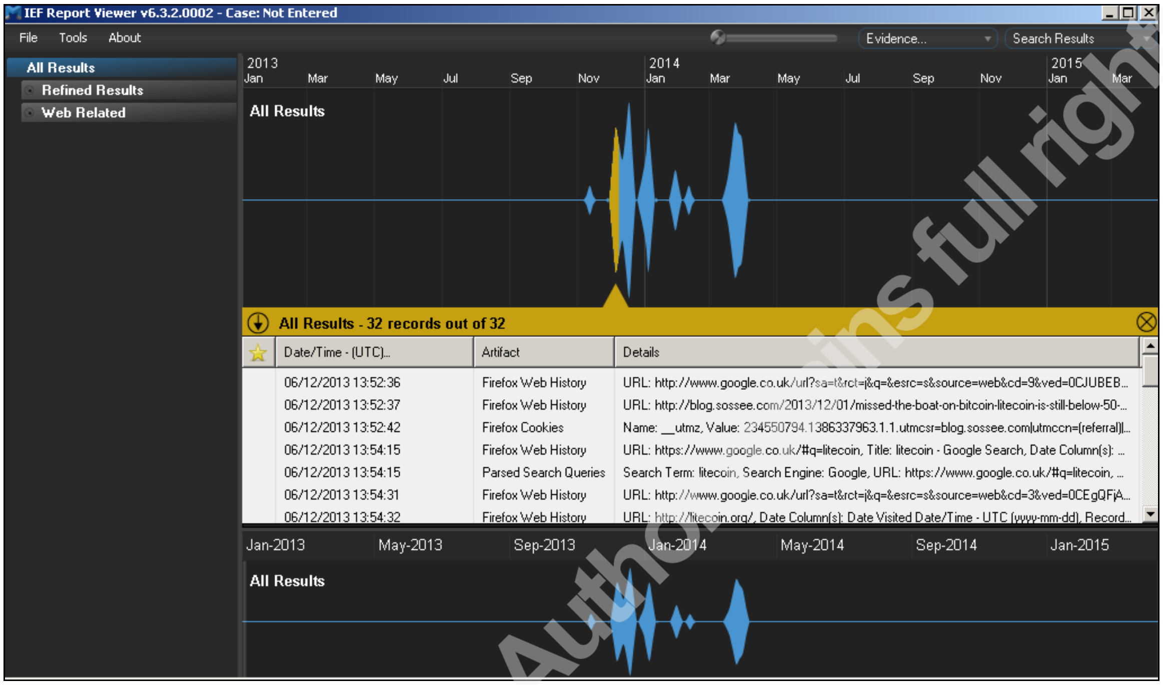
Go To Page:

Showing results 1 - 129 of 129

Last Visited Date/Time - (UTC) (dd/MM/yyyy)	22/03/2014 21:18:53
URL	http://litecoinexchangerate.org/c/GBP
Title	Litecoin Exchange Rate - £9.491 GBP - litecoinexchangerate.org

Figure 38 - Artifact search result for "Litecoin" (event 38).

There are many hits for Litecoin (event 37, 38) as expected. Therefore, we move to the timeline to give us more information.



All Results - 32 records out of 32

☆	Date/Time - (UTC)...	Artifact	Details
	06/12/2013 13:52:36	Firefox Web History	URL: http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=0CJUBEB...
	06/12/2013 13:52:37	Firefox Web History	URL: http://blog.sossee.com/2013/12/01/missed-the-boat-on-bitcoin-litecoin-is-still-below-50-...
	06/12/2013 13:52:42	Firefox Cookies	Name: __utmz, Value: 234550794.1386337963.1.1.utmcsr=blog.sossee.com|utmccn=(referral)|...
	06/12/2013 13:54:15	Firefox Web History	URL: https://www.google.co.uk/#q=litecoin, Title: litecoin - Google Search, Date Column(s): ...
	06/12/2013 13:54:15	Parsed Search Queries	Search Term: litecoin, Search Engine: Google, URL: https://www.google.co.uk/#q=litecoin, ...
	06/12/2013 13:54:31	Firefox Web History	URL: http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CEgQFjA...
	06/12/2013 13:54:32	Firefox Web History	URL: http://litecoin.org/, Date Column(s): Date Visited Date/Time - UTC (yyyy-mm-dd), Record...

Figure 39 - Timeline of Artifact search result for "Litecoin" (event 39).

