Fight crime.
Unravel incidents... one byte at a time.

Interested in learning more?
Check out the list of upcoming events offering "Advanced Incident Response, Threat Hunting, and Digital Forensics (FOR508) at http://digital-forensics.sans.org/events/
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

1. Introduction to Virtual/Crypto Currencies ................................................................. 5
   1.1. The Exchanges – Converting Physical Currency to Virtual Currency .................. 6
   1.2. The Peer-to-peer client ......................................................................................... 6
   1.3. Mining .................................................................................................................... 7
   1.4. Digital Wallet ......................................................................................................... 7
   1.5. Example of the user process to do a transaction .................................................. 8
   Summary ......................................................................................................................... 9
2. Test Schedule .................................................................................................................. 11
   2.1. Equipment utilised .................................................................................................. 11
   2.2. Methodology .......................................................................................................... 11
   2.3. Actions Taken ......................................................................................................... 12
       2.3.1 Scenario 1 ......................................................................................................... 12
       2.3.2 Scenario 2 ......................................................................................................... 13
       2.3.3 Scenario 3 ......................................................................................................... 14
   2.4. Analysis .................................................................................................................. 15
       2.4.1. Scenario 1 - Win 8 Laptop Analysis of Capture .............................................. 16
       2.4.2. Scenario 2 - Win 7 Laptop (running Litecoin) Analysis of Capture ................ 27
       2.4.3. Scenario 3 - Win 7 Laptop (Purchase Litecoins) Analysis of Capture .......... 33
3. Results ............................................................................................................................. 40
   3.1. Scenario 1 ................................................................................................................ 40
   3.2. Scenario 2 ................................................................................................................ 40
   3.3. Scenario 3 ................................................................................................................ 41
4. Summary and Conclusion .............................................................................................. 42
5. References ....................................................................................................................... 44
6. Appendix .......................................................................................................................... 46
   6.1. Test Environment & Software versions used ......................................................... 46
       6.1.1. Clean Windows 8 SP1 Professional 64 bit laptop ............................................ 46
       6.1.2. Scenario 2 - Used Windows 7 SP1 Professional 64 bit laptop ......................... 47
       6.1.3. Scenario 3- Used Windows 7 SP1 Professional 32 bit laptop ......................... 47
       6.1.4. Litecoin Windows Version 8.6.2 files extraction ............................................. 47
       6.1.5. Litecoin Windows Version 8.6.2 hashes ........................................................ 60
       6.1.6. Litecoin Windows Version 8.6.2 hashes after uninstallation ......................... 62
       6.1.7. Summary of trades ......................................................................................... 63
       6.1.8. Detail of first trade id 6279 .............................................................................. 63
       6.1.9. Detail of second trade id 7607 – cancelled ..................................................... 65
       6.1.10. Detail of third trade id 7743 – cancelled ....................................................... 66
       6.1.11. Detail of fourth trade id 7747 and user ........................................................... 66
       6.1.12. Detail of authors user id and trades ................................................................. 68
       6.1.13. Email trail of trades from litecoinlocal.org .................................................. 69
       6.1.14. Forensic Tool Log for Scenario 1 laptop ......................................................... 76
       6.1.15. Forensic Tool Log for Scenario 2 laptop ......................................................... 85
       6.1.16. Forensic Tool Log for Scenario 3 laptop ......................................................... 92
List of Figures

Figure 1 - Files created by IEF Triage (event 1) ................................................................. 16
Figure 2 - Running IEF Report Viewer (event 2) . ............................................................... 16
Figure 3 - Loading the IEF Triage file (event 3) ................................................................. 17
Figure 4 - Navigating to the IEF Triage file source (event 4) .............................................. 17
Figure 5 - IEF Triage file loading the artifacts from the file source (event 5) ....................... 18
Figure 6 - IEF Triage file listing of artifacts (event 6) .......................................................... 18
Figure 7 - Changing IEF Triage Time Zone to match our forensic source (event 7) ............ 19
Figure 8 - Searching IEF Triage file (event 8) ......................................................................... 19
Figure 9 - IEF searching (event 9) .......................................................................................... 19
Figure 10 - No results from IEF Triage file search (event 10) ............................................... 20
Figure 11 - Running IEF Triage Timeline (event 11) ............................................................ 20
Figure 12 - IEF Triage Timeline file (event 12) ..................................................................... 21
Figure 13 - Viewing correlated artifacts on the IEF Timeline (event 13) ............................... 22
Figure 14 - Viewing correlated artifacts on the IEF Timeline from our actions (event 14) ..... 23
Figure 15 - Viewing Tor artifacts on the IEF Timeline from our actions (event 15) ...... 23
Figure 16 - Searching for Tor artifacts (event 16) ................................................................. 23
Figure 17 - Hits found from a search for Tor (event 17) ......................................................... 24
Figure 18 - First hit confirms an Internet Explorer artifact for the URL (event 18) .......... 24
Figure 19 - Further hits confirming Internet Explorer artifacts for Tor (event 19) ............. 25
Figure 20 - Tor related artifacts in time order (event 20) ....................................................... 26
Figure 21 - Search query validation of actions taken (event 21) ............................................ 26
Figure 22 - Files created by IEF Triage (event 22) ................................................................. 27
Figure 23 - Bitcoin artifact hit (event 23) ............................................................................... 27
Figure 24 - Bitcoin artifact hit (event 24) ............................................................................... 28
Figure 25 - Bitcoin artifact hit (event 25) ............................................................................... 28
Figure 26 - Search for Litecoin artifacts (event 26) .............................................................. 28
Figure 27 - Results of a Bitcoin search parameter in IEF (event 27) .................................... 29
Figure 28 - Results of a Bitcoin search parameter in IEF (event 28) ................................. 29
Figure 29 - Results of a Litecoin search parameter in IEF (event 29) ................................. 30
Figure 30 - Results of Timeline for this machine (event 30) .................................................. 30
Figure 31 - Results of Timeline records for this machine (event 31) ..................................... 31
Figure 32 - Results of Timeline records for this machine (event 32) ..................................... 31
Figure 33 - Download of Litecoin-0.8.5.1 for Windows platform (event 33) ...................... 32
Figure 34 - Files created by IEF Triage (event 34) ................................................................. 33
Figure 35 - Files created by IEF Triage (event 35) ................................................................. 34
Figure 36 - Files created by Litecoin install (event 36) .......................................................... 34
Figure 37 - Artifact search for “Litecoin” (event 37) ............................................................. 35
Figure 38 - Artifact search result for “Litecoin” (event 38) .................................................. 35
Figure 39 - Timeline of Artifact search result for “Litecoin” (event 39) ............................... 36
Figure 40 - Artifact showing a possible Litecoin transaction (event 40) ............................... 37
Figure 41 - Artifact showing a possible Litecoin trade (event 41) ........................................ 37
Figure 42 - Artifact showing a possible Litecoin trade and user id (event 42) ....................... 37
Figure 43 - Checking URL artifact on the internet – (event 43) ............................................ 38

Daniel Piggott, Piggott.daniel@gmail.com
Figure 44 - Artifact showing a possible Litecoin trade and user id (event 44).................. 38
Figure 45 - Artifact showing a possible Litecoin trade and user id and username (event 45). ........................................................................................................................................ 38
Figure 46 - Artifact showing a possible Litecoin trade cancellation (event 46).............. 38
Figure 47 - multiple artifacts showing possible Litecoin transactions (event 47)......... 39
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 straightforward to purchase for the average user. Here is an example of Bitcoin/Litecoin:

![Figure AAT Comment, 2013 Bitcoin: what is it and how does it work?](image-url)

Daniel Piggott, Piggott.daniel@gmail.com
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,
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.

