Information Security and Computer Fraud, 2015, Vol. 3, No. 2, 25-31
Available online at http://pubs.sciepub.com/iscf/3/2/1
© Science and Education Publishing
DOI:10.12691/iscf-3-2-1

Investigation of Artefacts Left by BitTorrent Client in Windows 8 Registry

Algimantas Venčkauskas, Robertas Damaševičius, Nerijus Jusas, Vacius Jusas*, Stasys Maciulevičius, Romas Marcinkevičius, Kęstutis Paulikas, Jevgenijus Toldinas

Computer Department, Kaunas University of Technology, Kaunas, Lithuania
*Corresponding author: vacius.jusas@ktu.lt

Received August 28, 2015; Revised September 01, 2015; Accepted September 16, 2015

Abstract BitTorrent client application is a popular tool to download large files from Internet, but this application is quite frequently used for illegal purposes that are one of the types of cybercrimes. If order to fight against this type of cybercrime we carried out the research, during which we investigated the evidences left by BitTorrent client application in registry under Windows 8 operating system. The experiment was carried out in three steps: installation, download, and uninstallation. The snapshots of registry were taken and compared prior and after each step. Changes in Windows registry were collected and joined into tables. The experiment revealed that BitTorrent client application creates Windows registry artefacts that can contain information which might be used as evidence during an investigation. The evidence remains in the registry even after the removal of the application, although it can really prove the fact of usage of the application only. The investigation of file system can reveal the purpose and the contents of the BitTorrent client session.

Keywords: *BitTorrent protocol, forensics investigation, forensic evidence, registry*

Cite This Article: Algimantas Venčkauskas, Robertas Damaševičius, Nerijus Jusas, Vacius Jusas, Stasys Maciulevičius, Romas Marcinkevičius, Kęstutis Paulikas, and Jevgenijus Toldinas, “Investigation of Artefacts Left by BitTorrent Client in Windows 8 Registry.” *Information Security and Computer Fraud*, vol. 3, no. 2 (2015): 25-31. doi: 10.12691/iscf-3-2-1.

1. Introduction

As technology of Internet of Things and Services rapidly improves, new online services such as cloud computing architectures and peer-to-peer (P2P) protocols came to every day use. These services improve life of computer users having limited resources. Cloud computing offers storage and calculation facilities. P2P protocols come in two flavors: server-based model and direct communication between two computers ("peers") without participation of central authority – server.

Steve Crocker suggested an idea of P2P network services in 1969 [1]. P2P technology is now widely used in many application fields including (1) sharing of various type files, such as BitTorrent protocol, (2) instant messaging, like Skype and ICQ, (3) grid computing.

BitTorrent protocol was not the first one designed for file sharing. However, it was the most elaborate and became de facto standard for file sharing over Internet. BitTorrent protocol was designed with good intent but it is quite largely used for sharing of copyrighted material [2]. Illegal copies of copyrighted content can be found in more than two thirds of torrents registered at one of the most popular BitTorrent trackers [3]. Consequently, such use of protocol creates illegal revenue that downgrades the copyright holder’s share. Therefore, the use of BitTorrent protocol for illegal purposes creates new type of cybercrime and new challenges for forensics investigators in order to fight against it. Moreover, the users involved in the use of BitTorrent protocol have to allow using their resources for file sharing since BitTorrent applications may punish non-uploaders by limiting their download bandwidth [4]. In such a way, the users, which desire the service, are indirectly involved in committing cybercrimes.

Family of products using BitTorrent protocol constantly evolves and increases. The most recent product in this family is BitTorrent Sync. It is a file replication utility released as private alpha in April 2013 [5]. This utility is very desirable to those who are involved in illegal activities, because it ensures to keep data transfer secure from inspection while in transit [6]. Therefore, the utility can be exploited for several potential crimes as follows: to share copyrighted material, to share child pornography, to distribute malicious software, for industrial espionage, etc.

Not only the application software is developed, the operating system software is developed, as well. Several years ago Microsoft delivered new version of operating system, Windows 8. The purpose of the paper is to investigate and locate artefacts left by BitTorrent client in Windows 8 operating system registry. This will include artefacts created during installation of the software, downloading and uploading activity and the artefacts left after the user uninstalls the application. We will carry out the analysis to determine which information may be useful as forensic evidence in tracing a user’s file sharing activity.

In the next section, we review the concepts used and services provided by BitTorrent protocol.

2. BitTorrent Service

Programmer Bram Cohen is the author of the BitTorrent protocol [7]. He released the first version of the protocol in July of 2001. Later he released it to the public as an open source technology. Since the project was successful, B. Cohen established a company BitTorrent, Inc., which offers now numerous BitTorrent clients for many existing computing platforms, including smart phones.

An universe of BitTorrent protocol can be regarded as the structure consisting of several levels of hierarchy. At the highest level, the universe of BitTorrent network can be represented as being divided into many BitTorrent swarms. Each shared content forms a BitTorrent swarm that is composed of trackers and peers [8]. A peer is an agent that runs an implementation of the protocol. The same peer can participate in multiple swarms, if he wishes to share several files. Every peer participating in the swarm can act in two positions: seeder or leecher. A peer is a seeder having the whole content available and as such is uploading data only. A peer is a leecher that is either in the beginning of the process or in the middle of the process of downloading information from the swarm.