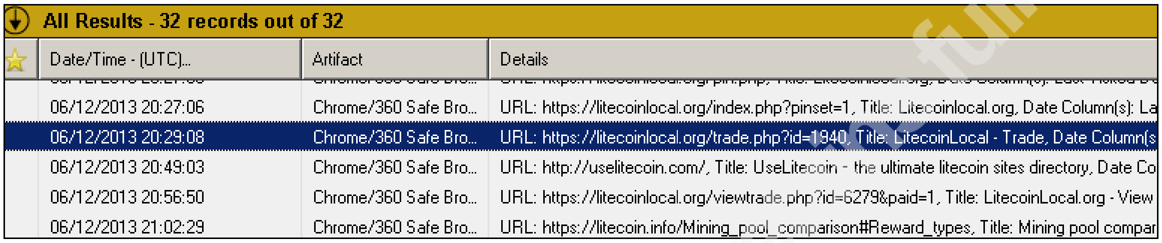
Studying the timeline the following events are recorded in the following periods (event 39), based in our "Litecoin" search:

3rd – 8th December 2013	32 artifacts
9th – 14th December 2013	7 artifacts
15th – 20th December 2013	125 artifacts
27th December – 1st January 2014	2 artifacts
2nd January – 7th January 2014	36 artifacts
26th January – 31st January 2014	3 artifacts
7th February – 12th February 2014	1 artifact
15th March – 20th March 2014	2 artifacts
21st March – 26th March 2014	41 artifacts

27th March – 2nd April 2014	17 artifacts

For the purpose of this paper the highlighted dates, consistent with our actions taken with the most artifacts are of interest.

Looking at the timeline for the 3rd to the 8th December 2013 these entries are of interest (event 40).

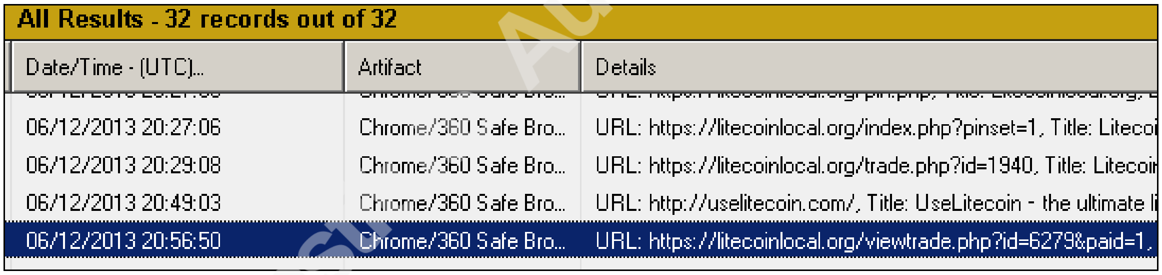


All Results - 32 records out of 32

Date/Time - (UTC)...	Artifact	Details
06/12/2013 20:27:06	Chrome/360 Safe Bro...	URL: https://litecoinlocal.org/index.php?pinset=1, Title: Litecoinlocal.org, Date Column(s): La
06/12/2013 20:29:08	Chrome/360 Safe Bro...	URL: https://litecoinlocal.org/trade.php?id=1940, Title: LitecoinLocal - Trade, Date Column(s
06/12/2013 20:49:03	Chrome/360 Safe Bro...	URL: http://uselitecoin.com/, Title: UseLitecoin - the ultimate litecoin sites directory, Date Co
06/12/2013 20:56:50	Chrome/360 Safe Bro...	URL: https://litecoinlocal.org/viewtrade.php?id=6279&paid=1, Title: LitecoinLocal.org - View
06/12/2013 21:02:29	Chrome/360 Safe Bro...	URL: https://litecoin.info/Mining_pool_comparison#Reward_types, Title: Mining pool compar

Figure 40 - Artifact showing a possible Litecoin transaction (event 40).

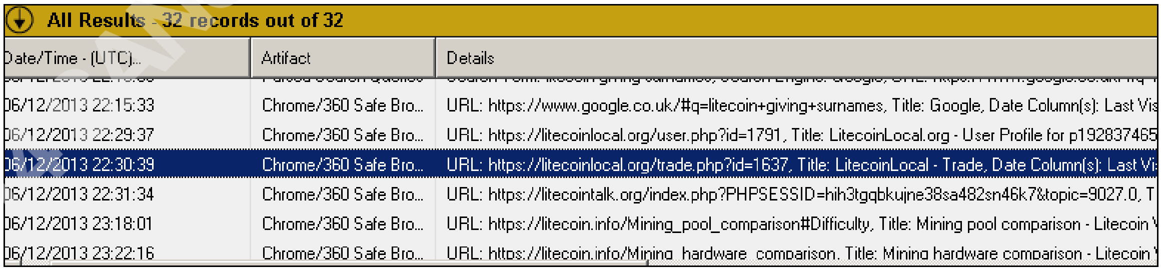
There is an interesting "view trade" URL (event 41):



All Results - 32 records out of 32

Date/Time - (UTC)...	Artifact	Details
06/12/2013 20:27:06	Chrome/360 Safe Bro...	URL: https://litecoinlocal.org/index.php?pinset=1, Title: Litecoi
06/12/2013 20:29:08	Chrome/360 Safe Bro...	URL: https://litecoinlocal.org/trade.php?id=1940, Title: Litecoi
06/12/2013 20:49:03	Chrome/360 Safe Bro...	URL: http://uselitecoin.com/, Title: UseLitecoin - the ultimate l
06/12/2013 20:56:50	Chrome/360 Safe Bro...	URL: https://litecoinlocal.org/viewtrade.php?id=6279&paid=1,

Figure 41 - Artifact showing a possible Litecoin trade (event 41).