LvvZVxxgCvYBzAuJm3v99uG48o3yG89h2Ph

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.

Daniel Piggott, Piggott.daniel@gmail.com
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.

Daniel Piggott, Piggott.daniel@gmail.com
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.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Date/Time</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>win8torproglaptopram.dmp</td>
<td>16/03/2014</td>
<td>DMP File</td>
<td>3,325,552 KB</td>
</tr>
<tr>
<td>Bookmark</td>
<td>16/03/2014</td>
<td>Data Base File</td>
<td>0 KB</td>
</tr>
<tr>
<td>trmpfc7c3ae2-83da-44e9-80bc-93d8da9bdfdd</td>
<td>16/03/2014</td>
<td>FLV File</td>
<td>1 KB</td>
</tr>
<tr>
<td>Case Information</td>
<td>16/03/2014</td>
<td>Text Document</td>
<td>10 KB</td>
</tr>
<tr>
<td>Filter</td>
<td>16/03/2014</td>
<td>Data Base File</td>
<td>1 KB</td>
</tr>
<tr>
<td>IEF\v6</td>
<td>16/03/2014</td>
<td>Data Base File</td>
<td>950,836 KB</td>
</tr>
<tr>
<td>logging</td>
<td>16/03/2014</td>
<td>WinRAR ZIP archive</td>
<td>1 KB</td>
</tr>
<tr>
<td>Search</td>
<td>16/03/2014</td>
<td>Data Base File</td>
<td>1 KB</td>
</tr>
<tr>
<td>SearchAlerts</td>
<td>16/03/2014</td>
<td>Data Base File</td>
<td>1 KB</td>
</tr>
</tbody>
</table>

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.

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”.

![Figure 3 - Loading the IEF Triage file (event 3).](image)

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).](image)

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).

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).

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](image)

**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).

![Search IEF Triage file](image)

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

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

![IEF searching](image)

**Figure 9 - IEF searching (event 9).**

Daniel Piggott, Piggott.daniel@gmail.com
Our search returns no results for the term “Litecoin” (event 10).

![Image of search hits with no results]

**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.

![Image of running IEF Triage Timeline]

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

The tool then presents the timeline (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).

![Figure 13 - Viewing correlated artifacts on the IEF Timeline (event 13).](image)

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).

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).

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).

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).

![Search Hits Table]

<table>
<thead>
<tr>
<th>Searched Artifacts</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Related</td>
<td></td>
</tr>
<tr>
<td>Browser Activity</td>
<td>1</td>
</tr>
<tr>
<td>Firefox Bookmarks</td>
<td>1</td>
</tr>
<tr>
<td>Firefox Downloads</td>
<td>1</td>
</tr>
<tr>
<td>Firefox Web History</td>
<td>1</td>
</tr>
<tr>
<td>IE InPrivate/Recovery URLs</td>
<td>12</td>
</tr>
<tr>
<td>Internet Explorer 10-11 Daily/Weekly</td>
<td>3</td>
</tr>
<tr>
<td>Internet Explorer 10-11 Main History</td>
<td>4</td>
</tr>
</tbody>
</table>

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

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

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)
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).

### Table 1: Additional Artifacts

<table>
<thead>
<tr>
<th>#</th>
<th>URL</th>
<th>Description</th>
<th>File Creation Date/Ti.</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><a href="https://www.torpr">https://www.torpr</a></td>
<td>Not Found</td>
<td>05/02/2014 12:02:00</td>
</tr>
<tr>
<td>16</td>
<td><a href="https://www.torproject.org/download/download-easy.html.en">https://www.torproject.org/download/download-easy.html.en</a></td>
<td>Not Found</td>
<td>05/02/2014 12:02:00</td>
</tr>
<tr>
<td>20</td>
<td><a href="https://www.torpl">https://www.torpl</a></td>
<td>Not Found</td>
<td>05/02/2014 12:02:00</td>
</tr>
<tr>
<td>22</td>
<td><a href="https://www.torproject.org/">https://www.torproject.org/</a></td>
<td>Not Found</td>
<td>05/02/2014 12:02:00</td>
</tr>
<tr>
<td>40</td>
<td><a href="https://www.torproject.org/download/download-easy.html.en%E2%80%9D">https://www.torproject.org/download/download-easy.html.en”</a></td>
<td>Not Found</td>
<td>05/02/2014 12:02:00</td>
</tr>
<tr>
<td>41</td>
<td><a href="https://www.torproject.org/donate/thankyou">https://www.torproject.org/donate/thankyou</a></td>
<td>Not Found</td>
<td>05/02/2014 12:02:00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>User</th>
<th>URL</th>
<th>Last Visited Date/Ti.</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>davessmith</td>
<td><a href="https://www.torproject.org/">https://www.torproject.org/</a></td>
<td>05/02/2014 12:14:44</td>
</tr>
<tr>
<td>38</td>
<td>davessmith</td>
<td><a href="https://www.torproject.org/distrbrowser/distr/torbrowser/3.5.1/torbrowser-install-3.5.1_en-US.exe">https://www.torproject.org/distrbrowser/distr/torbrowser/3.5.1/torbrowser-install-3.5.1_en-US.exe</a></td>
<td>05/02/2014 12:14:14</td>
</tr>
<tr>
<td>41</td>
<td>davessmith</td>
<td><a href="https://www.torproject.org/download/download-easy.html.en">https://www.torproject.org/download/download-easy.html.en</a></td>
<td>05/02/2014 12:15:01</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>User</th>
<th>URL</th>
<th>Last Visited Date/Ti.</th>
</tr>
</thead>
</table>
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

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.

Daniel Piggott, Piggott.daniel@gmail.com
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):

<table>
<thead>
<tr>
<th>File</th>
<th>Date</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bookmark</td>
<td>23/03/2014 11:14</td>
<td>Data Base File</td>
<td>0 KB</td>
</tr>
<tr>
<td>Case Information</td>
<td>24/03/2014 22:14</td>
<td>Text Document</td>
<td>9 KB</td>
</tr>
<tr>
<td>IEFCase</td>
<td>25/03/2014 22:14</td>
<td>IEF6 File</td>
<td>22 KB</td>
</tr>
<tr>
<td>Filter</td>
<td>25/03/2014 06:37</td>
<td>Data Base File</td>
<td>1 KB</td>
</tr>
<tr>
<td>IEFv6</td>
<td>25/03/2014 06:37</td>
<td>Data Base File</td>
<td>2,106,305 KB</td>
</tr>
<tr>
<td>Search</td>
<td>25/03/2014 06:37</td>
<td>Data Base File</td>
<td>1 KB</td>
</tr>
<tr>
<td>SearchAlerts</td>
<td>25/03/2014 06:37</td>
<td>Data Base File</td>
<td>1 KB</td>
</tr>
<tr>
<td>logging</td>
<td>25/03/2014 06:37</td>
<td>WinRAR ZIP archive</td>
<td>1 KB</td>
</tr>
</tbody>
</table>

**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).

**Figure 23 - Bitcoin artifact hit (event 23).**

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

**Figure 24 - Bitcoin artifact hit (event 24).**

**Figure 25 - Bitcoin artifact hit (event 25).**

**Figure 26 - Search for Litecoin artifacts (event 26).**
We can see from entering Bitcoin as a search parameter that the forensic tool still gives us other virtual currency artifacts (event 27/28). 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).
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).