In order to initiate a download of the content the user must firstly download a metadata .torrent file from some website. Then, the BitTorrent client application of the user interprets the metadata and uses it to detect other peers participating in that swarm using one of the following methods: tracker, distributed hash table (DHT), peer exchange (PEX). A tracker is a server that maintains a list of seeders and leechers. During content transfer, the client application periodically reports to the tracker in order to update its status and to keep up to date the list of active peers. PEX allows a direct interchange of peer lists with other peers.

DHT is a distributed tracker that allows peers to locate the other peers requesting information from BitTorrent clients without the requirement for a central server. DHT implemented in BitTorrent client is called Mainline. The results of recent measurement show that Mainline DHT is the largest P2P network having from 15 million to 27 million users concurrently online, with a daily churn of at least 10 million users [9].

The BitTorrent protocol reduces the impact of distributing large files on both the server and the network. The main strength of the protocol is the division of the file into separate equal size parts and separate management of these parts. Instead of downloading a file from a single source, BitTorrent enables users to join a swarm of peers. In the swarm, peers simultaneously download and upload from each other. In addition, protocol is adaptive to low band networks since it divides the file into smaller pieces in this case.

The file to be distributed is divided into pieces. When peer receives a new piece of the file, it becomes a source for other peers. Therefore, those peers, who participate in the swarm, have an obligation to allow using their resources for content distribution. Once the user is connected with the swarm, he can download available pieces from several peers (seeder and leechers) simultaneously. This mechanism improves the download speed.

The pieces of a file are downloaded randomly and the BitTorrent client rearranges them into the correct order. The client also monitors which pieces it has, which it can upload to other peers, and which it needs. In separate swarm, all the pieces of the file are of the same size (for example, a 100 MB file can be downloaded as ten 10 MB pieces or as five 20 MB pieces).

The artefacts left by BitTorrent client can be separated into two parts: 1) the artefacts on the client computer, and 2) the artefacts on the computer network. In the next section, we review the related work that considers the artefacts on the client computer.

3. Review of Related Work

We present the review of related work in chronological order of their appearance since it can be easier to understand the directions of the development of forensics investigation of BitTorrent clients on the local computer.

Adelstein and Joyce [10] presented a File Marshal tool for automatic detection and analysis of peer-to-peer client use on a computer disk. It was the first tool, announced in 2007, to automate the extraction of P2P data on the client computer. The File Marshal is an universal tool, since it is not associated to the particular P2P protocol. The configuration file is used to indicate the location of log files and names of registry keys. If special code is required to analyze a file (e.g., to decode a hash list or date format), the configuration file lists the Java modules to be used for parsing; new parsers have to be created as needed. So, File Marshal for its universality heavily relies on the right preparation of the configuration file. Moreover, the File Marshal initially did not include the analysis of the BitTorrent protocol.

The File Marshal operates on a mounted disk image. The tool examines the registry, looks for the presence of files, directories, allows searching for various usage-specific items, including IP addresses and DNS names of peer servers, names of files, and file hashes. File Marshal is able to examine alternate or backup registry files, in case some of the keys had been purged from the active registry when the computer was seized and the disk imaged. However, because File Marshal performs an offline analysis of static registry files, there is little support for retrieving keys and values from a file.

In order to provide all the tasks in a forensically valid way File Marshal logs all the operations it performs.

File Marshal provides log information, including peer or bootstrap servers contacted, files downloaded and shared, and other forensically sound data maintained by the specific P2P client. Since, the BitTorrent protocol was not included into the presented version of File Marshal, it is not possible to know what specific information is collected for BitTorrent client.

In order to provide all the tasks in a forensically valid way File Marshal logs all the operations it performs. Later File Marshal project was renamed to P2P Marshal [11].

Woodward and Valli [12] considered whether current erasure programs remove evidence of BitTorrent activity. The erasure programs MaxErase, P2PDoctor, Privacy

Suite, Window Washer, Windows R-Clean and Wipe were examined on a machine that had used the BitTorrent client Azureus. Woodward and Valli concluded that the current erasure tools are not effective at removing traces of BitTorrent activity.

In the next study, Woodward [13] examined whether current BitTorrent clients running on Windows 7 leave behind the meaningful data. The secondary goal of the investigation was to determine whether the artefacts created differ from Windows XP, and whether the locations of this information has changed. The popular BitTorrent clients programs BitCommet, BitTornado, µTorrent, and Vuze (formerly Azureus) were investigated using default settings. The investigation was limited to the topical analysis and examined the registry and local data area within Windows operating systems. Woodward determined that all BitTorrent client programs produced the same data as a function of their operation. This data could be used to locate the initial source of a downloaded file. It was also found that the key difference between Windows 7 and Windows XP was the location of the BitTorrent configuration files on the local computer.