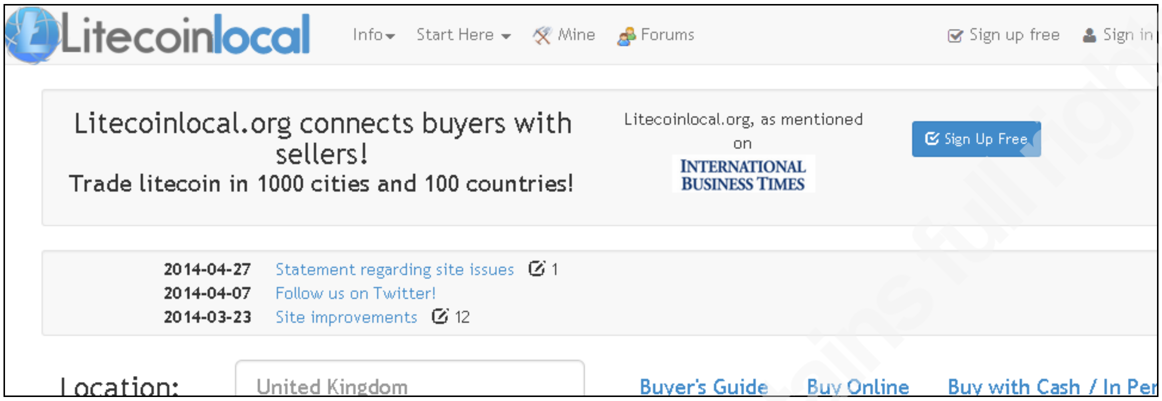
All Results - 32 records out of 32

Date/Time - (UTC)...	Artifact	Details
06/12/2013 22:15:33	Chrome/360 Safe Bro...	URL: https://www.google.co.uk/#q=litecoin+giving+surnames, Title: Google, Date Column(s): Last Vis
06/12/2013 22:29:37	Chrome/360 Safe Bro...	URL: https://litecoinlocal.org/user.php?id=1791, Title: LitecoinLocal.org - User Profile for p192837465
06/12/2013 22:30:39	Chrome/360 Safe Bro...	URL: https://litecoinlocal.org/trade.php?id=1637, Title: LitecoinLocal - Trade, Date Column(s): Last Vi
06/12/2013 22:31:34	Chrome/360 Safe Bro...	URL: https://litecointalk.org/index.php?PHPSESSID=hih3tgqbkujne38sa482sn46k7&topic=9027.0, T
06/12/2013 23:18:01	Chrome/360 Safe Bro...	URL: https://litecoin.info/Mining_pool_comparison#Difficulty, Title: Mining pool comparison - Litecoin
06/12/2013 23:22:16	Chrome/360 Safe Bro...	URL: https://litecoin.info/Mining_hardware_comparison, Title: Mining hardware comparison - Litecoin

Figure 42 - Artifact showing a possible Litecoin trade and user id (event 42).

There are no more trade references in this timeframe and know from our actions taken that our last trade was 22:30:39 that matches the timeline.

Taking a look at the Litecoinlocal.org website (event43), we can see what Litecoinlocal.org is and what it can be used for.



Litecoinlocal.org connects buyers with sellers!
Trade litecoin in 1000 cities and 100 countries!

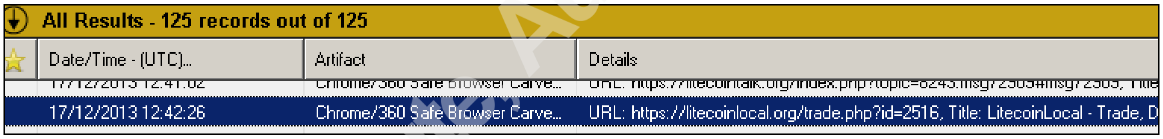
Litecoinlocal.org, as mentioned on

2014-04-27 Statement regarding site issues 1
2014-04-07 Follow us on Twitter!
2014-03-23 Site improvements 12

Location: United Kingdom Buyer's Guide Buy Online Buy with Cash / In Per

Figure 43 - Checking URL artifact on the internet – (event 43).

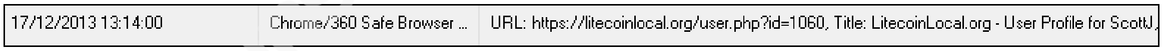
Looking at the timeline for the 15th to the 20th December 2013, these entries are of interest.



All Results - 125 records out of 125

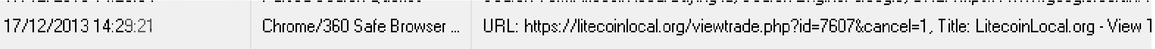
Date/Time - (UTC)...	Artifact	Details
17/12/2013 12:41:02	Chrome/360 Safe Browser Carve...	URL: https://litecointalk.org/index.php?topic=8243.msg72505#msg72505, Title
17/12/2013 12:42:26	Chrome/360 Safe Browser Carve...	URL: https://litecoinlocal.org/trade.php?id=2516, Title: LitecoinLocal - Trade, D

Figure 44 - Artifact showing a possible Litecoin trade and user id (event 44).



