Computer Forensic Investigative Analysis Report (CFIAR)

Incident Report Number	**[2019-11-03, II, 1.0]**
Reported Incident Date	**Not Provided**

Examiner(s)	**Group 05** **Emma Francke emfr8571@student.su.se** **Vivek Rao vira3085@student.su.se** **Denise Jonsson dejo4698@student.su.se**
Requester(s)	**The Super Secret Police**
Suspected Offence	**Fraud, Counterfeit**
Investigation hours	**120 hours**

Case Evgeny Gachev

Evgeny Gachev was suspected to have committed counterfeit and fraud under the alias lucky12345. The Super Secret Police has requested the digital forensic group to conduct a forensic investigation of the acquired hard drive image. The physical hard drive was already acquired by the first responder who was in-charge of house search. The evidence hard drive image was acquired in a raw format using an Image MASSter Solo 4 forensic acquisition device. The digital forensic group was also handed the pre-processed EnCase evidence file (.E01).

Objective: To search for evidence that directly or indirectly indicates activities related to fraud and/or counterfeit by the subject
Computer type: Not specified
Operating system: Windows 7 Professional v6.1, Product ID: 00371-868-0000007-85582
Offense: Fraud, Counterfeit
Case agent: Emma Francke emfr8571@student.su.se, Vivek Rao vira3085@student.su.se, Denise Jonsson dejo4698@student.su.se
Evidence number: #1234567
Where examination took place: CS2Lab at Stockholm University, Department of Computer and System Sciences (DSV), Borgarfjordsgatan 12(Nod Building), Stockholm, Sweden.
Tools used: FTK Imager, FTK Registry Viewer, EnCase Forensic, Windows Event Viewer, Prefetch Parser v1.4, HexEdit

Processing

Identification:

1. The EnCase evidence file (ending in .E01) was provided to the case agents by the requester.

2. The requester is authorized to submit the digital evidence to the case agents for the purpose of digital forensic investigation.

3. Since the hash values (i.e. MD5, SHA1) were provided along with the evidence files, the integrity was verified. Also, the evidence files were authenticated.

4. A list of tools and procedures were suggested to initiate the investigation.

5. A list of system related, and case specific questions were stated in the request by the requester.

Acquisition:

1. The two evidence files (including raw image file and EnCase evidence file, .E01) were already

acquired by the requester.

2. The EnCase evidence file (ending in .E01) was considered by the digital forensic examiners to be the primary source of artefacts.

3. The EnCase evidence file was located at C:\CS2Lab\DIFO_Lab_Files\DiFo_Lab_2_E01 folder.

4. The MD5 hash value of the Encase evidence file (ending in .E01) was already stated in the request.

5. The Windows command-line utility was utilized to run the hashing tool, md5deep64.exe to verify the integrity and subsequently authenticate the primary evidence for this case.

6. The MD5 hash value computed by md5deep64.exe was "e6dc38a4f429107296699901 38f86265".

7. The Linux "dd" command was utilized to create a forensic copy of the original evidence (i.e. EnCase evidence file)

8. The hash value of the forensic copy was computed by utilizing the tool, md5deep64.exe, which was verified and hence the forensic copy was authenticated.

Examination:

1. The investigation initiated by examining the file structure of the forensic copy using the tool, EnCase forensic.

2. The first sector of the hard disk drive was analysed and extract information about the partition table.

3. The disk image of the forensic copy was viewed and analysed.

4. Using Access Data's FTK registry viewer, the registry hives were analysed to extract information about user accounts, installed programs, uninstalled programs, operating system, system configuration and web browsing artefacts.

5. Subsequently, the forensic copy was subject to additional processing via EnCase Forensic tool in order to confirm and verify the findings.

6. The Windows Event Viewer was utilized to conduct a temporal forensic analysis related to events.

7. Hex Editor tool was utilized to interpret the page file (i.e. pagefil.sys).

8. The payload of the electronic communication via e-mail clients were also extracted by means of

additional processing.

9. The forensic copy was also subjected to keyword searching in order to get hits of interest.

Documentation and reporting:

1. The findings were documented in respective files which were saved in the local repository.
2. The examination phase culminated on the 2019-10-22.
3. The Computer Forensic Investigative Analysis Report (CFIAR) was created from the content of the local repository and handed over to the requester on the 2019-11-03.

Case Evgeny Gachev brief report

REPORT OF Requested Windows Forensics Investigation

MEMORANDUM FOR: *The Super Secret Police*
Stockholm, Sweden.

SUBJECT: *Forensic Media Analysis Report*
SUBJECT: Gachev, Evgeny
Case Number: 012345

1. **Status: Closed.**

2. **Summary of Findings:**

Prefetch files as obtained under C:\Windows\Prefetch can be found at the end of this summary under the title “Appendix A”.

Link files as obtained which indicate possible interaction with the mentioned files by the user can be found under the title “Appendix B” at the end of this document.

Both appendix A and appendix B serve as an explanation and as further evidence for those interested in further reading regarding prefetched files and link files.

3. Items Analysed:

TAG NUMBER:	**ITEM DESCRIPTION:**
012345	*EnCase evidence file, DiFo_Lab_2_E01.E01*

4. Details of Findings:

Findings in this paragraph relate to the results obtained from the forensic copy:

1. File system: The file system identified was NTFS and the number of sectors were 88 162 304 with 512 bytes per sector divided into 8 clusters. Allocated bytes were 36 690 026 496 (34,2 GB) and unallocated bytes were 8 449 069 0556 (7,9 GB).

2. Partition: The partition table was examined at offset 446 F0 446 LE 64 and continuing 64 bytes in the first sector (i.e. sector 0) of the image.

Partition Entry

Type	Name	Status	Start	Stop	Relative	Size
4F	Unknown	0D	335:10:2	327:84:13	1936269394	1836016416
73	Unknown	70	371:114:37	256:101:36	1917848077	544437093
2B	Unknown	43	364:116:50	372:65:44	1818575915	544175136
61	Speedstor	72	372:101:51	269:114:52	2844524554	54974

3. System settings: The windows registry hives present under *Windows\System32\Config* was examined and the evidence corresponds to Windows 7 Professional, version 6.1 operating system. The operating system was installed on Wed, 15 Jul 2015 10:35:41 GMT. The registered owner was *evgeny*. Computer Name was *EVGENY-LAPTOP*.

4. Accounts: The windows registry file Security Account Manager (SAM) at SAM\Domains\Account\Users\Names was examined and revealed four user accounts, *Administrator, evgeny, Guest and HomeGroupUser$.* Of these accounts there was only one identified active user, evgeny. The account was created on 2015-07-15. AccessData Registry Viewer also confirmed this date. Last logoff for evgeny according to EventViewer: 2015-11-06 16:30:37.

5. Programs: The programs of interest installed on the computer were: *VeraCrypt (VeraCrypt, 2019), TrueCrypt (TrueCrypt, 2019), FileZilla (FileZilla, 2019) , The Tor-Project browser (Tor, 2019), Bitcoin (Bitcoin, 2019), Chromium (Chromium, 2019) and Eraser*. TrueCrypt and VeraCrypt were both installed on 2015-09-29 11:48:32. however the presence of corresponding .lnk files indicate that the executables were interacted by the user. The usage of Tor network also keeps anonymity. Using the email service Ghostmail is also a way of keeping users identity hidden as well as using the forum Orwell FreeNode for communication. The subject's computer was not connected to any network domain. The evidence was found by examining the :