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

<table>
<thead>
<tr>
<th>File Type</th>
<th>Date/Time</th>
<th>File Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEFv6</td>
<td>07/04/2014 12:31</td>
<td>4,194,303 KB</td>
</tr>
<tr>
<td>IEFv6.db-shm</td>
<td>07/04/2014 12:26</td>
<td>17,664 KB</td>
</tr>
<tr>
<td>SearchAlerts.db-wal</td>
<td>07/04/2014 12:20</td>
<td>0 KB</td>
</tr>
<tr>
<td>logging</td>
<td>07/04/2014 12:16</td>
<td>1 KB</td>
</tr>
<tr>
<td>IEFv6.db-wal</td>
<td>07/04/2014 12:14</td>
<td>2,310,598 KB</td>
</tr>
<tr>
<td>Case Information</td>
<td>07/04/2014 11:58</td>
<td>12 KB</td>
</tr>
<tr>
<td>IEFCase</td>
<td>07/04/2014 11:58</td>
<td>22 KB</td>
</tr>
</tbody>
</table>

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):
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.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>blocks</td>
<td>05/12/2013 16:14</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>chainstate</td>
<td>05/12/2013 16:13</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>.lock</td>
<td>05/12/2013 16:12</td>
<td>LOCK File</td>
<td>0 KB</td>
</tr>
<tr>
<td>db</td>
<td>05/12/2013 16:12</td>
<td>Text Document</td>
<td>0 KB</td>
</tr>
<tr>
<td>debug</td>
<td>05/12/2013 19:39</td>
<td>Text Document</td>
<td>197 KB</td>
</tr>
<tr>
<td>peers.dat</td>
<td>05/12/2013 19:39</td>
<td>DAT File</td>
<td>2 KB</td>
</tr>
<tr>
<td>wallet.dat</td>
<td>05/12/2013 19:34</td>
<td>DAT File</td>
<td>88 KB</td>
</tr>
</tbody>
</table>

**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 dc798f70c9694a8ccdad1b3dfff087ff91c740b
MD5 Hash of peers.dat fbe71c09d316f156d924cbded62104ea
SHA1 Hash of peers.dat 71ed864680383e05c22ccd4cbbee2f7fd4ba01359

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

Figure 37 - Artifact search for “Litecoin” (event 37).

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.

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).

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

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

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

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 (event 43), we can see what Litecoinlocal.org is and what it can be used for.

Daniel Piggott, Piggott.daniel@gmail.com
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.

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

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

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

**Figure 47 - multiple artifacts showing possible Litecoin transactions (event 47).**
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 6\textsuperscript{th} December 2013, a trade was initiated with a user called lewardington on the website litecoinlocal.org.

Looking at the transaction in more detail the trade was initiated at 20:30:52 on the 6\textsuperscript{th} 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

Daniel Piggott, Piggott.daniel@gmail.com
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


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


Heid, Alex (2013) Analysis Of The Cryptocurrency Marketplace

Daniel Piggott, Piggott.daniel@gmail.com

Couts, Andrew (2013) HOW TO BUY BITCOIN, LITECOIN, AND DOGECOIN  

Kirk, Jeremy (2014) 'Coinkrypt' malware mines cryptocurrencies on Android  

Smith, Chris (2014) Legit Google Play apps found to be covertly mining digital currency  
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 – 7d66b27f9d06aafef618191ab43db95ce8dce2d

Timeline version v6.3.2.0002 – release 02/10/13, file size 902,984
MD5 – 8c7e8c3e1ea6d281c1ced3dc8dce5d86
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 – cca4df067f39ccac017a9eccc9616bf9d
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: addman.cpp
Extract: addman.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
Extract: version_edit_test.cc
Extract: version_set.cc
Extract: version_set.h
Extract: version_set_test.cc
Extract: write_batch.cc
Extract: write_batch_internal.h
Extract: write_batch_test.cc
Output folder: C:\Program Files\Litecoin\src\leveldb\doc
Extract: benchmark.html
Extract: doc.css

Extract: impl.html
Extract: index.html
Extract: log_format.txt
Extract: table_format.txt
Output folder: C:\Program Files\Litecoin\src\leveldb\doc\bench
Extract: db_bench_sqlite3.cc
Extract: db_bench_tree_db.cc
Output folder: C:\Program Files\Litecoin\src\leveldb\helpers
Output folder: C:\Program Files\Litecoin\src\leveldb\helpers\memenv
Extract: memenv.cc

Extract: memenv.h
Extract: memenv_test.cc
Output folder: C:\Program Files\Litecoin\src\leveldb\include
Output folder: C:\Program Files\Litecoin\src\leveldb\include\leveldb
Extract: c.h
Extract: cache.h
Extract: comparator.h
Extract: db.h
Extract: env.h
Extract: filter_policy.h

Extract: iterator.h
Extract: options.h
Extract: slice.h
Extract: status.h
Extract: table.h
Extract: table_builder.h
Extract: write_batch.h
Output folder: C:\Program Files\Litecoin\src\leveldb\issues
Extract: issue178_test.cc
Output folder: C:\Program Files\Litecoin\src\leveldb\port
Extract: README
Extract: atomic_pointer.h
Extract: port.h
Extract: port_example.h
Extract: port_posix.cc
Extract: port_posix.h
Extract: port_win.cc
Extract: port_win.h
Extract: thread_annotations.h
Output folder: C:\Program Files\Litecoin\src\leveldb\port\win

Extract: stdint.h
Output folder: C:\Program Files\Litecoin\src\leveldb\table
Extract: block.cc
Extract: block.h
Extract: block_builder.cc
Extract: block_builder.h
Extract: filter_block.cc
Extract: filter_block.h
Extract: filter_block_test.cc
Extract: format.cc

Extract: format.h
Extract: iterator.cc
Extract: iterator_wrapper.h
Extract: merger.cc
Extract: merger.h
Extract: table.cc
Extract: table_builder.cc
Extract: table_test.cc
Extract: two_level_iterator.cc
Extract: two_level_iterator.h

Output folder: C:\Program Files\Litecoin\src\leveldb\util
Extract: arena.cc
Extract: arena.h
Extract: arena_test.cc
Extract: bloom.cc
Extract: bloom_test.cc
Extract: cache.cc
Extract: cache_test.cc
Extract: coding.cc
Extract: coding.h
Extract: bitcoin_lv_LV.ts
Extract: bitcoin_nb.ts
Extract: bitcoin_nl.ts
Extract: bitcoin_pl.ts
Extract: bitcoin_pt_BR.ts
Extract: bitcoin_pt_PT.ts
Extract: bitcoin_ro_RO.ts
Extract: bitcoin_ru.ts
Extract: bitcoin_sk.ts
Extract: bitcoin_sr.ts

Extract: bitcoin_sv.ts
Extract: bitcoin_th_TH.ts
Extract: bitcoin_tr.ts
Extract: bitcoin_uk.ts
Extract: bitcoin_zh_CN.ts
Extract: bitcoin_zh_TW.ts
Output folder: C:\Program Files\Litecoin\src\qt\res
Extract: bitcoin-qt.rc
Output folder: C:\Program Files\Litecoin\src\qt\res\icons
Extract: add.png

Extract: address-book.png
Extract: bitcoin.icns
Extract: bitcoin.ico
Extract: bitcoin.png
Extract: bitcoin_testnet.icns
Extract: bitcoin_testnet.png
Extract: clock1.png
Extract: clock2.png
Extract: clock3.png
Extract: clock4.png

Extract: clock5.png
Extract: configure.png
Extract: connect0_16.png
Extract: connect1_16.png
Extract: connect2_16.png
Extract: connect3_16.png
Extract: connect4_16.png
Extract: debugwindow.png
Extract: edit.png
Extract: editcopy.png
6.1.5. Litecoin Windows Version 8.6.2 hashes