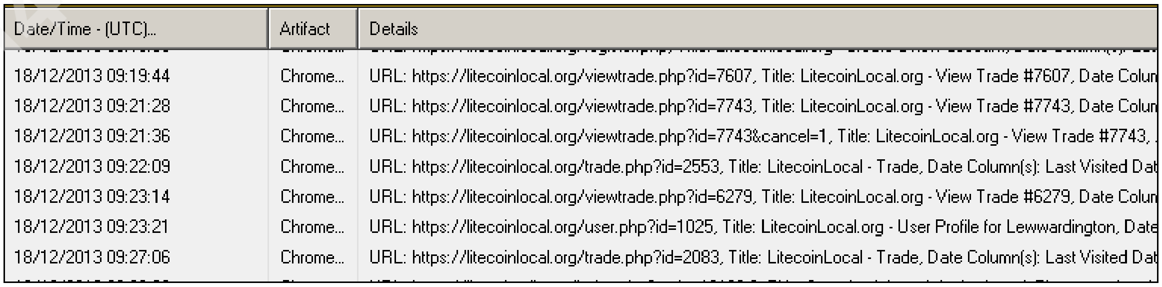
17/12/2013 13:14:00	Chrome/360 Safe Browser ...	URL: https://litecoinlocal.org/user.php?id=1060, Title: LitecoinLocal.org - User Profile for ScottJ,

Figure 45 - Artifact showing a possible Litecoin trade and user id and username (event 45).

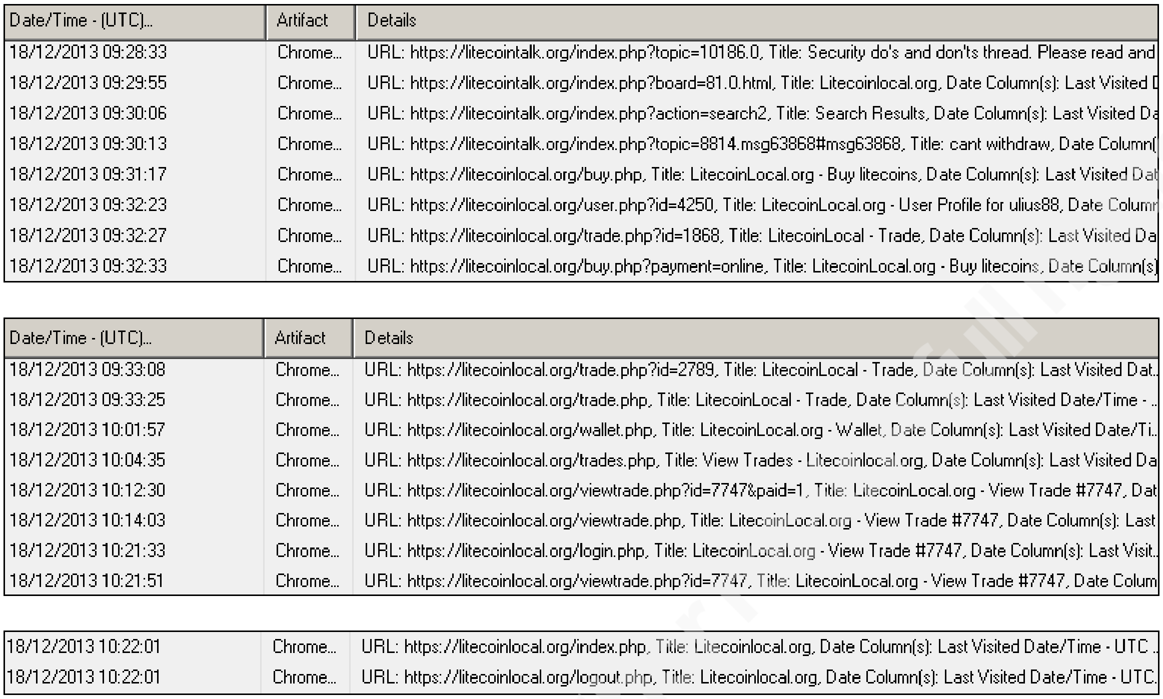


17/12/2013 14:29:21	Chrome/360 Safe Browser ...	URL: https://litecoinlocal.org/viewtrade.php?id=7607&cancel=1, Title: LitecoinLocal.org - View T

Figure 46 - Artifact showing a possible Litecoin trade cancellation (event 46).