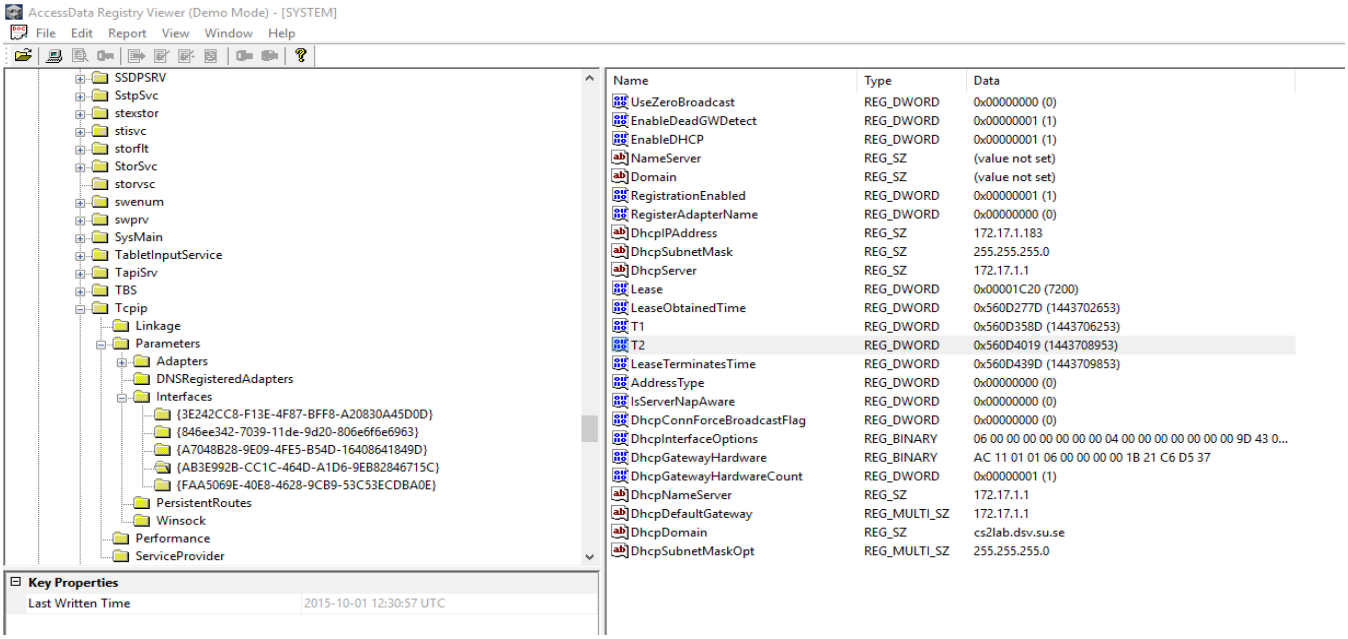

Figure 2: Network connections located in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetworkList\ :

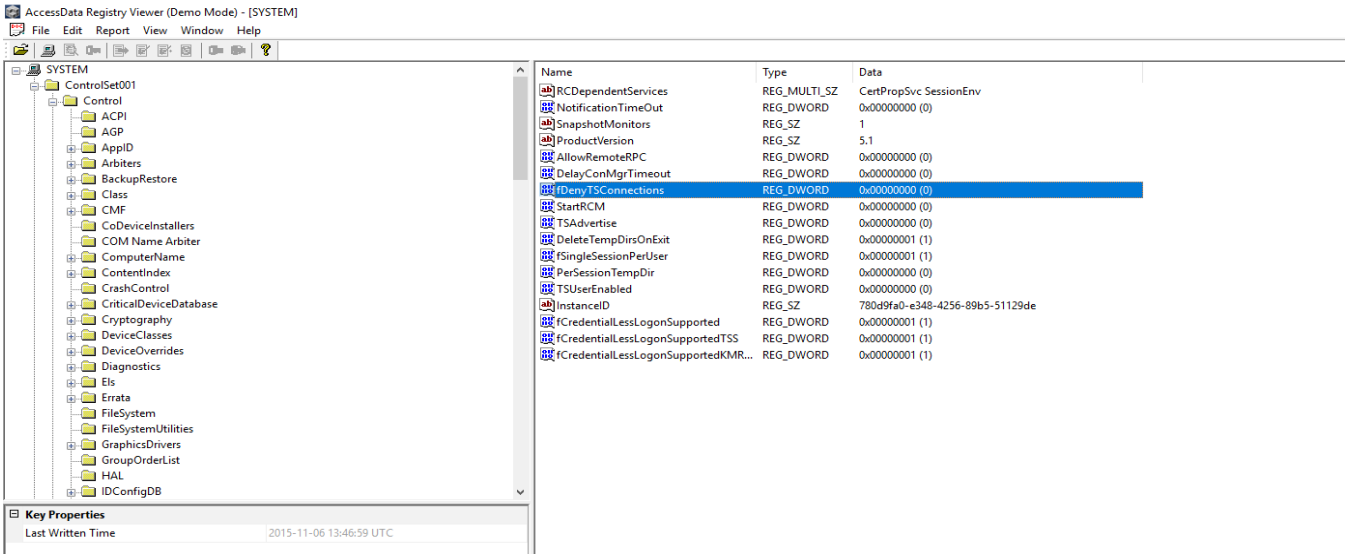

Figure 3: Remote Connection

6) There were no failed installation events but there were 9 successful installation. Some of the programs were Java programs but other were programs like Eraser which could indicate criminal activity or at least a wish to delete data.

7) Using Access data registry viewer and the path: Software\Microsoft\Internet Explorer\TypedURLS provided no significant information of interest. The following browsers were found by processing the evidence in EnCase: Mozilla (Windows/Mac), Mozilla 3 (Windows/Mac), Internet Explorer (Windows) and Chrome (Windows).Information regarding history could not be found but we found bookmarks in Internet Explorer linked to VeraCrypt in EnCase. In Chrome we found that he has been visiting Palikan.com.

8) The history was mostly clear, indicating that the web search had been cleared and that the computer could have been defragmented, deleting all traces. This however is just a theory. Chrome cache folder however contained a *"palican"*, this browser hijacker application that can infiltrate original search engine. The user has used *"palican"* according to the artefact.

9) The user has the Tor network, because the user had saved three different torproject.org sites saved as bookmarks. SQLite Browser was downloaded from sqlitebrowser.org to be able to view the files that ended with *".sqlite".* The files were run through the program said that the logical size was 0 indicating that no peculiar activity had been done. In one last attempt to try to find what is in appdata-roaming-thunderbird-file.sqlite3 we ran it through a downloaded program called fileinfo. This tool was found searching for alternative ways to open *".lib"* files.

10) The user has some pictures of TrueCrypt and other pictures indicating ransomware but nothing that indicates that it has been run or used in any type and or form.

11) Thunderbird (Email) and FileZilla (FTP) have been used for communication and interaction over the web. It has been in the form of emails and instant messaging. evgeny.lucky one@mail.ru is used for email correspondence together with chingiz112@ghostmail.com was also used for correspondence.

12) Ghostmail is used for anonymity and is mostly served as a way of being unknown in the interaction with others. This might indicate some sort of criminal activity or it could just be a sign that the user has a very high integrity.

13) A user with the email address kykypykv@ghostmail.com also sent our user an email to him. There is a friend request from a man working as a Tax Collection Consultant at “Skatteverket” which is the Swedish equivalent to what is otherwise known as state tax agency.

14) The user also communicated through Facebook messenger. He used the name evgeny during this conversation. We have not been able to get access to the information or the content of the messages.

15) The user also had a phone through which he could communicate. The number to the phone is: 076-965 01 74.

16) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters → Domain, where it says that the (value has not been set). Hence, the subject’s system was not connected to network domain

17) In conclusion: Significant amount direct evidence indicating fraud or counterfeit could not be found. Though there has been correspondence that cannot rule out other forms of criminal activity. There was correspondence in a forum called "Orwell FreeNode" between the user *"lucky456" and "kykypykv"* regarding asking for a burner phone. Another complicating factor was that some of the email were in Russian language. Google Translate was utilized to interpret the meaning but we cannot with total certainty conclude that we have interpreted the messages correctly since none of us in the investigation group speak Russian.

References

Lib, 2019. Retrieved 10 October 2019, from https://fileinfo.com/extension/lib

Chromium, 2019. Retrieved 10 October 2019, from https://www.Chromium.org

VeraCrypt, 2019. Retrieved 11 October 2019, from https://sourceforge.net/projects/veracrypt/

TrueCrypt, 2019. Retrieved 21 October 2019, from http://truecrypt.sourceforge.net/

FileZilla, 2019. Retrieved 22 October 2019, from https://sourceforge.net/projects/filezilla/files/

Tor, 2019. Retrieved 14 October 2019, from https://www.torproject.org/

Bitcoin, 2019. Retrieved 17 October 2019, from https://www.bitcoin.com/

Appendix A:

- **Pre-fetch files as obtained under C:\Windows\Pre-fetch**

SourceFilename	Source Created	Source Modified	Source Accessed	Executable Name	Run Count	Last Run
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\AUDIODG.EXE-BDFD3029.pf	2015-08-17 13:39:49	2015-11-06 15:30:21	2015-08-17 13:39:49	AUDIODG.EXE	188	2015-11-06 15:30:11
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\CHROME.EXE-2BCCABC3.pf	2015-11-06 13:50:28	2015-11-06 13:50:50	2015-11-06 13:50:28	CHROME.EXE	3	2015-11-06 13:50:40
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\CONHOST.EXE-1F3E9D7E.pf	2015-07-15 19:32:00	2015-11-06 14:20:50	2015-07-15 19:32:00	CONHOST.EXE	537	2015-11-06 14:20:49
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\CONSENT.EXE-531BD9EA.pf	2015-08-17 13:48:11	2015-10-01 11:16:43	2015-08-17 13:48:11	CONSENT.EXE	26	2015-10-01 11:16:41
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\CSC.EXE-BE9AC2DF.pf	2015-11-06 14:20:56	2015-11-06 14:20:59	2015-11-06 14:20:56	CSC.EXE	4	2015-11-06 14:20:59
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\CSRSS.EXE-3FE41F7E.pf	2015-09-11 08:31:46	2015-09-30 11:03:18	2015-09-11 08:31:46	CSRSS.EXE	13	2015-09-30 11:03:15
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\CVTRES.EXE-2B9D810D.pf	2015-11-06 14:20:56	2015-11-06 14:20:59	2015-11-06 14:20:56	CVTRES.EXE	4	2015-11-06 14:20:59
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\DEFRAG.EXE-588F90AD.pf	2015-11-06 14:10:59	2015-11-06 14:14:00	2015-11-06 14:10:59	DEFRAG.EXE	2	2015-11-06 14:13:50
C:\Users\Administrator\Documents\EnCase\Cases\	2015-10-01 10:54:52	2015-10-01 11:16:30	2015-10-01 10:54:52	DINOTIFY.EXE	2	2015-10-01 11:16:20

Lab2\Export\DINOTIFY.EXE-35A869D6.pf						
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\DLLHOST.EXE-5E46FA0D.pf	2015-08-17 13:40:55	2015-11-06 15:21:24	2015-08-17 13:40:55	DLLHOST.EXE	53	2015-11-06 15:21:14
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\DLLHOST.EXE-766398D2.pf	2015-08-17 13:48:16	2015-11-06 13:48:59	2015-08-17 13:48:16	DLLHOST.EXE	48	2015-11-06 13:48:53
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\DLLHOST.EXE-76936ED5.pf	2015-09-10 13:38:45	2015-09-29 15:25:03	2015-09-10 13:38:45	DLLHOST.EXE	12	2015-09-29 15:24:58
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\DLLHOST.EXE-A8DE6D5B.pf	2015-08-17 13:48:03	2015-11-06 15:05:09	2015-08-17 13:48:03	DLLHOST.EXE	301	2015-11-06 15:05:03
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\DRVINST.EXE-4CB4314A.pf	2015-09-14 15:11:05	2015-10-01 11:16:22	2015-09-14 15:11:05	DRVINST.EXE	13	2015-10-01 11:16:20
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\DUMPIT.EXE-379FB822.pf	2015-10-01 11:16:53	2015-10-01 11:16:53	2015-10-01 11:16:53	DUMPIT.EXE	1	2015-10-01 11:16:43
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\DWM.EXE-6FFD3DA8.pf	2015-11-06 13:50:27	2015-11-06 13:50:27	2015-11-06 13:50:27	DWM.EXE	1	2015-11-06 13:50:15
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\EFSUI.EXE-92E32A3C.pf	2015-11-06 13:48:55	2015-11-06 13:48:55	2015-11-06 13:48:55	EFSUI.EXE	1	2015-11-06 13:48:54
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\EXPLORER.EXE-A80E4F97.pf	2015-11-06 13:50:28	2015-11-06 13:50:28	2015-11-06 13:50:28	EXPLORER.EXE	1	2015-11-06 13:50:15
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\FIR	2015-08-17 12:02:59	2015-09-30 11:19:22	2015-08-17 12:02:59	FIREFOX.EXE	23	2015-09-30 11:19:22

EFOX.EXE-18ACFCFF.pf						
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\GPG2.EXE-1B9A0D5C.pf	2015-09-10 13:31:47	2015-09-30 11:19:08	2015-09-10 13:31:47	GPG2.EXE	35	2015-09-30 11:19:07
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\GPG2.EXE-991DA12B.pf	2015-09-10 13:40:51	2015-09-30 11:19:08	2015-09-10 13:40:51	GPG2.EXE	26	2015-09-30 11:19:07
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\GPG2KEYS_HKP.EXE-954DD732.pf	2015-09-29 18:44:37	2015-09-29 18:44:37	2015-09-29 18:44:37	GPG2KEYS_HKP.EXE	1	2015-09-29 18:44:27
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\GWX.EXE-D35CFF90.pf	2015-11-06 13:49:10	2015-11-06 13:49:10	2015-11-06 13:49:10	GWX.EXE	2	2015-11-06 13:49:10
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\ICQ.EXE-8679171E.pf	2015-09-09 09:25:16	2015-11-06 13:50:40	2015-09-09 09:25:16	ICQ.EXE	11	2015-11-06 13:50:16
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\LOGONUI.EXE-09140401.pf	2015-09-10 14:33:58	2015-09-30 11:03:18	2015-09-10 14:33:58	LOGONUI.EXE	14	2015-09-30 11:03:15
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\MAINTENANCESERVICE.EXE-FA0B1B99.pf	2015-09-30 21:39:27	2015-10-01 10:36:58	2015-09-30 21:39:27	MAINTENANCESERVICE.EXE	2	2015-10-01 10:36:52
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\MAKECAB.EXE-0F1704A4.pf	2015-11-06 13:50:15	2015-11-06 13:50:15	2015-11-06 13:50:15	MAKECAB.EXE	1	2015-11-06 13:50:05
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\MPAM-E5DA2111.EXE-405C9AE8.pf	2015-10-01 01:19:59	2015-10-01 01:19:59	2015-10-01 01:19:59	MPAM-E5DA2111.EXE	1	2015-10-01 01:19:53
C:\Users\Administrator\Documents\EnCase\Cases\	2015-07-25 02:46:33	2015-10-01 01:19:48	2015-07-25 02:46:33	MPCMDRUN.EXE	108	2015-10-01 01:19:42

Lab2\Export\MPCMDRUN.EXE-F401FBB4.pf						
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\MSCORSVW.EXE-57D17DAF.pf	2015-11-06 13:49:08	2015-11-06 13:49:08	2015-11-06 13:49:08	MSCORSVW.EXE	1	2015-11-06 13:49:08
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\MSCORSVW.EXE-C3C515BD.pf	2015-11-06 13:49:08	2015-11-06 13:49:08	2015-11-06 13:49:08	MSCORSVW.EXE	1	2015-11-06 13:49:08
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\NOTEPAD.EXE-D8414F97.pf	2015-09-30 11:23:03	2015-09-30 11:23:03	2015-09-30 11:23:03	NOTEPAD.EXE	1	2015-09-30 11:22:53
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\NTOSBOOT-B00DFAAD.pf	2015-07-15 19:29:43	2015-11-06 13:48:45	2015-07-15 19:29:43	NTOSBOOT	5	2015-11-06 13:46:45
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\PINENTRY.EXE-7A2106A9.pf	2015-09-10 13:38:36	2015-09-30 11:13:55	2015-09-10 13:38:36	PINENTRY.EXE	11	2015-09-30 11:13:50
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\PING.EXE-7E94E73E.pf	2015-11-06 14:21:01	2015-11-06 14:21:01	2015-11-06 14:21:01	PING.EXE	2	2015-11-06 14:21:01
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\RDPCLIP.EXE-9067FA0E.pf	2015-09-29 18:41:32	2015-09-30 11:03:29	2015-09-29 18:41:32	RDPCLIP.EXE	3	2015-09-30 11:03:29
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\RUNDLL32.EXE-230FC512.pf	2015-11-06 14:20:59	2015-11-06 14:20:59	2015-11-06 14:20:59	RUNDLL32.EXE	1	2015-11-06 14:20:49
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\RUNDLL32.EXE-3F482158.pf	2015-10-01 12:24:54	2015-10-01 12:24:54	2015-10-01 12:24:54	RUNDLL32.EXE	1	2015-10-01 12:24:52
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\RU	2015-10-01 11:16:30	2015-10-01 11:16:30	2015-10-01 11:16:30	RUNDLL32.EXE	1	2015-10-01 11:16:20