MD5 hash of Litecoin-qt.exe after install
7a7a4d440e3124f2f7b6f99a998ed3bd

SHA1 hash of Litecoin-qt.exe after install
8bd61b6e27467284afd0e9712bba013444b2086
MD5 hash of *wallet.dat* after install
464676815909de36e5678aa9bd229126

SHA1 hash of *wallet.dat* after install
a67b1687afac2bf050a360ab470468df3a3ce40

MD5 hash of *peers.dat* after install
163536ff7c1fe45e41843f58a2d16b52

SHA1 hash of *peers.dat* after install
f9092ae632b9c4b53024018ad430eabe8267b08d
6.1.6. Litecoin Windows Version 8.6.2 hashes after uninstallation

MD5 hash of wallet.dat after uninstall
4f8957e0405270fca06558b6959ded74

SHA1 hash of wallet.dat after install
88fc79c81818df06b5a7b89bd8ba5b51465e6d6d

MD5 hash of peers.dat after install
163536ff7c1fe45e41843f58a2d16b52

SHA1 hash of peers.dat after install
f9092ae632b9c4b53024018ad430eabe8267b08d
6.1.7. Summary of trades

<table>
<thead>
<tr>
<th>User</th>
<th>Type</th>
<th>Price</th>
<th>Amount</th>
<th>Reference</th>
<th>Created</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>jordem (100%, 21)</td>
<td>Buying</td>
<td>11.42 GPB</td>
<td>100,000,000.00 GPB</td>
<td>LLLLLL7747</td>
<td>2013-12-18 09:33:29</td>
<td>Bought</td>
</tr>
<tr>
<td>ScottJ (100%, 148)</td>
<td>Buying</td>
<td>10.08 GPB</td>
<td>100,000,000.00 GPB</td>
<td>LLLLLL7745</td>
<td>2013-12-18 09:18:12</td>
<td>Cancelled</td>
</tr>
<tr>
<td>ScottJ (100%, 148)</td>
<td>Buying</td>
<td>14.24 GPB</td>
<td>100,000,000.00 GPB</td>
<td>LLLLLL7607</td>
<td>2013-12-17 13:13:22</td>
<td>Cancelled</td>
</tr>
<tr>
<td>Lowwardington (100%, 116)</td>
<td>Buying</td>
<td>21.08 GPB</td>
<td>100,000,000.00 GPB</td>
<td>LLLLLL6279</td>
<td>2013-12-06 20:30:51</td>
<td>Bought</td>
</tr>
</tbody>
</table>

© 2014 litecoinlocal.org Latest trade: Fort Collins, CO, United States, 45 minutes ago.

6.1.8. Detail of first trade id 6279

Trade Status

No action required
Trade complete.

You bought blocks from Lowwardington.

Information from Lowwardington:
Hello! Yes currently -ONLINE- and able to trade. Payment is via bank transfer. Trades will be transacted very FAST-- If your a newbie to cryptocurrency or litecoin in general I'll be more than happy to help with any queries :)

Bank Transfer Information: Bank transfer to: Lewis Ward 09-01-28 502192302
Payment Method: Cash deposit
Cash Trade Information:
Hello! I'm currently -ONLINE- and able to trade. Payment is via bank transfer. Trades will be transacted very FAST-- If your a newbie to cryptocurrency or litecoin in general I'll be more than happy to help with any queries :)

Reference/Message: N/A
Trade: LP: 6279

This trade is complete. You left the feedback very helpful and prompt, thank you.
5 min ago    Lewwardington says: Hello. I'm now back from my short hiatus and able to sell again ;)
5 min ago    Lewwardington says: Received, thankyou!
5 min ago    thestitch says: sure its piggott
5 min ago    Lewwardington says: Hey, sorry for the delay, I was AFK. What's your surname? Just so I can confirm I've received the money!
5 min ago    thestitch says: that's helpful. Payment has been sent.
5 min ago    Lewwardington says: Once the trade is funded, you send me the money via bank transfer. As soon as the money appears in my account I will release the LTC to you)
5 min ago    Lewwardington says: That may answer some questions ;)
5 min ago    Lewwardington says: https://litcoinlocal.org/buyer-guide.php
5 min ago    Lewwardington says: Confirming that escrow is funded ;) thestitch says: ok, what are the confirmations it is waiting for?
5 min ago    Lewwardington says: LTC is on its way to escrow
5 min ago    Lewwardington says: I will fund the escrow now then ;) thestitch says: Yes that is correct
5 min ago    Lewwardington says: You're looking for £300 worth?
5 min ago    Lewwardington says: Hey, welcome!
theStitch says: Newbie, first trade!
6.1.9. Detail of second trade id 7607 – cancelled

Trade Status

No action required
Trade cancelled by Admin.
No more changes can be made to this trade.

You are buying litecoins from ScottJ.

Information from ScottJ:
ONLINE NOW (11am to 11pm, Tuesday 17th December) UK Faster Payments Only please :)

Bank Transfer Information: Faster Payments transfers from UK banks only,
Payment Method: Cash deposit
Cash Trade Information:
ONLINE NOW (11am to 11pm, Tuesday 17th December) UK Faster Payments Only please :)

Reference/message: N/A
Trading: 21.06185445 LTC for 300.00 GBP (14.24 GBP / LTC)
Trade ID: 7607

Upload Pictures (other person can see) (max 3 images, .png, .gif, .jpeg or .jpg)

4 mon ago
thebitch says: found one, bitcointalk.co.uk does litecoins, could you give me tips on how to place my balance on this site in a wallet offline? can't see an option?

4 mon ago
ScottJ says: Just bitcoins?

4 mon ago
thebitch says: ok, does that do buy/sell litecoins as well? or just bitcoins?

4 mon ago
ScottJ says: Currently I have to do it myself, which, as you've experienced, isn't a great process.

4 mon ago
ScottJ says: On localbitcoins.com the site does the ID verification, which makes it a lot easier

4 mon ago
ScottJ says: Yes, this is something they are working on

4 mon ago
thebitch says: maybe there is an opportunity for the site to verify sellers and buyers

4 mon ago
ScottJ says: I'm afraid so, sorry about that

4 mon ago
thebitch says: If it is a problem for you, do we agree to cancel the trade?

4 mon ago
ScottJ says: By showing me that you have the card linked to the account, I can safely presume that you own it. Otherwise people could use my service to buy litecoins from hackable bank account.

4 mon ago
thebitch says: yes I do understand that with escrow it's between. so uk to uk bank account under uk law should be sufficient.

4 mon ago
ScottJ says: If you were to email your card with the long number obscured, this is the exact same information I will be getting.

4 mon ago
ScottJ says: account number, sort-code, name on account

4 mon ago
ScottJ says: To me, I get the following information:

4 mon ago
thebitch says: That won't work I'm afraid.

4 mon ago
thebitch says: and then telling you the name of the account it's from (surname)

4 mon ago
thebitch says: I wouldn't do that in any electronic transaction especially on the net. I am making payment from a UK bank account to escrow

4 mon ago
ScottJ says: Simplest way is just to take a photo of your bank card (hiding your long number for security)

4 mon ago
thebitch says: hi, on last trade I made payment to escrow then gave name of account it came from, is that ok? It's a UK bank account.

4 mon ago
ScottJ says: Most people sent a photo of part of their bank statement or card, with sensitive bits hidden/blurred

4 mon ago
ScottJ says: And are you able to provide some basic ID, just something that matches the name on your bank account.