Date/Time - (UTC)...	Artifact	Details
18/12/2013 09:19:44	Chrome...	URL: https://litecoinlocal.org/viewtrade.php?id=7607, Title: LitecoinLocal.org - View Trade #7607, Date Colun
18/12/2013 09:21:28	Chrome...	URL: https://litecoinlocal.org/viewtrade.php?id=7743, Title: LitecoinLocal.org - View Trade #7743, Date Colun
18/12/2013 09:21:36	Chrome...	URL: https://litecoinlocal.org/viewtrade.php?id=7743&cancel=1, Title: LitecoinLocal.org - View Trade #7743,
18/12/2013 09:22:09	Chrome...	URL: https://litecoinlocal.org/trade.php?id=2553, Title: LitecoinLocal - Trade, Date Column(s): Last Visited Dat
18/12/2013 09:23:14	Chrome...	URL: https://litecoinlocal.org/viewtrade.php?id=6279, Title: LitecoinLocal.org - View Trade #6279, Date Colun
18/12/2013 09:23:21	Chrome...	URL: https://litecoinlocal.org/user.php?id=1025, Title: LitecoinLocal.org - User Profile for Lewwardington, Date
18/12/2013 09:27:06	Chrome...	URL: https://litecoinlocal.org/trade.php?id=2083, Title: LitecoinLocal - Trade, Date Column(s): Last Visited Dat



Date/Time - (UTC)...	Artifact	Details
18/12/2013 09:28:33	Chrome...	URL: https://litecointalk.org/index.php?topic=10186.0, Title: Security do's and don'ts thread. Please read and
18/12/2013 09:29:55	Chrome...	URL: https://litecointalk.org/index.php?board=81.0.html, Title: Litecoinlocal.org, Date Column(s): Last Visited D
18/12/2013 09:30:06	Chrome...	URL: https://litecointalk.org/index.php?action=search2, Title: Search Results, Date Column(s): Last Visited Da
18/12/2013 09:30:13	Chrome...	URL: https://litecointalk.org/index.php?topic=8814.msg63868#msg63868, Title: cant withdraw, Date Column(
18/12/2013 09:31:17	Chrome...	URL: https://litecoinlocal.org/buy.php, Title: LitecoinLocal.org - Buy litecoins, Date Column(s): Last Visited Dat
18/12/2013 09:32:23	Chrome...	URL: https://litecoinlocal.org/user.php?id=4250, Title: LitecoinLocal.org - User Profile for ulius88, Date Column
18/12/2013 09:32:27	Chrome...	URL: https://litecoinlocal.org/trade.php?id=1868, Title: LitecoinLocal - Trade, Date Column(s): Last Visited Da
18/12/2013 09:32:33	Chrome...	URL: https://litecoinlocal.org/buy.php?payment=online, Title: LitecoinLocal.org - Buy litecoins, Date Column(s)
18/12/2013 09:33:08	Chrome...	URL: https://litecoinlocal.org/trade.php?id=2789, Title: LitecoinLocal - Trade, Date Column(s): Last Visited Dat...
18/12/2013 09:33:25	Chrome...	URL: https://litecoinlocal.org/trade.php, Title: LitecoinLocal - Trade, Date Column(s): Last Visited Date/Time - ...
18/12/2013 10:01:57	Chrome...	URL: https://litecoinlocal.org/wallet.php, Title: LitecoinLocal.org - Wallet, Date Column(s): Last Visited Date/Ti...
18/12/2013 10:04:35	Chrome...	URL: https://litecoinlocal.org/trades.php, Title: View Trades - Litecoinlocal.org, Date Column(s): Last Visited Da
18/12/2013 10:12:30	Chrome...	URL: https://litecoinlocal.org/viewtrade.php?id=7747&paid=1, Title: LitecoinLocal.org - View Trade #7747, Dat
18/12/2013 10:14:03	Chrome...	URL: https://litecoinlocal.org/viewtrade.php, Title: LitecoinLocal.org - View Trade #7747, Date Column(s): Last
18/12/2013 10:21:33	Chrome...	URL: https://litecoinlocal.org/login.php, Title: LitecoinLocal.org - View Trade #7747, Date Column(s): Last Visit...
18/12/2013 10:21:51	Chrome...	URL: https://litecoinlocal.org/viewtrade.php?id=7747, Title: LitecoinLocal.org - View Trade #7747, Date Colum
18/12/2013 10:22:01	Chrome...	URL: https://litecoinlocal.org/index.php, Title: Litecoinlocal.org, Date Column(s): Last Visited Date/Time - UTC ...
18/12/2013 10:22:01	Chrome...	URL: https://litecoinlocal.org/logout.php, Title: Litecoinlocal.org, Date Column(s): Last Visited Date/Time - UTC.

Figure 47 - multiple artifacts showing possible Litecoin transactions (event 47).

Knowing the actions that have been taken to generate these artifacts, this is the second trade as the timeline matches. There is a wealth of artifact information here and by studying these transactions one is able to identify usernames and the four digit numbers that make up a user ID. However, an investigator can also identify this just from browsing Litecoinlocal.org, as the information is present in the web page URL when you click on a user.

3. Results

3.1. Scenario 1

A user has a Windows 8 laptop, has installed Firefox, with no script add-on and Tor on the laptop. They have browsed for "Utopia" and browsed the site but have not made any purchases. They have browsed various Litecoin currency exchanges.