NDLL32.EXE-C76E65B5.pf						
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\RUNDLL32.EXE-DE9673F9.pf	2015-11-06 13:55:05	2015-11-06 13:55:05	2015-11-06 13:55:05	RUNDLL32.EXE	1	2015-11-06 13:55:05
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\RUNDLL32.EXE-F54415A0.pf	2015-09-29 22:29:14	2015-11-06 14:14:00	2015-09-29 22:29:14	RUNDLL32.EXE	3	2015-11-06 14:13:50
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\RUNDLL32.EXE-FA1A9AFC.pf	2015-10-01 10:54:52	2015-10-01 10:54:52	2015-10-01 10:54:52	RUNDLL32.EXE	1	2015-10-01 10:54:42
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\SDIAGNHOST.EXE-8D72177C.pf	2015-11-06 14:21:00	2015-11-06 14:21:00	2015-11-06 14:21:00	SDIAGNHOST.EXE	1	2015-11-06 14:20:50
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\SEARCHFILTERHOST.EXE-77482212.pf	2015-07-15 10:35:57	2015-11-06 15:24:14	2015-07-15 10:35:57	SEARCHFILTERHOST.EXE	183	2015-11-06 15:24:04
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\SEARCHINDEXER.EXE-4A6353B9.pf	2015-11-06 13:49:20	2015-11-06 13:49:20	2015-11-06 13:49:20	SEARCHINDEXER.EXE	1	2015-11-06 13:49:09
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\SEARCHPROTOCOLHOST.EXE-0CB8CADE.pf	2015-07-15 10:35:57	2015-11-06 15:24:14	2015-07-15 10:35:57	SEARCHPROTOCOLHOST.EXE	174	2015-11-06 15:24:04
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\SETUP_WM.EXE-D33FD27D.pf	2015-11-06 13:55:38	2015-11-06 13:55:38	2015-11-06 13:55:38	SETUP_WM.EXE	1	2015-11-06 13:55:28
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\SLUI.EXE-724E99D9.pf	2015-07-17 13:42:56	2015-11-06 15:23:56	2015-07-17 13:42:56	SLUI.EXE	239	2015-11-06 15:23:56
C:\Users\Administrator\Documents\EnCase\Cases\	2015-09-11 08:31:37	2015-09-30 11:03:15	2015-09-11 08:31:37	SMSS.EXE	12	2015-09-30 11:03:15

Lab2\Export\SMSS.EXE-E9C28FC6.pf						
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\SPPSVC.EXE-B0F8131B.pf	2015-11-06 13:49:05	2015-11-06 13:49:05	2015-11-06 13:49:05	SPPSVC.EXE	1	2015-11-06 13:48:54
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\SVCHOST.EXE-007FEA55.pf	2015-11-06 13:49:19	2015-11-06 13:49:19	2015-11-06 13:49:19	SVCHOST.EXE	1	2015-11-06 13:49:09
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\SVCHOST.EXE-6168E4A3.pf	2015-11-06 13:56:55	2015-11-06 13:56:55	2015-11-06 13:56:55	SVCHOST.EXE	1	2015-11-06 13:56:52
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\SVCHOST.EXE-7AC6742A.pf	2015-09-30 23:32:55	2015-11-06 14:11:02	2015-09-30 23:32:55	SVCHOST.EXE	2	2015-11-06 14:10:52
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\SVCHOST.EXE-80F4A784.pf	2015-09-10 12:00:57	2015-11-06 13:53:25	2015-09-10 12:00:57	SVCHOST.EXE	8	2015-11-06 13:53:19
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\TASKHOST.EXE-7238F31D.pf	2015-07-15 10:35:59	2015-11-06 15:13:28	2015-07-15 10:35:59	TASKHOST.EXE	1841	2015-11-06 15:13:18
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\THUNDERBIRD.EXE-A0DA674F.pf	2015-09-10 13:25:07	2015-09-30 11:09:18	2015-09-10 13:25:07	THUNDERBIRD.EXE	13	2015-09-30 11:09:17
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\TRUSTEDINSTALLER.EXE-3CC531E5.pf	2015-11-06 13:50:14	2015-11-06 13:50:14	2015-11-06 13:50:14	TRUSTEDINSTALLER.EXE	1	2015-11-06 13:50:05
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\TSTHEME.EXE-14AC78EA.pf	2015-09-11 08:31:52	2015-09-30 11:23:46	2015-09-11 08:31:52	TSTHEME.EXE	15	2015-09-30 11:23:40
C:\Users\Administrator\Documents\EnCase\Cases\	2015-09-10 11:05:01	2015-11-06 15:05:10	2015-09-10 11:05:01	UNINSTALL.EXE	466	2015-11-06 15:05:00

Lab2\Export\UNINSTALL.EXE-81EB6B01.pf						
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\UPDATER.EXE-55F63489.pf	2015-09-30 21:39:28	2015-10-01 10:36:55	2015-09-30 21:39:28	UPDATER.EXE	2	2015-10-01 10:36:53
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\UPDATER.EXE-58AE5631.pf	2015-09-30 21:39:27	2015-09-30 21:39:27	2015-09-30 21:39:27	UPDATER.EXE	1	2015-09-30 21:39:17
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\UPDATER.EXE-B2224489.pf	2015-10-01 10:36:58	2015-10-01 10:36:58	2015-10-01 10:36:58	UPDATER.EXE	1	2015-10-01 10:36:52
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\USERINIT.EXE-2257A3E7.pf	2015-11-06 13:50:25	2015-11-06 13:50:25	2015-11-06 13:50:25	USERINIT.EXE	1	2015-11-06 13:50:15
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\VSSVC.EXE-B8AFC319.pf	2015-07-15 11:21:31	2015-11-06 14:21:07	2015-07-15 11:21:31	VSSVC.EXE	102	2015-11-06 14:20:57
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\W32TM.EXE-1101AF41.pf	2015-11-06 14:21:00	2015-11-06 14:21:00	2015-11-06 14:21:00	W32TM.EXE	1	2015-11-06 14:21:00
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\WATADMINSVC.EXE-082508A5.pf	2015-11-06 13:56:14	2015-11-06 13:56:14	2015-11-06 13:56:14	WATADMINSVC.EXE	1	2015-11-06 13:56:10
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\WERFAULT.EXE-37549B7E.pf	2015-11-06 13:53:29	2015-11-06 13:53:29	2015-11-06 13:53:29	WERFAULT.EXE	1	2015-11-06 13:53:19
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\WERMGR.EXE-0F2AC88C.pf	2015-10-01 02:32:30	2015-11-06 14:01:55	2015-10-01 02:32:30	WERMGR.EXE	3	2015-11-06 14:01:55
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\WI	2015-09-11 08:31:47	2015-09-30 11:03:18	2015-09-11 08:31:47	WINLOGON.EXE	13	2015-09-30 11:03:15

NLOGON.EXE-B020DC41.pf						
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\WINZIPRO.EXE-833B92D4.pf	2015-09-10 13:01:10	2015-11-06 14:01:10	2015-09-10 13:01:10	WINZIPRO.EXE	24	2015-11-06 14:01:00
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\WMIADAP.EXE-F8DFDFA2.pf	2015-09-14 15:10:00	2015-11-06 13:55:30	2015-09-14 15:10:00	WMIADAP.EXE	11	2015-11-06 13:55:20
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\WMIPRVSE.EXE-1628051C.pf	2015-07-15 10:35:47	2015-11-06 14:49:21	2015-07-15 10:35:47	WMIPRVSE.EXE	257	2015-11-06 14:49:11
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\WMIPRVSE.EXE-6768A320.pf	2015-11-06 13:50:53	2015-11-06 13:50:53	2015-11-06 13:50:53	WMIPRVSE.EXE	1	2015-11-06 13:50:43
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\WMPLAYER.EXE-26C72A86.pf	2015-11-06 13:55:28	2015-11-06 13:55:28	2015-11-06 13:55:28	WMPLAYER.EXE	1	2015-11-06 13:55:28
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\WMPNETWK.EXE-D9F2A96F.pf	2015-11-06 13:49:19	2015-11-06 13:49:19	2015-11-06 13:49:19	WMPNETWK.EXE	1	2015-11-06 13:49:09
C:\Users\Administrator\Documents\EnCase\Cases\Lab2\Export\WUDFHOST.EXE-AFFEF87C.pf	2015-10-01 09:53:29	2015-11-06 15:30:24	2015-10-01 09:53:29	WUDFHOST.EXE	6	2015-11-06 15:30:14

Appendix B

- Link files as obtained which indicate possible interaction with the mentioned files by the user:

Name	Base Path	Relative Path	Created
WinZip Registry Optimizer.lnk	C:\Program Files (x86)\WinZip Registry Optimizer\Winzipro.exe	.\..\Program Files (x86)\WinZip Registry Optimizer\Winzipro.exe	09/09/15 12:04:30
TrueCrypt.lnk	C:\Program Files\TrueCrypt\TrueCrypt.exe	..\..\..\Program Files\TrueCrypt\TrueCrypt.exe	09/29/15 10:44:23
7-Zip File Manager.lnk	C:\Program Files\7-Zip\7zFM.exe	..\..\..\..\..\..\Program Files\7-Zip\7zFM.exe	09/29/15 12:46:55
7-Zip Help.lnk	C:\Program Files\7-Zip\7-zip.chm	\..\..\..\..\Program Files\7-Zip\7-zip.chm	09/29/15 12:46:55
Speech Recognition.lnk		.\..\..\..\..\..\Windows\Speech\Common\sapisvr.exe	07/14/09 02:33:53
Character Map.lnk		.\..\..\..\..\..\Windows\System32\charmap.exe	07/14/09 01:56:49
dfrgui.lnk		.\..\..\..\..\..\Windows\System32\dfrgui.exe	07/14/09 01:36:36
Disk Cleanup.lnk		.\..\..\..\..\..\Windows\System32\cleanmgr.exe	07/14/09 01:56:06
Resource Monitor.lnk		.\..\..\..\..\..\Windows\System32\perfmon.exe	07/14/09 01:31:45
System Information.lnk		.\..\..\..\..\..\Windows\System32\msinfo32.exe	07/14/09 01:31:55
System Restore.lnk		.\..\..\..\..\..\Windows\System32\rstrui.exe	07/14/09 01:36:50
Task Scheduler.lnk		.\..\..\..\..\..\Windows\System32\taskschd.msc	07/13/09 23:36:47
Windows Easy Transfer Reports.lnk		.\..\..\..\..\..\Windows\System32\migwiz\PostMig.exe	07/14/09 01:28:57
Windows Easy Transfer.lnk		.\..\..\..\..\..\Windows\System32\migwiz\migwiz.exe	07/14/09 01:29:02
TabTip.lnk		..\..\..\..\..\..\..\Program Files\Common Files\Microsoft Shared\ink\TabTip.exe	07/14/09 02:01:43
ShapeCollector.lnk		..\..\..\..\..\..\..\Program Files\Common Files\Microsoft Shared\ink\ShapeCollector.exe	07/14/09 02:02:45
Windows Journal.lnk		..\..\..\..\..\..\..\Program Files\Windows Journal\Journal.exe	11/21/10 04:25:06
Windows PowerShell (x86).lnk			07/08/08 03:27:28
Windows PowerShell ISE (x86).lnk		\..\..\..\..\..\Windows\SysWOW64\WindowsPowerShell\v1.0\p	07/13/09 23:47:02

		owershell_ise.exe	
Windows PowerShell ISE.lnk		\..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe	07/13/09 23:37:36
Windows PowerShell.lnk			12/01/07 07:40:30
Bluetooth File Transfer Wizard.lnk	C:\Windows\System32\fsquirt.exe	\..\..\..\..\Windows\System32\fsquirt.exe	11/21/10 04:23:47
Calculator.lnk		\..\..\..\..\Windows\System32\calc.exe	07/14/09 01:57:11
displayswitch.lnk		\..\..\..\..\Windows\System32\DisplaySwitch.exe	07/14/09 01:55:17
Paint.lnk		..\..\..\..\..\Windows\System32\mspaint.exe	07/14/09 01:58:41
Remote Desktop Connection.lnk		..\..\..\..\..\Windows\System32\mstsc.exe	07/14/09 02:17:08
Sound Recorder.lnk		\..\..\..\..\Windows\System32\SoundRecorder.exe	07/14/09 02:25:34
Sync Center.lnk		..\..\..\..\..\Windows\System32\mobsync.exe	07/14/09 01:55:04
Welcome Center.lnk		\..\..\..\..\Windows\System32\rundll32.exe	07/14/09 01:57:20
Wordpad.lnk		..\..\..\..\..\Program Files\Windows NT\Accessories\wordpad.exe	07/14/09 01:58:42
NetworkProjection.lnk		\..\..\..\..\Windows\System32\NetProj.exe	07/14/09 02:12:02
Math Input Panel.lnk		..\..\..\..\..\Program Files\Common Files\Microsoft Shared\ink\mip.exe	11/21/10 04:24:39
Snipping Tool.lnk		\..\..\..\..\Windows\System32\SnippingTool.exe	07/14/09 02:03:20
Mobility Center.lnk		..\..\..\..\..\Windows\System32\mblctr.exe	11/21/10 04:24:39
Sticky Notes.lnk		\..\..\..\..\Windows\System32\StikyNot.exe	07/14/09 01:57:57
Component Services.lnk		\..\..\..\..\Windows\System32\comexp.msc	07/13/09 23:52:42
Computer Management.lnk		\..\..\..\..\Windows\System32\compmgmt.msc	07/13/09 23:34:41
Data Sources (ODBC).lnk		\..\..\..\..\Windows\System32\odbcad32.exe	07/14/09 02:28:30
Event Viewer.lnk		\..\..\..\..\Windows\System32\eventvwr.msc	07/13/09 23:36:47
iSCSI Initiator.lnk		\..\..\..\..\Windows\System32\iscsicpl.exe	07/14/09 02:01:23
Memory Diagnostics Tool.lnk		..\..\..\..\..\Windows\System32\MdSched.exe	07/14/09 01:32:43
Performance Monitor.lnk		\..\..\..\..\Windows\System32\perfmon.msc	07/13/09 23:14:23

services.lnk		..\..\..\..\..\Windows\System32\services.msc	07/13/09 23:34:42
System Configuration.lnk		..\..\..\..\..\Windows\System32\msconfig.exe	07/14/09 01:31:56
Task Scheduler.lnk		..\..\..\..\..\Windows\System32\taskschd.msc	07/13/09 23:36:47
Windows Firewall with Advanced Security.lnk		..\..\..\..\..\Windows\System32\WF.msc	07/14/09 00:01:54
Windows PowerShell Modules.lnk			12/01/07 07:40:30
Print Management.lnk		..\..\..\..\..\Windows\System32\printmanagement.msc	07/14/09 00:51:21
Security Configuration Management.lnk		..\..\..\..\..\Windows\System32\secpol.msc	07/13/09 23:34:43
GameExplorer.lnk			
Gpg4win HOWTO SMIME.lnk	C:\Program Files (x86)\GNU\GnuPG\share\gpg4win\HOWTO-SMIME.en.txt	..\..\..\..\..\..\..\Program Files (x86)\GNU\GnuPG\share\gpg4win\HOWTO-SMIME.en.txt	07/10/15 12:49:04
Gpg4win README.lnk	C:\Program Files (x86)\GNU\GnuPG\share\gpg4win\README.en.txt	..\..\..\..\..\..\..\Program Files (x86)\GNU\GnuPG\share\gpg4win\README.en.txt	07/10/15 12:49:04
Uninstall.lnk	C:\Program Files (x86)\GNU\GnuPG\gpg4win-uninstall.exe	..\..\..\..\..\..\Program Files (x86)\GNU\GnuPG\gpg4win-uninstall.exe	09/29/15 16:39:29
ckup and Restore Center.lnk		..\..\..\..\..\Windows\System32\control.exe	07/14/09 01:55:53
Create Recovery Disc.lnk		..\..\..\..\..\Windows\System32\recdisc.exe	07/14/09 01:36:52
Remote Assistance.lnk		..\..\..\..\..\Windows\System32\msra.exe	07/14/09 01:32:03
TrueCrypt.lnk	C:\Program Files\TrueCrypt\TrueCrypt.exe	..\..\..\..\..\..\Program Files\TrueCrypt\TrueCrypt.exe	09/29/15 10:44:23
Uninstall TrueCrypt.lnk	\Program Files\TrueCrypt\TrueCrypt Setup.exe	..\..\..\..\..\..\Program Files\TrueCrypt\TrueCrypt Setup.exe	09/29/15 10:44:23
VeraCrypt.lnk	C:\Program Files\VeraCrypt\VeraCrypt.exe	..\..\..\..\..\..\Program Files\VeraCrypt\VeraCrypt.exe	09/29/15 11:48:33
VeraCryptExpander.lnk	C:\Program Files\VeraCrypt\VeraCryptExpander.exe	..\..\..\..\..\..\Program Files\VeraCrypt\VeraCryptExpander.exe	09/29/15 11:48:33
Uninstall VeraCrypt.lnk	C:\Windows\System32\control.exe	..\..\..\..\..\Windows\System32\control.exe	07/14/09 01:40:14
WinZip Registry Optimizer.lnk	C:\Program Files (x86)\nZip Registry Optimizer\Winzipro.exe	..\..\..\..\..\..\Program Files (x86)\WinZip Registry Optimizer\Winzipro.exe	09/09/15 12:04:30
Uninstall WinZip Registry Optimizer.lnk	C:\Program Files (x86)\nZip Registry Optimizer\unins000.exe	..\..\..\..\..\..\Program Files (x86)\WinZip Registry Optimizer\unins000.exe	09/09/15 12:04:30