4 mon ago
ScottJ says: Will you be sending from a UK bank account?

4 mon ago
ScottJ says: Hello
thebitch says: Hello, like to purchase 300GBP worth
6.1.10. Detail of third trade id 7743 – cancelled

No action required
Trade cancelled by Admin.
No more changes can be made to this trade.

You are buying litecoins from ScottJ.

Information from ScottJ:
ONLINE NOW (11am to 11pm, Tuesday 17th December) UK Faster Payments Only please :)
Bank Transfer Information: Faster Payments transfers from UK banks only,
Payment Method: Cash deposit
Cash Transfer Information:
ONLINE NOW (11am to 11pm, Tuesday 17th December) UK Faster Payments Only please :)
Reference/message: N/A
Trading: 29.76565499 LTC for 300.00 GBP (10.08 GBP / LTC)
Trade ID: 7743

6.1.11. Detail of fourth trade id 7747 and user

Viewing user profile for ScottJ

Trade Feedback for ScottJ

Add Feedback

6.1.11. Detail of fourth trade id 7747 and user

Daniel Piggott, Piggott.daniel@gmail.com
Trade Status

No action required
Trade complete.

You bought litecoins from jpsdesign.

Information from jpsdesign:
Hi, I am currently online and can trade quickly! Payment is via bank transfer or Barclays Pingit....

Bank Transfer Information: Barclays JP Skinner 60461857 20-96-55
Payment Method: Bank wire (SWIFT)
Cash Trade Information:
Hi, I am currently online and can trade quickly! Payment is via bank transfer or Barclays Pingit....

Reference/message: LLLLL7747
Trading: 26.37791700 LTC for 300.00 GBP (11.42 GBP / LTC)
Trade ID: 7747

This trade is complete. You left the feedback: A-

Chat

Your message...

Send Message

4 min ago thestitch says: escrow received and payment made, thks
4 min ago jpsdesign says: Funds released - thanks for the trade and have a good day!
4 min ago jpsdesign says: All done - usually takes a few minutes for the 8 confirmations to go through...
4 min ago thestitch says: great, thks
4 min ago jpsdesign says: Hi there no problem, will fund escrow now!
4 min ago thestitch says: hello, like to buy
6.1.12. Detail of authors user id and trades

Viewing user profile for jpsdesign

<table>
<thead>
<tr>
<th>Info</th>
<th>Trade Feedback for jpsdesign</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username: jpsdesign</td>
<td>Username: jpsdesign</td>
</tr>
<tr>
<td>Total Trades: 26</td>
<td>Total Trades: 26</td>
</tr>
<tr>
<td>Positive Trades: 21</td>
<td>Positive Trades: 21</td>
</tr>
<tr>
<td>Negative Trades: 0</td>
<td>Negative Trades: 0</td>
</tr>
<tr>
<td>Last Active: 2609 years ago</td>
<td>Last Active: 2609 years ago</td>
</tr>
<tr>
<td>Total LTC Volume: 211.1264625</td>
<td>Total LTC Volume: 211.1264625</td>
</tr>
</tbody>
</table>

This user has never been reported

- **Trade Feedback for jpsdesign**
  - Username: jpsdesign (100%, 26) Positive: Great patient buyer :) 
  - jpsdesign (100%, 5) Positive: after a few battery problems which was not his fault- a smooth transaction. Thanks
  - HMMVgot (100%, 1) Positive: fast and honest transaction
  - HMMVgot (100%, 1) Positive: great, fast and secure
  - Utracko (100%, 70) Positive: Excellent seller, good comms and fast release of coins.+++++
  - lightcoin (50%, 1) Positive: fast trader thanks
  - Invokes (100%, 1) Positive: Very professional. Great seller!
  - ceng (100%, 1) Positive: Quick release of funds. A++ seller
  - dpcc (100%, 5) Positive: Thanks for a great first experience buying Litecoin!
  - Invokes (100%, 2) Positive: This was my first transfer, this guy was very helpful and was quick replying to messages.
  - thestitch (100%, 1) Positive: A++
  - maw (100%, 1) Positive: A++

Viewing user profile for thestitch

<table>
<thead>
<tr>
<th>Info</th>
<th>Trade Feedback for thestitch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username: thestitch</td>
<td>Username: thestitch</td>
</tr>
<tr>
<td>Total trades: 2</td>
<td>Total trades: 2</td>
</tr>
<tr>
<td>Positive Trades: 1</td>
<td>Positive Trades: 1</td>
</tr>
<tr>
<td>Negative Trades: 0</td>
<td>Negative Trades: 0</td>
</tr>
<tr>
<td>Last Active: 1 second ago</td>
<td>Last Active: 1 second ago</td>
</tr>
<tr>
<td>Total LTC Volume: 40.506825</td>
<td>Total LTC Volume: 40.506825</td>
</tr>
</tbody>
</table>

This user has never been reported

- **Trade Feedback for thestitch**
  - jpsdesign (100%, 21) Positive: Very prompt payment, a pleasure to deal with, great buyer!
6.1.13. Email trail of trades from litecoinlocal.org

You have started a trade with Lewwardington

From: noreply@litecoinlocal.org (noreply@litecoinlocal.org)
To: dtm.p@hotmail.co.uk

I trust noreply@litecoinlocal.org. Always show content.

Hello,

You have initiated a trade with Lewwardington. View trade progress or message the seller at https://LitecoinLocal.org.

Sincerely,

The LitecoinLocal Team

Daniel Piggott, Piggott.daniel@gmail.com
New message from Lewwardington about your trade

From: noreply@litecoinlocal.org  
Sent: 09 December 2013 15:46:49  
To:  

Hello,

You received a new message from Lewwardington about your trade.
Visit https://litecoinlocal.org/viewtrade.php?id=6279 to view it.

Sincerely,

The LitecoinLocal Team

You have started a trade with ScottJ

From: noreply@litecoinlocal.org  
To:  

Hello,

You have initiated a trade with ScottJ. View trade progress or message the seller at https://LitecoinLocal.org.

Sincerely,

The LitecoinLocal Team
New message from ScottJ about your trade

From: noreply@litecoinlocal.org
Sent: 17 December 2013 13:15:20
To: [removed]

Hello,

You received a new message from ScottJ about your trade. Visit https://litecoinlocal.org/viewtrade.php?id=7607 to view it.

Sincerely,

The Litecoin Local Team

Same message 17/12/13 13:15:32
Same message 17/12/13 13:15:38
Same message 17/12/13 13:15:44
Same message 17/12/13 14:17:57
Same message 17/12/13 14:18:53
Same message 17/12/13 14:22:54
Same message 17/12/13 14:23:26
Same message 17/12/13 14:24:02
Same message 17/12/13 14:24:15
Same message 17/12/13 14:24:25
Same message 17/12/13 14:25:39
Same message 17/12/13 14:26:23
Same message 17/12/13 14:26:38

Daniel Piggott, Piggott.daniel@gmail.com
Your trade with ScottJ is canceled

From: noreply@litecoinlocal.org
Sent: 17 December 2013 14:29:25
To: 

Hello,

Your trade with ScottJ is now cancelled.

Sincerely,

The LitecoinLocal Team

New message from ScottJ about your trade

From: noreply@litecoinlocal.org
Sent: 17 December 2013 14:32:07
To: 

Hello,

You received a new message from ScottJ about your trade. Visit https://litecoinlocal.org/viewtrade.php?id=7607 to view it.