The steps taken on this machine were to download and install Tor. The artifacts found in Figure 14 show the Tor download. Figure 15 shows search strings entered in the browser in relation to Tor. However, what was not found were any artifacts in relation to search entries made by the user through the Tor browser once it was installed. By keeping a record of the actions taken, the search terms entered in the Tor browser were the same as were entered and no artifacts were matched by the forensic product.

Moving on to looking for Bitcoin artifacts, a search was actioned for *wallet.dat*. This was also not located on this machine and neither was any other Bitcoin or crypto currency artifacts known to the forensic program.

3.2. Scenario 2

A user has a Windows 7 laptop, has installed the Litecoin application.

The steps taken on this machine were to download and install Litecoin as a peer-to-peer program. This then participates in the Litecoin P2P community processing transactions when it is running on the machine.

On running the forensic tool on this machine, it immediately highlighted a Bitcoin artifact as seen in Figure 23.

Upon closer inspection, the tool seems to do this when it finds a file called *wallet.dat* which can be seen in Figure 25.

Once it was known that *wallet.dat* was on this system a search for "Litecoin" was entered to go over all the artifacts and pull out these. Figure 28 shows the artifact hits for "Litecoin". There are various artifacts ranging from picture files to URLs and search queries in various browsers. Appendix 6.1.4 shows the icons and image files installed on a machine when the Litecoin install package runs. The download of the Litecoin application can be seen in Figure 33 and this matches our download as documented in Appendix 6.1.2

3.3. Scenario 3

A user has used a Windows 7 laptop to buy Litecoins through a Litecoin currency website.

The forensic product again found on this laptop the file *wallet.dat* indicating the possible use of a crypto currency on this machine. Looking through the timeline artifacts in Figure 40 it clearly correlates with our Appendix 6.1.3. On the 6th December 2013, a trade was initiated with a user called lewwardington on the website litecoinlocal.org

Looking at the transaction in more detail the trade was initiated at 20:30:52 on the 6th December 2013. The trade id can be seen in Appendix 6.1.7 which has a summary of the trades and in Appendix 6.1.8 for this specific trade. The Trade ID is 6279. Our forensic timeline in (event 40, 41) shows a machine user viewing this trade in the URL artifact.

4. Summary and Conclusion

Our results confirm that the use of Tor can present problems for forensic artifacts to be found in terms of activity. This was demonstrated in our first scenario on Windows 8. From a forensic perspective live memory analysis would be a next interesting area to investigate Tor. Our results can prove forensically that someone used a web browser to search for Tor and download the Tor browser bundle. A user then used Tor on the machine. Once the user was running the Tor browser the tool was unable to identify what actions were taken and proved in our search (event 21).

Virtual currency artifacts from the peer-to-peer Litecoin install demonstrated the download of Litecoin onto a machine and presence of crypto currency artifacts. However, other than that, to explore this further the key files of interest to a forensic investigator would be the *wallet.dat* and *peers.dat*.

Peers.dat contains connection information. This may assist in an investigation in terms of network connections to and from a machine participating on a peer-to-peer currency network.

The third test where four transactions, (two processed, two cancelled) have created a host of artifacts shows that cloud forensics is just as important to corroborate the tools findings. Litecoin and the open nature of transactions have allowed us to draw together transaction data from the forensic tool. This matches the actions taken. The key artifacts for an investigator would appear to be user.php web page URLs which contain user IDs in relation to the website Litecoinlocal.org. Trade IDs and the buy.php URL are also key artifacts but they do not always confirm a buying transaction. They merely demonstrate a possible intent to buy and need verifying with other artifacts.

Litecoinlocal.org holds a lot of information to corroborate user's activity on its site. Transaction parties are listed, as are all their trades and conversations.

In conclusion, an investigator would be interested in the artifacts, the online exchange website, the user's transactions through the online exchange and their Litecoin balance if one exists. *Wallet.dat* in this case was not used or taken off line, for example on removable media, encrypted. Interestingly if the user removes the Litecoin application *wallet.dat* and *peers.dat* remain on the machine.

Technology offers the use of crypto currencies in a variety of ways in terms of purchasing and selling. The tools that exist would allow a user to do the following. A user who wishes to remain anonymous could take the following actions:

1. Download Tor onto a USB device.
2. Connect the USB device to a workstation of choice anywhere.
3. Browse to a crypto currency exchange and agree to meet in person and purchase for cash.
4. Connect the USB device to a different workstation of choice anywhere.
5. Browse to the crypto currency exchange and download currency to *wallet.dat* on the USB device.
6. Print the details of the private key of the wallet.
7. Lock the USB away or distribute the USB to others.
8. Repeat step 1 with a new USB device.

Further research in this area and consideration of the above may produce a quicker forensic process when looking for the potential use of crypto currency in forensic field.