Sidebar.lnk		\..\..\..\Program Files\Windows Sidebar\sidebar.exe	07/14/09 01:57:29
Windows Fax and Scan.lnk		.\..\..\..\Windows\System32\WFS.exe	07/14/09 02:36:26
Windows Media Player.lnk		..\..\..\..\..\Program Files (x86)\Windows Media Player\wmplayer.exe	11/21/10 04:25:10
XPS Viewer.lnk		\..\..\..\Windows\System32\xpsrchvw.exe	07/14/09 02:47:50
Windows DVD Maker.lnk		.\..\..\..\..\Program Files\DVD Maker\DVDMaker.exe	07/14/09 02:26:53
Media Center.lnk		\..\..\..\Windows\ehome\ehshell.exe	07/14/09 02:24:51
Eraser.lnk	C:\Program Files\ Eraser\Eraser.exe	..\..\..\..\..\Program Files\Eraser\Eraser.exe	04/13/15 17:42:52
Mozilla Thunderbird.lnk	C:\Program Files (x86)\Mozilla Thunderbird\ thunderbird.exe	..\..\..\..\..\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe	09/09/15 12:21:17
Default Programs.lnk		\..\..\Windows\System32\control.exe	07/14/09 01:55:53
Windows Update.lnk		\..\..\Windows\System32\wuapp.exe	07/14/09 02:34:58
Bitcoin Core (64-bit).lnk	C:\Program Files\ Bitcoin\bitcoin-qt.exe	..\..\..\..\..\..\..\..\..\Program Files\Bitcoin\bitcoin-qt.exe	06/01/15 02:00:00
Uninstall Bitcoin Core (64-bit).lnk	C:\Program Files\ Bitcoin\uninstall.exe	..\..\..\..\..\..\..\..\..\Program Files\Bitcoin\uninstall.exe	07/24/15 13:50:53
Code.lnk	C:\Users\	\..\..\..\..\Local\Code\Update.exe	07/24/15 12:51:02
mIRC.lnk	:\Program Files (x86)\mIRC\mirc.exe	..\..\..\..\..\..\Program Files (x86)\mIRC\mirc.exe	07/22/15 15:55:27
Readme.txt.lnk	C:\Program Files (x86)\ mIRC\readme.txt	..\..\..\..\..\..\Program Files (x86)\mIRC\readme.txt	07/22/15 15:55:27
Versions.txt.lnk	C:\Program Files (x86)\mIRC\versions.txt	..\..\..\..\..\..\Program Files (x86)\mIRC\versions.txt	07/22/15 15:55:27
IRCIntro Help.lnk	C:\Program Files (x86)\mIRC\ircintro.chm	..\..\..\..\..\..\Program Files (x86)\mIRC\ircintro.chm	07/22/15 15:55:27
mIRC Help.lnk	C:\Program Files (x86) \mIRC\mirc.chm	..\..\..\..\..\..\Program Files (x86)\mIRC\mirc.chm	07/22/15 15:55:27
Oracle VM VirtualBox.lnk	C:\Program Files\Oracle\VirtualBox\VirtualBox.exe	..\..\..\..\..\..\Program Files\Oracle\VirtualBox\VirtualBox.exe	07/09/15 12:09:38
User manual (CHM, English).lnk		..\..\..\..\..\..\Program Files\Oracle\VirtualBox\VirtualBox.chm	
User manual (PDF, English).lnk		..\..\..\..\..\..\Program Files\Oracle\VirtualBox\doc\ UserManual.pdf	
License (English).lnk	C:\Program Files\Oracle\ VirtualBox\ License_en_US.rtf	..\..\..\..\..\..\Program Files\Oracle\VirtualBox\License_en_US.rtf	08/29/14 15:10:18

ICQ.lnk	C:\Users\	..\AppData\Roaming\ ICQM\icq.exe	07/22/15 15:53:59
amd64_microsoft-windows-e. .os-loader.resources_ 31bf3856ad364e35_ 6.1.7601.23072_ru-ru_2c1931d0a0156ad1. manifest	C:\Program Files\FileZilla FTP Client\filezilla.exe	..\..\..\..\..\..\..\..\..\Program Files\FileZilla FTP Client\filezilla.exe	08/24/15 15:56:34
amd64_ 50851c14f4bacc86 fba999208f5b57ac_ 31bf3856ad364e35_ 6.1.7600.20910_ none_ 5f3fb1e9d67e75ae. manifest	C:\Users\	..\..\..\ICQM\icq.exe	07/22/15 15:53:59
package_for_ kb2985461_sp1~ 31bf3856ad364e35~ amd64~~6.1.1.0.mum	C:\Program Files (x86)\GNU\GnuPG\gpg4 win-uninstall.exe	..\..\..\..\..\..\Program Files (x86)\GNU\GnuPG\gpg4win-uninstall.exe	09/29/15 16:39:29
30457969_ 1336722676.back.xml	C:\Users\	..\..\..\ICQM\icq.exe	07/22/15 15:53:59
package_66_ for_kb982018~ 31bf3856ad364e35~ amd64~ ~6.1.3.2.cat		\..\..\..\..\..\Windows\System32 \perfmon.exe	07/14/09 01:31:45
package_84_for_ kb982018_bf~ 31bf3856ad364e35~ amd64~~6.1.3.2.cat		\..\..\..\..\..\Windows\System32 \msinfo32.exe	07/14/09 01:31:55
Launch Internet Explorer Browser.lnk	C:\Program Files\Internet Explorer\iexplore.exe	..\..\..\..\..\..\..\..\Program Files\Internet Explorer\iexplore.exe	07/17/15 12:24:51
package_3_for_ kb3079904_bf~ 31bf3856ad364e35~ amd64~~6.1.1.0.cat	C:\Program Files (x86)\ mIRC\mirc.chm	..\..\..\..\..\..\Program Files (x86)\mIRC\mirc.chm	07/22/15 15:55:27
package_for_ kb3079904_sp1~ 31bf3856ad364e35 ~amd64~~6.1.1.0.mum		..\..\..\..\..\..\Program Files\Oracle\VirtualBox\VirtualBox.chm	
removed-files	C:\Users\	\ppData\Roaming\ICQM\icq.exe	07/22/15 15:53:59
Mozilla Firefox.lnk	C:\Program Files (x86) \Mozilla Firefox\ firefox.exe	..\..\..\..\..\Program Files (x86)\Mozilla Firefox\firefox.exe	07/22/15 10:27:50
Mozilla Firefox.lnk	C:\Program Files (x86)\ Mozilla Firefox\firefox.exe	.\..\Program Files (x86)\Mozilla Firefox\firefox.exe	07/22/15 10:27:50
ICQ.lnk	C:\Users\	..\..\..\..\..\ICQM\icq.exe	07/22/15 15:53:59

Uninstall ICQ.lnk	C:\Users\	.\..\..\..\..\..\ICQM\icqsetup.exe	07/22/15 15:53:59
icq.com.lnk			
ICQ.lnk	C:\Users\	..\..\..\ICQM\icq.exe	07/22/15 15:53:59
ICQ.lnk	C:\Users\	..\..\..\ICQM\icq.exe	07/22/15 15:53:59
$RCP5EAB.lnk	C:\Users\	\ppData\Roaming\ICQM\icq.exe	07/22/15 15:53:59
ICQ.lnk	C:\Users\	\ppData\Roaming\ICQM\icq.exe	07/22/15 15:53:59
mIRC.lnk	C:\Program Files (x86)\mIRC\mirc.exe	..\..\..\Program Files (x86)\mIRC\mirc.exe	07/22/15 15:55:27
SuperPuTTY-1.4.0.6.lnk	C:\Users\	\..\..\..\Downloads\SuperPuTTY-1.4.0.6.zip	07/22/15 15:55:59
$RT92BRF.lnk	C:\Users\	.\SuperPutty.exe	05/09/15 16:54:52
$RE6BXKQ.lnk	C:\Users\	\ppData\Local\Code\Update.exe	07/24/15 12:51:02
slide05.png		\..\..\..\..\Windows\System32\SoundRecorder.exe	07/14/09 02:25:34
compat_critical_icon.png	C:\Program Files (x86)\mIRC\ircintro.chm	..\..\..\..\..\..\Program Files (x86)\mIRC\ircintro.chm	07/22/15 15:55:27
compat_notes_icon.png	C:\Program Files (x86)\mIRC\versions.txt	..\..\..\..\..\..\Program Files (x86)\mIRC\versions.txt	07/22/15 15:55:27
slide05.png		\..\..\..\..\Windows\System32\NetProj.exe	07/14/09 02:12:02
slide03.png		..\..\..\..\..\..\..\Program Files\Common Files\Microsoft Shared\ink\TabTip.exe	07/14/09 02:01:43
System.Web.Mobile.ni.dll.aux	C:\Users\	..\..\..\..\Downloads\tails-i386-1.5.1.torrent	09/09/15 12:07:47
µTorrent.lnk	C:\Users\	Users\evgeny\AppData\Roaming\uTorrent\uTorrent.exe	07/24/15 13:53:55
µTorrent.lnk	C:\Users\	Users\evgeny\AppData\Roaming\uTorrent\uTorrent.exe	07/24/15 13:53:55
Oracle VM VirtualBox.lnk	C:\Program Files\Oracle\VirtualBox\VirtualBox.exe	..\..\..\Program Files\Oracle\VirtualBox\VirtualBox.exe	07/09/15 12:09:38
Downloads.lnk	C:\Users\	..\..\..\..\..\Downloads	07/15/15 12:35:47
Shows Desktop.lnk			
Window Switcher.lnk			
Fax Recipient.lnk		\..\..\..\..\..\..\Windows\System32\WFS.exe	07/14/09 02:36:26
Ease of Access.lnk		\..\..\..\..\..\..\..\..\Windows\System32\control.exe	07/14/09 01:55:53
Magnify.lnk		\..\..\..\..\..\..\..\..\..\Windows\System32\Magnify.exe	07/14/09 02:33:51
Narrator.lnk		\..\..\..\..\..\..\..\..\..\Windows\System32\Narrator.exe	07/13/09 23:27:28
On-Screen Keyboard.lnk		\..\..\..\..\..\..\..\..\..\Windows\Syst	07/14/09 02:33:55