Sincerely,

The LitecoinLocal Team

Same message 17/12/13 14:33:06

Same message 17/12/13 14:33:52

Daniel Piggott, Piggott.daniel@gmail.com
Your trade with ScottJ is canceled

From: noreply@litecoinlocal.org
Sent: 18 December 2013 08:21:42
To: [REDACTED]

Hello,

Your trade with ScottJ is now cancelled.

Sincerely,

The LitecoinLocal Team
You have started a trade with jpsdesign

From: noreply@litecoinlocal.org  
Sent: 18 December 2013 09:33:31  
To: [REDACTED]

Hello,

You have initiated a trade with jpsdesign. View trade progress or message the seller at https://LitecoinLocal.org.

Sincerely,

The LitecoinLocal Team

New message from jpsdesign about your trade

From: noreply@litecoinlocal.org  
Sent: 18 December 2013 09:34:44  
To: [REDACTED]

Hello,

You received a new message from jpsdesign about your trade. Visit https://litecoinlocal.org/viewtrade.php?id=7747 to view it.

Sincerely,

The LitecoinLocal Team

Same message 18/12/13 09:41:37

Daniel Piggott, Piggott.daniel@gmail.com
Escrow for your trade with jpsdesign is funded

From: noreply@litecoinlocal.org
Sent: 18 December 2013 10:06:04
To: [REDACTED]

Hello,

Your trade with jpsdesign is fully funded.

Sincerely,

The LitecoinLocal Team

Your trade with jpsdesign is complete

From: noreply@litecoinlocal.org
Sent: 18 December 2013 10:13:31
To: [REDACTED]

Hello,

Your trade with jpsdesign is now complete. Please remember to leave feedback at https://litecoinlocal.org/viewtrade.php?id=7747.

Sincerely,

The LitecoinLocal Team
New message from jpsdesign about your trade

From: noreply@litecoinlocal.org
Sent: 18 December 2013 10:13:52
To: 

Hello,

You received a new message from jpsdesign about your trade. Visit https://litecoinlocal.org/viewtrade.php?id=7747 to view it.

Sincerely,

The LitecoinLocal Team

6.1.14. Forensic Tool Log for Scenario 1 laptop

IEF Triage 6.3.0.0021
Copyright 2009-2014 Magnet Forensics® Inc.
Build 6.3.0.0021
Case Information Generated At: 03/16/2014 10:56:33
Operating System: Microsoft Windows NT 6.2.9200.0

Selected source:
------------------
PhysicalDrive0 - Partition 1 (Microsoft NTFS, 450 MB) System

Searches selected:
------------------
pagefile.sys
swapfile.sys

Daniel Piggott, Piggott.daniel@gmail.com
$MFT
$LogFile
hiberfil.sys
Volume Shadow Copies
Unallocated Clusters
File Slack Space
All Files and Folder
Uninitialized File Area

Selected source:
------------------
PhysicalDrive0 - Partition 2 (Microsoft FAT32, 260 MB) NO NAME

Searches selected:
------------------
Unallocated Clusters
File Slack Space
All Files and Folder

Selected source:
------------------
PhysicalDrive0 - Partition 3 (Microsoft NTFS, 128 MB)

Searches selected:
------------------
pagefile.sys
swapfile.sys
$MFT
$LogFile
hiberfil.sys
Volume Shadow Copies
Unallocated Clusters
File Slack Space

Daniel Piggott, Piggott.daniel@gmail.com
All Files and Folder
Uninitialized File Area

Selected source:
------------------
PhysicalDrive0 - Partition 4 (Microsoft NTFS, 100.38 GB) TI31036500A [C:]

Searches selected:
------------------
pagefile.sys
swapfile.sys
$MFT
$LogFile
hiberfil.sys
Volume Shadow Copies
Unallocated Clusters
File Slack Space
All Files and Folder
Uninitialized File Area

Selected source:
------------------
PhysicalDrive0 - Partition 5 (Microsoft NTFS, 350 MB)

Searches selected:
------------------
pagefile.sys
swapfile.sys
$MFT
$LogFile
hiberfil.sys
Volume Shadow Copies
Unallocated Clusters
File Slack Space
All Files and Folder
Uninitialized File Area

Selected source:
------------------
PhysicalDrive0 - Partition 6 (Microsoft NTFS, 9.71 GB) Recovery

Searches selected:
------------------
pagefile.sys
swapfile.sys
$MFT
$LogFile
hiberfil.sys
Volume Shadow Copies
Unallocated Clusters
File Slack Space
All Files and Folder
Uninitialized File Area

Selected source:
------------------
PhysicalDrive0 - Partition 7 (8 GB)

Searches selected:
------------------
Sector Level

Selected source:
------------------
PhysicalDrive0 - Unpartitioned Space
Searches selected:

------------------
Unpartitioned Space

Search items selected:

----------------------
Platform: Computer
----------------------
AIM
Adium
Ares
BeBo
Bing Bar
Bitcoin
Browser Activity
Carbonite
Chatroulette
Chrome
Dropbox
Emule
Facebook Chat
Facebook Email
Facebook Email 'Snippets'
Facebook Pictures
Facebook Status Updates / Wall Posts / Comments
Facebook Web Page Fragments
Firefox
Flash Cookies
Flash Video Fragments
Flickr
Frostwire.props Files
Gigatribe
Gmail
Google Bar
Google Maps
Google Plus
Google Talk
GoogleDocs
GoogleDrive
Hotmail
Hushmail
ICQ
IRC
Instagram
Internet Explorer 10-11 History
Internet Explorer v5-9
Internet Explorer v7-v10 InPrivate/Recovery URLs
LINE Pictures
Limerunner
Limewire searches (v5.2.8 - v5.5.16)
Limewire shared Files
Limewire.props Files
Limewire®/Frostwire® 4.x.x Searches
LinkedIn
Luckywire
Mail.ru Chat
Mailinator
Messenger Plus
MySpace
Omeagle
Oovoo
Opera
Outlook Webmail
Pal Talk
Pictures
Pidgin
QQ Chat
RebuildWeb
Safari
SafeBrowser
Second Life
Shareaza
Sina Weibo
SkyDrive
Skype
TorChat
Torrent
Trillian
Twitter
Usenet
Videos
WeChat
Webpage Recovery
Windows Live Messenger
WoW
XBox Internet Explorer History
Yahoo Mail
Yahoo! Messenger - Non-encrypted Chat
Yahoo! Messenger Chat
Yahoo! Messenger Diagnostic Logs
Yahoo! Messenger Group Chat
Yahoo! Webmail Chat
iChat
iMessage
iOS Backups

------------
Output folder: D:\IEF - Mar 16 2014 105609\
Start time: Mar 16, 2014 10:56:33

End time: Mar 16, 2014 14:38:54

Duration: 03:42:21

Final results of search:

Pictures: 60690 items
Pictures_DATA: 60690 items
Browser Activity: 7505 items
Flash Cookies: 6 items
Carved Video: 311 items
Carved Video_DATA: 311 items
Cloud Services URLs: 6 items
Social Media URLs: 5 items
Videos: 802 items
Facebook URLs: 12 items
Parsed Search Queries: 10 items
Malware/Phishing URLs: 31 items
Safari Bookmarks: 2 items
Pornography URLs: 2 items
QQ: 2 items
Internet Explorer 10-11 Content: 104 items
Internet Explorer 10-11 Main History: 50 items
Internet Explorer 10-11 Daily/Weekly History: 29 items
Facebook Chat: 103 items
Firefox Downloads: 2 items
Firefox Bookmarks: 9 items
Firefox FavIcons: 2 items
Firefox Web History: 2 items
IE InPrivate/Recovery URLs: 73 items
6.1.15. Forensic Tool Log for Scenario 2 laptop