5. References

Kashmir, Hill (2014) A $100 Worth Of Litecoin A Year Ago Is Worth $30,000 Today
http://www.forbes.com/sites/kashmirhill/2014/01/13/a-100-worth-of-litecoin-a-year-ago-is-worth-30000-today/

Wikipedia, Litecoin, (2014)
http://en.wikipedia.org/wiki/Litecoin

Wikipedia, Bitcoin, (2014)
http://en.wikipedia.org/wiki/Bitcoin

AAT Comment, (2013) Bitcoin: what is it and how does it work?
http://www.aatcomment.org.uk/aat-view/front-page-latest-featured-articles/bitcoin-what-is-it-how-it-works

Jules, (2013) Maintaining Anonymity While Using Bitcoins
http://thedailyattack.com/2013/06/maintaining-anonymity-while-using-bitcoins/

Sandvik, Runa A, (2013) Forensic Analysis of the Tor Browser Bundle on OX X, Linux, and Windows.
https://research.Torproject.org/techreports/tbb-forensic-analysis-2013-06-28.pdf

Chadwick, Luke, (2013). Unauthorised Amazon mining
http://vertis.io/2013/12/16/unauthorised-litecoin-mining.html

Barker, Ian (2014) Cyber criminals Pony up to steal BitCoins
http://betanews.com/2014/02/25/cyber-criminals-pony-up-to-steal-bitcoins/

Rugato.com (2013) Accessing Silk Road without Tor
http://www.rugatu.com/questions/7938/do-you-know-how-to-access-silk-road-without-using-the-Tor-browser

Saliba, Jad (2013) Bitcoin Forensics – A Journey into the Dark Web
http://articles.forensicfocus.com/2013/11/06/bitcoin-forensics-a-journey-into-the-dark-web/

Saliba, Jad (2013) Bitcoin Forensics Part II: The Secret Web Strikes Back
http://articles.forensicfocus.com/2013/11/14/bitcoin-forensics-part-2-the-secret-web-strikes-back/

http://www.hackmiami.org/whitepapers/HackMiami-Analysis_of_the_Cryptocurrency_Marketplace.pdf

Couts, Andrew (2013) HOW TO BUY BITCOIN, LITECOIN, AND DOGECOIN
http://www.digitaltrends.com/cool-tech/buy-bitcoin-litecoin-dogecoin/

Kirk, Jeremy (2014) 'Coinkrypt' malware mines cryptocurrencies on Android
http://www.networkworld.com/news/2014/032714-39coinkrypt39-malware-mines-cryptocurrencies-on-280135.html

Smith, Chris (2014) Legit Google Play apps found to be covertly mining digital currency
http://bgr.com/2014/03/27/Google-play-malware-android-apps/

6. Appendix

6.1. Test Environment & Software versions used

Magnet Forensics

Internet Evidence Finder v6.3.2.0002 – release 02/10/13, file size 11,328,344

MD5 - d12687d731934c34bcbf7c5a0e8563cd

SHA1 - e4ddd0d910fb998aa488c67c7780ee8a901f905b

Report Viewer v6.3.2.0002 – release 02/10/13, file size 2,949,968

MD5 - fa3a58d64d80caef51c63b5ee50f5164

SHA1 – 7d66b27f9d06aafeff618191ab43db95ce8dcc2d

Timeline version v6.3.2.0002 – release 02/10/13, file size 902,984

MD5 – 8c7e8c3e1ea6d281c1dcd3dc8dcc5d86

SHA1 - b87e36690162daed46eed68f0b19e2ce15ec680b

Litecoin version v0.8.5.1 – release 12/9/13, file size 13,633,097

MD5 - d816f8124b0caf4d939150bb4ad446ea

SHA1 - b67187d29d222d158aa69cc628d9b468713433c7

Litecoin version v0.8.6.2 – release 11/1/14, file size 13,227,723

MD5 – cea4df067f39ccac017a9ecc9616bf9d

SHA1 – 3c3a38aa97e55859d43a471e33618f6c08af2785

6.1.1. Clean Windows 8 SP1 Professional 64 bit laptop

(1.6Ghz, 4GB, 128GB, NTFS)

6.1.2. Scenario 2 - Used Windows 7 SP1 Professional 64 bit laptop

(2Ghz, 2GB, 300GB, NFTS)

6/12/13 – 20:01 – Litecoin.qt 0.8.5.1 installed.

13/1/14 – 10:11 – Litecoin.qt 0.8.6.2 installed.

6.1.3. Scenario 3- Used Windows 7 SP1 Professional 32 bit laptop

(1.6Ghz, 2GB, 160GB, NFTS)

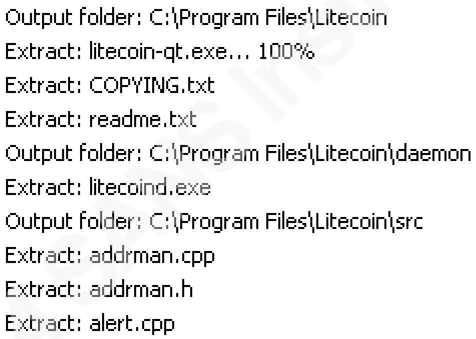
6/12/13 – Trade on Litecoin.local.org with lewwardington