		em32\osk.exe	
computer.lnk			
Control Panel.lnk			
Private Character Editor.lnk		\..\..\..\..\..\..\..\..\Windows\System32\eudcedit.exe	07/14/09 01:56:50
Windows Explorer.lnk		\..\..\..\..\..\..\..\Windows\explorer.exe	07/14/09 01:56:52
Command Prompt.lnk		.\..\..\..\..\..\..\..\Windows\System32\cmd.exe	07/14/09 01:34:38
Notepad.lnk		.\..\..\..\..\..\..\..\Windows\System32\notepad.exe	07/14/09 01:56:36
Run.lnk			
Help.lnk			
Chromium.lnk	C:\Users\	\..\..\..\..\..\Local\Chromium\Application\chrome.exe	09/09/15 12:06:35
Internet Explorer.lnk	C:\Program Files (x86)\ Internet Explorer\ iexplore.exe	..\..\..\..\..\..\..\..\Program Files (x86)\Internet Explorer\iexplore.exe	08/11/15 22:55:45
Windows Explorer.lnk		\..\..\..\..\..\..\..\Windows\explorer.exe	07/14/09 01:56:52
Windows Media Player.lnk		..\..\..\..\..\Program Files (x86)\Windows Media Player\wmplayer.exe	11/21/10 04:25:10
Mozilla Firefox.lnk	C:\Program Files (x86) \Mozilla Firefox\firefox.exe	..\..\..\..\..\..\..\..\Program Files (x86)\Mozilla Firefox\firefox.exe	07/22/15 10:27:50
Chromium.lnk	C:\Users\	\..\..\..\..\Local\Chromium\Application\chrome.exe	09/09/15 12:06:35
Chromium (2).lnk	C:\Users\	\..\..\..\..\Local\Chromium\Application\chrome.exe	09/09/15 12:06:35
Mozilla Thunderbird.lnk	C:\Program Files (x86) \Mozilla Thunderbird\ thunderbird.exe	..\..\..\..\..\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe	09/09/15 12:21:17
Window Switcher.lnk			
Shows Desktop.lnk			
m32978_ 1920x1200-01.lnk	C:\Users\	\..\..\..\Pictures\m32978_1920x1200-01.jpg	09/11/15 11:40:19
11226563_ 1159283474085029_ 6036277529785033447_ n.lnk	C:\Users\	.\..\..\..\Pictures\11226563_1159283474085029_6036277529785033447_n.jpg	
My Pictures.lnk	C:\Users\	..\..\..\..\..\Pictures	07/15/15 12:35:47
homenetworkkey.lnk	C:\Users\ evgeny\Desktop\ homenetworkkey.txt	.\..\..\..\Desktop\homenetworkkey.txt	07/16/15 14:19:47
EvgenyPub.asc.lnk	C:\Users\	\..\..\..\Documents\EvgenyPub.asc	09/29/15 16:40:57

Key 0x48FE4AD3424A6212(1). asc.lnk	C:\Users\	\..\..\..\Downloads\key0x48FE4 AD3424A6212(1).asc	09/29/15 16:58:40
tails-i386-1.5.1.lnk	C:\Users\	..\..\..\..\Downloads\tails-i386-1.5.1.torrent	09/09/15 12:07:47
test.lnk	C:\Users\	.\..\..\..\Downloads\test.torrent	09/16/15 10:11:01
CustomerRegistry.lnk	C:\Users\	\..\..\..\Documents\CustomerRegistry.txt	09/09/15 12:06:39
cash.lnk	C:\Users\	..\..\..\..\..\Pictures\cash.jpg	
kali-linux-2.0-i386.lnk	C:\Users\	..\..\..\..\Downloads\kali-linux-2.0-i386.torrent	09/09/15 11:26:06
Downloads.lnk	C:\Users\	..\..\..\..\..\Downloads	07/15/15 12:35:47
003.lnk	C:\Users\	..\..\..\..\..\Pictures\2015-08-17\003.jpg	02/07/13 15:56:34
2015-08-17.lnk	C:\Users\	\..\..\..\..\Pictures\2015-08-17	08/17/15 15:40:58
Windows6.0 -KB933246-x86.lnk	C:\Users\	.\..\..\..\Downloads\Windows6.0-KB933246-x86.msu	09/29/15 11:46:44
Documents.lnk	C:\Users\	ibraries\Documents.library-ms	07/15/15 12:36:08
sokrovishche.lnk	C:\Users\	.\..\..\..\Documents\sokrovishche	09/29/15 11:41:50
links.lnk	C:\Users\	..\..\..\..\..\Desktop\links.txt	09/09/15 12:23:51
Key 0x48FE4AD3424A6212. asc.lnk	C:\Users\	\..\..\..\Downloads\key0x48FE4 AD3424A6212.asc	09/29/15 16:58:33
filezilla_logfile.lnk	C:\Users\	..\..\..\..\..\filezilla_logfile.log	
evgeny.lnk	C:\Users\	..\..\..\..\..	07/15/15 12:35:44
ali-linux-1.1.0a-amd64.lnk	C:\Users\	..\..\..\..\Downloads\kali-linux-1.1.0a-amd64.iso	07/24/15 16:55:43
Pictures.lnk	C:\Users\	\Libraries\Pictures.library-ms	07/15/15 12:36:08
#businessclub.freenode.lnk	C:\Users\	\..\mIRC\logs\##businessclub.freenode.log	09/10/15 10:53:04
logs.lnk	C:\Users\	..\..\..\mIRC\logs	09/10/15 10:45:39
Montenegro 1.lnk	C:\Users\	...\..\..\..\Pictures\Montenegro 1.jpg	
Montenegro 11.lnk	C:\Users\	...\..\..\..\Pictures\Montenegro 11.jpg	
Windows6.0 -KB933246-x64.lnk	C:\Users\	.\..\..\..\Downloads\Windows6.0-KB933246-x64.msu	09/29/15 11:46:31
12009598_ 10154061227926840_ 7073363885670468183_ n.lnk	C:\Users\	.\..\..\..\Pictures\12009598_10154061227926840_7073363885670468183_n.jpg	
fayly.lnk	C:\Users\	\..\..\..\..\Downloads\fayly.zip	09/29/15 14:10:42
keyserver2. pgp.com GlobalDirectoryKey. asc.lnk	C:\Users\	.\..\..\..\Downloads\keyserver2.pgp.comGlobalDirectoryKey.asc	09/29/15 16:44:49