IEF Triage 6.3.2.0005
Copyright 2009-2014 Magnet Forensics® Inc.
Build 6.3.2.0005
Case Information Generated At: 03/23/2014 12:14:06
Operating System: Microsoft Windows NT 6.1.7601 Service Pack 1

Selected source:
------------------
PhysicalDrive0 - Partition 1 (Microsoft NTFS, 100 MB) System Reserved

Searches selected:
------------------
pagefile.sys
swapfile.sys
$MFT
$LogFile
hiberfil.sys
Volume Shadow Copies
Unallocated Clusters
File Slack Space
All Files and Folder
Uninitialized File Area

Selected source:
------------------
PhysicalDrive0 - Partition 2 (Microsoft NTFS, 297.99 GB) [C:\]

Searches selected:
------------------
pagefile.sys

Daniel Piggott, Piggott.daniel@gmail.com
swapfile.sys
$MFT
$LogFile
hiberfil.sys
Volume Shadow Copies
Unallocated Clusters
File Slack Space
All Files and Folder
Uninitialized File Area

Selected source:

-----------
PhysicalDrive0 - Unpartitioned Space

Searches selected:

-----------
Unpartitioned Space

Search items selected:

-----------
Platform: Computer

-----------
Adium
AIM
Ares
BeBo
Bing Bar
Bitcoin
Browser Activity
Carbonite
Chatroulette
Chrome
Dropbox
Emule
Facebook Chat
Facebook Email
Facebook Email 'Snippets'
Facebook Pictures
Facebook Status Updates / Wall Posts / Comments
Facebook Web Page Fragments
Firefox
Flash Cookies
Flash Video Fragments
Flickr
Frostwire.props Files
Gigatribe
Gmail
Google Bar
Google Maps
Google Plus
Google Talk
GoogleDocs
GoogleDrive
Hotmail
Hushmail
iChat
ICQ
iMessage
Instagram
Internet Explorer 10-11 History
Internet Explorer v5-9
Internet Explorer v7-v10 InPrivate/Recovery URLs
iOS Backups
IRC
Limerunner
Limewire searches (v5.2.8 - v5.5.16)
Limewire shared Files
Limewire.props Files
Limewire®/Frostwire® 4.x.x Searches
LINE Pictures
LinkedIn
Luckywire
Mail.ru Chat
Mailinator
Malware/Phishing sites
Messenger Plus
MySpace
Omegle
Oovoo
Opera
Outlook Webmail
Pal Talk
Pictures
Pidgin
Pornography sites
QQ Chat
RebuildWeb
Safari
SafeBrowser
Second Life
Shareaza
Sina Weibo
SkyDrive
Skype
TorChat
Torrent
Trillian
Twitter
Usenet

Daniel Piggott, Piggott.daniel@gmail.com
Videos
Webpage Recovery
WeChat
Windows Live Messenger
WoW
XBox Internet Explorer History
Yahoo Mail
Yahoo! Messenger - Non-encrypted Chat
Yahoo! Messenger Chat
Yahoo! Messenger Diagnostic Logs
Yahoo! Messenger Group Chat
Yahoo! Webmail Chat

------------------------
Output folder: E:\IEF - Mar 23 2014 121338\
------------------------

---------------------------------
Start time: Mar 23, 2014 12:14:06
---------------------------------

---------------------------------
End time: Mar 24, 2014 23:14:46
---------------------------------

---------------------------------
Duration: 1 days 11:00:40
---------------------------------

Final results of search:

---------------------------------
Browser Activity: 14517 items

---------------------------------
Pictures: 52174 items
Pictures_DATA: 52174 items
Cloud Services URLs: 5 items
Malware/Phishing URLs: 25 items
Internet Explorer 10-11 Content: 12678 items
Ares Search Keywords: 10 items
Internet Explorer 10-11 Main History: 2217 items
Parsed Search Queries: 1371 items
Facebook URLs: 632 items
Skype IP Addresses: 17 items
Internet Explorer 10-11 Daily/Weekly History: 504 items
IE InPrivate/Recovery URLs: 1245 items
Social Media URLs: 879 items
Skype Calls Carved: 4 items
Skype Chat Messages: 67 items
Classifieds URLs: 1042 items
Facebook Pages: 22 items
Google Maps: 1 items
Carved Video: 788 items
Carved Video_DATA: 788 items
Internet Explorer Typed URLs: 7 items
Videos: 164 items
Bitcoin Addresses: 1 items
Internet Explorer Cache Records Carved: 2337 items
Internet Explorer Redirect Records: 36 items
Internet Explorer PrivacIE Records: 473 items
Internet Explorer Leak Records: 6 items
Torrent URLs: 4 items
Internet Explorer Main History: 177 items
Internet Explorer Daily History: 66 items
Internet Explorer Cookie Records: 75 items
Skype Calls - djpiggott: 1 items
Skype Accounts - djpiggott: 1 items

Daniel Piggott, Piggott.daniel@gmail.com
Skype Group Chat - djpiggott: 2 items
Skype Contacts - djpiggott: 17 items
Internet Explorer Cookies: 152 items
Internet Explorer 10-11 Downloads: 5 items
Internet Explorer Cache Records: 20 items
Rebuilt Webpages: 1 items
Skype Chatsync Messages: 1 items
Internet Explorer 10-11 Cookies: 62 items
Skype Chatsync Messages Carved: 4 items
6.1.16. Forensic Tool Log for Scenario 3 laptop

IEF Standard 6.3.2.0002
Copyright 2009-2014 Magnet Forensics® Inc.
Build 6.3.2.0002
Case Information Generated At: 04/04/2014 14:27:24
Operating System: Microsoft Windows NT 6.1.7601 Service Pack 1

Selected source:
------------------
PhysicalDrive0 - Partition 1 (Microsoft NTFS, 141.55 GB) TI102717P0A [C:\]

Searches selected:
------------------
pagfile.sys
swapfile.sys
$MFT
$LogFile
hiberfil.sys
Volume Shadow Copies
Unallocated Clusters
File Slack Space
All Files and Folder
Uninitialized File Area

Selected source:
------------------
PhysicalDrive0 - Unpartitioned Space

Searches selected:
------------------
Unpartitioned Space
Search items selected:

Platform: Computer

Adium
AIM
Ares
BeBo
Bing Bar
Bitcoin
Browser Activity
Carbonite
Chatroulette
Chrome
Dropbox
Emule
Facebook Chat
Facebook Email
Facebook Email 'Snippets'
Facebook Pictures
Facebook Status Updates / Wall Posts / Comments
Facebook Web Page Fragments
Firefox
Flash Cookies
Flash Video Fragments
Flickr
Frostwire.props Files
Gigatribe
Gmail
Google Bar
Google Maps
Google Plus
Google Talk
GoogleDocs
GoogleDrive
Hotmail
Hushmail
iChat
ICQ
iMessage
Instagram
Internet Explorer 10-11 History
Internet Explorer v5-9
Internet Explorer v7-v10 InPrivate/Recovery URLs
IRC
Limerunner
Limewire searches (v5.2.8 - v5.5.16)
Limewire shared Files
Limewire.props Files
Limewire®/Frostwire® 4.x.x Searches
LINE Pictures
LinkedIn
Luckywire
Mail.ru Chat
Mailinator
Malware/Phishing sites
Messenger Plus
MySpace
Omegle
Oovoo
Opera
Outlook Webmail
Pal Talk
Pictures
Pidgin