17/12/13 – Password reset request for Litecoin.local.org

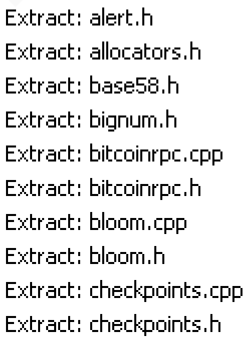
17/12/13 – Aborted trade Dialogue with Scottj on Litecoin.local.org

18/12/13 – Trade Litecoin.local.org with jpsdesign

6.1.4. Litecoin Windows Version 8.6.2 files extraction



```
Output folder: C:\Program Files\Litecoin
Extract: litecoin-qt.exe... 100%
Extract: COPYING.txt
Extract: readme.txt
Output folder: C:\Program Files\Litecoin\daemon
Extract: litecoind.exe
Output folder: C:\Program Files\Litecoin\src
Extract: addrman.cpp
Extract: addrman.h
Extract: alert.cpp
```



```
Extract: alert.h
Extract: allocators.h
Extract: base58.h
Extract: bignum.h
Extract: bitcoinrpc.cpp
Extract: bitcoinrpc.h
Extract: bloom.cpp
Extract: bloom.h
Extract: checkpoints.cpp
Extract: checkpoints.h
```

Last Updated: March 21st, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Pen Test Austin 2017	**Austin, TXUS**	**Mar 27, 2017 - Apr 01, 2017**	**Live Event**
SANS NetWars at NSM Security Conference	**Oslo, NO**	**Mar 28, 2017 - Mar 29, 2017**	**Live Event**
SEC564: Red Team Ops	**Atlanta, GAUS**	**Apr 06, 2017 - Apr 07, 2017**	**Live Event**
SANS 2017	**Orlando, FLUS**	**Apr 07, 2017 - Apr 14, 2017**	**Live Event**
Threat Hunting and IR Summit	**New Orleans, LAUS**	**Apr 18, 2017 - Apr 25, 2017**	**Live Event**
SANS London April 2017	**London, GB**	**Apr 24, 2017 - Apr 25, 2017**	**Live Event**
SANS Baltimore Spring 2017	**Baltimore, MDUS**	**Apr 24, 2017 - Apr 29, 2017**	**Live Event**
Automotive Cybersecurity Summit	**Detroit, MIUS**	**May 01, 2017 - May 08, 2017**	**Live Event**
SANS Riyadh 2017	**Riyadh, SA**	**May 06, 2017 - May 11, 2017**	**Live Event**
SANS Security West 2017	**San Diego, CAUS**	**May 09, 2017 - May 18, 2017**	**Live Event**
SANS Zurich 2017	**Zurich, CH**	**May 15, 2017 - May 20, 2017**	**Live Event**
SANS Northern Virginia - Reston 2017	**Reston, VAUS**	**May 21, 2017 - May 26, 2017**	**Live Event**
SANS Melbourne 2017	**Melbourne, AU**	**May 22, 2017 - May 27, 2017**	**Live Event**
SANS London May 2017	**London, GB**	**May 22, 2017 - May 27, 2017**	**Live Event**
SANS Stockholm 2017	**Stockholm, SE**	**May 29, 2017 - Jun 03, 2017**	**Live Event**
SANS Madrid 2017	**Madrid, ES**	**May 29, 2017 - Jun 03, 2017**	**Live Event**
SANS Atlanta 2017	**Atlanta, GAUS**	**May 30, 2017 - Jun 04, 2017**	**Live Event**
SANS San Francisco Summer 2017	**San Francisco, CAUS**	**Jun 05, 2017 - Jun 10, 2017**	**Live Event**
Security Operations Center Summit & Training	**Washington, DCUS**	**Jun 05, 2017 - Jun 12, 2017**	**Live Event**
SANS Houston 2017	**Houston, TXUS**	**Jun 05, 2017 - Jun 10, 2017**	**Live Event**
SANS Milan 2017	**Milan, IT**	**Jun 12, 2017 - Jun 17, 2017**	**Live Event**
SANS Thailand 2017	**Bangkok, TH**	**Jun 12, 2017 - Jun 30, 2017**	**Live Event**
SANS Rocky Mountain 2017	**Denver, COUS**	**Jun 12, 2017 - Jun 17, 2017**	**Live Event**
SANS Charlotte 2017	**Charlotte, NCUS**	**Jun 12, 2017 - Jun 17, 2017**	**Live Event**
SANS Secure Europe 2017	**Amsterdam, NL**	**Jun 12, 2017 - Jun 20, 2017**	**Live Event**
SEC555: SIEM-Tactical Analytics	**San Diego, CAUS**	**Jun 12, 2017 - Jun 17, 2017**	**Live Event**
SANS Philippines 2017	**Manila, PH**	**Jun 19, 2017 - Jun 24, 2017**	**Live Event**
SANS Minneapolis 2017	**Minneapolis, MNUS**	**Jun 19, 2017 - Jun 24, 2017**	**Live Event**
SANS Abu Dhabi 2017	**OnlineAE**	**Mar 25, 2017 - Mar 30, 2017**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**