tails-i386-1.5.1 (2).lnk	C:\Users\	..\..\..\..\Downloads\tails-i386-1.5.1\tails-i386-1.5.1.iso	09/09/15 12:09:54
tails-i386-1.5.1 (3).lnk	C:\Users\	..\..\..\..\Downloads\tails-i386-1.5.1	09/09/15 12:09:54
evgeny.luckyone@mail.ru (0x50725755) rev.asc.lnk	C:\Users\	\..\..\..\Documents\evgeny.luckyone@mail.ru (0x50725755) rev.asc	09/10/15 15:38:43
facebook-evgenyluckyone.lnk	C:\Users\	..\..\..\..\Downloads\facebook-evgenyluckyone.zip	09/30/15 13:19:28
Fax Recipient.lnk		.\..\..\..\..\..\Windows\System32\WFS.exe	07/14/09 02:36:26
Bluetooth File Transfer.LNK	C:\Windows\System32\fsquirt.exe	.\..\..\..\..\..\Windows\System32\fsquirt.exe	11/21/10 04:23:47
On-Screen Keyboard.lnk		\..\..\..\..\..\..\..\..\Windows\System32\osk.exe	07/14/09 02:33:55
Narrator.lnk		\..\..\..\..\..\..\..\..\Windows\System32\Narrator.exe	07/13/09 23:27:28
Magnify.lnk		\..\..\..\..\..\..\..\..\Windows\System32\Magnify.exe	07/14/09 02:33:51
Ease of Access.lnk		\..\..\..\..\..\..\..\..\Windows\System32\control.exe	07/14/09 01:55:53
Control Panel.lnk			
computer.lnk			
Private Character Editor.lnk		\..\..\..\..\..\..\..\..\Windows\System32\eudcedit.exe	07/14/09 01:56:50
Internet Explorer (No Add-ons).lnk	C:\Program Files\Internet Explorer\iexplore.exe	..\..\..\..\..\..\..\..\..\Program Files\Internet Explorer\iexplore.exe	07/16/15 17:28:53
Windows Explorer.lnk		\..\..\..\..\..\..\..\..\Windows\explorer.exe	07/14/09 01:56:52
Run.lnk			
Notepad.lnk		.\..\..\..\..\..\..\..\..\Windows\System32\notepad.exe	07/14/09 01:56:36
Command Prompt.lnk		.\..\..\..\..\..\..\..\..\Windows\System32\cmd.exe	07/14/09 01:34:38
FileZilla.lnk	C:\Program Files\FileZilla FTP Client\filezilla.exe	..\..\..\..\..\..\..\..\..\Program Files\FileZilla FTP Client\filezilla.exe	08/24/15 15:56:34
Uninstall.lnk	C:\Program Files\FileZilla FTP Client\uninstall.exe	..\..\..\..\..\..\..\..\..\Program Files\FileZilla FTP Client\uninstall.exe	09/09/15 12:04:42
Help.lnk			
Internet Explorer.lnk	C:\Program Files\Internet Explorer\iexplore.exe	..\..\..\..\..\..\..\..\..\Program Files\Internet Explorer\iexplore.exe	07/16/15 17:28:53
Start Tor Browser.lnk	C:\Users\	..\..\..\..\..\..\Desktop\Tor Browser\Browser\firefox.exe	01/01/00 01:00:00
Start Tor Browser.lnk	C:\Users\	.\Browser\firefox.exe	01/01/00 01:00:00
Apple_iPhone 5S	J:\Apple iPhone 5S	Apple_iPhone 5S (A1530).ufd	04/03/12 00:52:39

(A1530).ufd - Shortcut.lnk	(A1530) 2012_04_03 (001)\ FileSystem 01\Apple_iPhone 5S (A1530).ufd		
Chromium.lnk	C:\Users\	\ppData\Local\Chromium\Application\chrome.exe	09/09/15 12:06:35
Start Tor Browser.lnk	C:\Users\	.\Tor Browser\Browser\firefox.exe	01/01/00 01:00:00
RecentPlaces.lnk			
Desktop.lnk	C:\Users\	..\Desktop	07/15/15 12:35:47
Downloads.lnk	C:\Users\	..\Downloads	07/15/15 12:35:47
Gpg4win README.lnk	C:\Program Files (x86)\GNU\GnuPG\share\gpg4win\ README.en.txt	..\..\..\..\Program Files (x86)\GNU\GnuPG\share\gpg4win\README.en.txt	07/10/15 12:49:04
Gpg4win HOWTO SMIME.lnk	C:\Program Files (x86)\GNU\GnuPG\share\gpg4win\ HOWTO-SMIME.en.txt	..\..\..\..\Program Files (x86)\GNU\GnuPG\share\gpg4win\HOWTO-SMIME.en.txt	07/10/15 12:49:04
Eraser.lnk	C:\Program Files\ Eraser\Eraser.exe	..\..\..\Program Files\Eraser\Eraser.exe	04/13/15 17:42:52
Mozilla Thunderbird.lnk	C:\Program Files (x86)\ Mozilla Thunderbird\ thunderbird.exe	.\..\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe	09/09/15 12:21:17
VeraCrypt.lnk	C:\Program Files\VeraCrypt\VeraCrypt.exe	..\..\..\Program Files\VeraCrypt\VeraCrypt.exe	09/29/15 11:48:33
migwiz.lnk		.\migwiz\migwiz.exe	07/14/09 01:29:02
Windows PowerShell (x86).lnk			07/08/08 03:27:28
Windows PowerShell.lnk			12/01/07 07:40:30
Windows PowerShell Modules.lnk			12/01/07 07:40:30
package_33_for_ kb2973112 ~31bf3856ad364e 35~amd64~ ~6.1.1.0.cat	C:\Users\	\..\..\..\Documents\EvgenyPub.asc	09/29/15 16:40:57
amd64_microsoft -windows-a..on-authui.resources_31bf3856ad364e35_6.1.7601.18896_de-de_405d3702c50a1cb6.manifest	C:\Users\	\..\..\..\Downloads\key0x48FE4AD3424A6212.asc	09/29/15 16:58:33
amd64_ c7aa7f000cd 0529384240fbaa 5f3a1_31bf3856ad364e35_ 6.1.7600.17184_ none_ f507a4ee201d1f07 .manifest	C:\Program Files \Bitcoin\bitcoin-qt.exe	..\..\..\..\..\..\..\..\..\..\Program Files\Bitcoin\bitcoin-qt.exe	06/01/15 02:00:00

md64_microsoft-windows-p..gssystems.resources_31bf3856ad364e35_6.1.7600.17184_pl-pl_b73dae6a60d720f5.manifest	C:\Users\	.\Browser\firefox.exe	01/01/00 01:00:00
ıd64_98bfd5c74c935312ac3e03acb2a7f4a5_31bf3856ad364e35_6.1.7600.17135_none_3944d92b5c708735.manifest	C:\Program Files (x86)\mIRC\mirc.chm	..\..\..\..\..\..\Program Files (x86)\mIRC\mirc.chm	07/22/15 15:55:27
amd64_microsoft-windows-kernel32.resources_31bf3856ad364e35_6.1.7600.17135_tr-tr_276ef69d75b71bcf.manifest	C:\Users\	..\..\..\..\..\ICQM\icq.exe	07/22/15 15:53:59
amd64_microsoft-windows-kernel32.resources_31bf3856ad364e35_6.1.7600.17135_uk-ua_c34ed9446ce8421b.manifest	C:\Users\	.\..\..\..\..\ICQM\icqsetup.exe	07/22/15 15:53:59
windows6.1-kb2791765-x64-express.cab	C:\Users\	..\..\..\..\..\filezilla_logfile.log	
amd64_76150c35973d684f2ae56aa95f4af9_31bf3856ad364e35_6.1.7601.21666_none_40b47d6a442fdcbd.manifest	C:\Program Files (x86)\mIRC\ircintro.chm	..\..\..\..\..\..\Program Files (x86)\mIRC\ircintro.chm	07/22/15 15:55:27
msil_system.runtime.remoting.resources_b77a5c561934e089_6.1.7601.18586_zh-tw_04a0df67ae70bbc9.manifest	C:\Program Files (x86)\mIRC\versions.txt	..\..\..\..\..\..\Program Files (x86)\mIRC\versions.txt	07/22/15 15:55:27
package_14_for_kb2978120~31bf3856ad364e35~amd64~~6.1.1.0.mum	C:\Users\	..\..\..\..\..\Pictures\cash.jpg	
amd64_aa754fdafa045c495dd8dcc5d9059d55_31bf3856ad364e35_6.1.7600.16905_none_3d0fe520648293e	C:\Users\	.\..\..\..\Downloads\keyserver2.pgp.comGlobalDirectoryKey.asc	09/29/15 16:44:49

0.manifest			
amd64_ be53602cba88de6253e1f14 1bd668d_31bf3856ad364 e35_6.1.7601.22948_none _255b55faf18e13f1.manif est	C:\Users\	..\..\..\..\Downloads\tails-i386- 1.5.1	09/09/15 12:09:54