Daniel Piggott, Piggott.daniel@gmail.com
Pornography sites
QQ Chat
RebuildWeb
Safari
SafeBrowser
Second Life
Shareaza
Sina Weibo
SkyDrive
Skype
TorChat
Torrent
Trillian
Twitter
Usenet
Videos
Webpage Recovery
WeChat
Windows Live Messenger
WoW
XBox Internet Explorer History
Yahoo Mail
Yahoo! Messenger - Non-encrypted Chat
Yahoo! Messenger Chat
Yahoo! Messenger Diagnostic Logs
Yahoo! Messenger Group Chat
Yahoo! Webmail Chat

--------------
Output folder: G:\IEF - Apr 04 2014 142657\
--------------

Daniel Piggott, Piggott.daniel@gmail.com
Start time: Apr 04, 2014 14:27:22

End time: Apr 07, 2014 11:57:55

Duration: 2 days 21:30:33

Final results of search:

Browser Activity: 41318 items
Pictures: 198286 items
Pictures_DATA: 198286 items
Parsed Search Queries: 19733 items
Malware/Phishing URLs: 21 items
Flash Cookies: 549 items
Gmail Fragments: 104 items
Limewire.props Files: 29 items
Hotmail Webmail: 268 items
AIM: 71 items
Safari History Carved: 3 items
Facebook Chat: 94 items
Facebook URLs: 2604 items
Google Maps Tiles: 409 items
Carved Video: 2329 items
Carved Video_DATA: 2329 items
Videos: 311 items
Internet Explorer Privacy Records: 878 items
Social Media URLs: 12314 items
Firefox Web History: 7137 items
Firefox FormHistory: 546 items
Firefox SessionStore Artifacts: 1023 items
Classifieds URLs: 2583 items
Google Maps: 345 items
Ares Search Keywords: 113 items
Internet Explorer Cookie Records: 137 items
Facebook Pictures: 6 items
Facebook Pictures_DATA: 0 items
Web Video Fragments: 7 items
Web Video Fragments_DATA: 7 items
Skype Calls Carved: 14 items
Internet Explorer Typed URLs: 11 items
Opera Web History: 4 items
Facebook Pages: 128 items
Bebo: 39 items
Yahoo! Webmail: 23 items
Internet Explorer Cookies: 284 items
Chrome/360 Safe Browser Carved Web History: 9768 items
IE InPrivate/Recovery URLs: 2269 items
Bitcoin Addresses: 1 items
Skype IP Addresses: 49 items
Firefox Cookies: 4124 items
Firefox Input History: 58 items
Firefox Downloads: 20 items
Firefox Bookmarks: 190 items
Firefox FavIcons: 662 items
Torrent URLs: 68 items
SkyDrive: 5 items
Google Drive Desktop App: 18 items
Safari Bookmarks: 52 items
Skype Chat Messages: 191 items
Skype Voicemails - djpiggott: 1 items
Skype Calls - djpiggott: 26 items
Skype Accounts - djpiggott: 1 items

Daniel Piggott, Piggott.daniel@gmail.com
Skype Group Chat - djpiggott: 7 items
Skype Contacts - djpiggott: 16 items
Google Toolbar: 30 items
Internet Explorer Main History: 173 items
Internet Explorer Cache Records: 3679 items
Rebuilt Webpages: 844 items
Internet Explorer Cache Records Carved: 3801 items
Google Maps Queries: 62 items
Internet Explorer Leak Records: 6 items
Internet Explorer Redirect Records: 87 items
Facebook Status Updates/Wall Posts/Comments: 44 items
Internet Explorer 10-11 Main History: 13902 items
Internet Explorer 10-11 Daily/Weekly History: 6549 items
Internet Explorer 10-11 Content: 51567 items
Internet Explorer 10-11 Downloads: 1 items
Internet Explorer 10-11 Cookies: 8 items
Cloud Services URLs: 64 items
Dating Sites URLs: 14 items
Internet Explorer Weekly History: 37 items
Internet Explorer Daily History: 83 items
Chrome Cookies: 1307 items
Chrome Bookmarks: 2 items
Chrome Current Session: 2 items
Chrome Current Tabs: 1 items
Chrome FavIcons: 1140 items
Chrome Web History: 1427 items
Chrome Last Session: 22 items
Chrome Last Tabs: 17 items
Chrome Logins: 7 items
Chrome Keyword Search Terms: 180 items
Chrome Downloads: 22 items
Chrome Top Sites: 20 items
Chrome Autofill: 548 items

Daniel Piggott, Piggott.daniel@gmail.com
Google Drive: 1 items
Skype Chatsync Messages: 5 items
Chrome Cache Records: 7995 items
Firefox Cache Records: 9123 items
Twitter: 20 items
LinkedIn Emails: 7 items
MSN Plus!: 7 items
Opera Search Field History: 1 items
Chrome/360 Safe Browser Carved Session/Tabs: 18 items
Chatroulette: 2 items
Google+ Chat: 2 items
Skype Chatsync Messages Carved: 3 items
# Upcoming SANS Forensics Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>South by Southeast Asia Online 2020</td>
<td>Singapore</td>
<td>Aug 03, 2020 - Aug 14, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 3 MT</td>
<td>CA</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
</tr>
<tr>
<td>SANS Special Investigations 2020</td>
<td>United Arab Emirates</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Reboot - NOVA 2020 - Live Online</td>
<td>Arlington, VA</td>
<td>Aug 10, 2020 - Aug 15, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>FOR498 Australia Live Online 2020</td>
<td>Australia</td>
<td>Aug 10, 2020 - Aug 15, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS FOR508 Sydney August 2020</td>
<td>Sydney, Australia</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Summer Forensics Europe 2020</td>
<td>United Arab Emirates</td>
<td>Aug 17, 2020 - Aug 28, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 17 ET</td>
<td>DC</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
</tr>
<tr>
<td>Cyber Defence APAC Live Online 2020</td>
<td>Singapore</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 24 MT</td>
<td>CA</td>
<td>Aug 24, 2020 - Aug 29, 2020</td>
</tr>
<tr>
<td>SANS Virginia Beach 2020</td>
<td>Virginia Beach, VA</td>
<td>Aug 30, 2020 - Sep 04, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2020 - Live Online</td>
<td>Virginia Beach, VA</td>
<td>Aug 30, 2020 - Sep 04, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Japan Bi-Lingual Live Online</td>
<td>Japan</td>
<td>Aug 31, 2020 - Sep 05, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS London September 2020</td>
<td>London, United Kingdom</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2020</td>
<td>Manila, Philippines</td>
<td>Sep 07, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2020 - Live Online</td>
<td>London, United Kingdom</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020 - Live Online</td>
<td>Baltimore, MD</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020</td>
<td>Baltimore, MD</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response Summit &amp; Training 2020</td>
<td>Virtual - US Eastern,</td>
<td>Sep 10, 2020 - Sep 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Munich September 2020</td>
<td>Munich, Germany</td>
<td>Sep 14, 2020 - Sep 19, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Munich September 2020</td>
<td>Munich, Germany</td>
<td>Sep 14, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Network Security 2020 - Live Online</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Australia Spring 2020 - Live Online</td>
<td>Australia</td>
<td>Sep 21, 2020 - Oct 03, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Australia Spring 2020</td>
<td>Australia</td>
<td>Sep 21, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Antonio Fall 2020</td>
<td>San Antonio, TX</td>
<td>Sep 28, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Antonio Fall 2020 - Live Online</td>
<td>San Antonio, TX</td>
<td>Sep 28, 2020 - Oct 03, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Northern VA - Reston Fall 2020</td>
<td>Reston, VA</td>
<td>Sep 28, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
</tbody>
</table>