Lallie and Briggs [14] explored three popular BitTorrent client applications, BitComet, Vuze and µTorrent and outlined the registry artefacts that are produced by the installation and use of these programs on a Windows 7 client. Several authors [13], [15] were already sceptic about the evidential value of registry keys before publication of this study. Many artefacts are produced in the registry keys, but they mainly identify that a BitTorrent client has been run on the computer only. The most significant data discovered in the registry was identified in the BitComet sub-key that contains a record of the website URL from which the last torrent was opened and downloaded [15]. Lallie and Briggs confirmed already known result that the artefacts of the registry keys can only prove who installed each application and which users used the software.

The presented research works so far analyzed the artefacts left by BitTorrent client programs in Windows registry and in local file folders. Windows operating system creates special type of files, which are event logs, used to record significant events on computer, such as user logging on to the computer or encountering an error by a program. Sahoo et al. [16] explored the various processes involved in the Windows event logging environment and stressed the centralization of the logging process. The proposed architecture to centralize the storage of log data enhances the security of the logging data that are important for forensic investigation.

In the next section, we present the methodology used during the experiments.

4. Methodology of the Experiment

The research was based on the recent version of the BitTorrent client application: 7.9.3.40634 (TimeStamp Friday, June 26, 2015). This version was chosen because it has all the latest developments and it is representative of new technologies. The typical installation recommended by BitTorrent was applied. For this application, installation and usage data was collected and then analyzed.

For the experiment, we have used Windows host machine and eight virtual machines. Seven virtual machines were used to download the file that was proposed for sharing on eight virtual machine. Virtual machines were connected to the Internet during file download only using private network and virtual server Guest Default Gateway with Forefront Threat Management Gateway 2010 installed to protect virtual machines from threats. The hardware and software used in the machines are presented in Table 1.

Table 1. Parameters of the machines

Name	Host	Guest Default Gateway	Virtual machines
Operating system	Windows Server 2008 R2 Enterprise SP1 (64 bit)	Windows Server 2008 R2 Enterprise SP1 (64 bit) with Microsoft Forefront Threat Management Gateway 2010	Windows 8.1 Enterprise (64 bit)
Virtualization technology	Hyper-V Manager Microsoft Version: 6.1.7601.17514		
Windows updates	All latest updates were installed	All latest updates were installed	All latest updates were installed
Processor	Intel® Core™ i5 CPU 650 @ 3.20Ghz	Intel® Core™ i5 CPU 650 @ 3.20Ghz	Intel® Core™ i5 CPU 650 @ 3.20Ghz
RAM	12 GB	2048 MB	4096 MB
Network adapter	Realtek PCI GBE Family Controller	External Network Adapter connected to the Realtek PCI GBE Family Controller & Private Network Adapter connected to the Microsoft Virtual Switch	Private Network Adapter connected to the Microsoft Virtual Switch

Data was collected using a free and open source utility Regshot (regshot_x64.exe) that allows to take quickly a snapshot of registry and then compare it with a second one.

The experiment was carried out in three following steps:

- Installation of BitTorrent client;
- Download of file using BitTorrent client;
- Uninstallation of BitTorrent client.

The goal was to find out all the changes that BitTorrent client makes to Windows registry, therefore, the snapshots were taken prior and after each step of the experiment.

In the next section, we provide and discuss the results of the experiment.

5. Artefacts of BitTorrent Client in Windows Registry

Every activity of any application is registered with Windows registry. We collected the data of changes in Windows registry for all the steps of the experiment. We provide Windows registry hives affected by BitTorrent client in Table 2.

The denotation “USER SID” used in Table 2 identifies the user security identifier such as follows: S-1-5-21-

2954371515-1340710186-4262677133-1001. The denotation “USER SID_Classes used in Table 2 identifies the user security identifier such as follows: S-1-5-21-2954371515-1340710186-4262677133-1001_Classes.

Table 2. Windows registry hives modified by BitTorrent

When	Hive	Acronym	Action with registry
Installation	HKEY_LOCAL_MACHINE\SYSTEM	HKLM\SYST	Firewall rules added
	HKEY_LOCAL_MACHINE\SOFTWARE	HKLM\SW	Keys and values added
	HKEY_USERS\USER SID\SOFTWARE	HKU\US\SW	Keys and values added
	HKEY_USERS\USER SID_Classes	HKU\USCL	Keys and values added
Download	HKEY_USERS\USER SID	HKU\US	Keys and values added
Uninstallation	HKEY_LOCAL_MACHINE\SYSTEM	HKLM\SYST	Firewall rules deleted
	HKEY_LOCAL_MACHINE\SOFTWARE	HKLM\SW	Keys and values deleted
	HKEY_USERS\USER SID\SOFTWARE	HKU\US\SW	Keys and values deleted
	HKEY_USERS\USER SID_Classes	HKU\USCL	Keys and values deleted

In the next three subsections, we provide affected Windows registry values for all three steps of the experiment.

5.1. Installation

Installation process adds several keys and values to different Windows registry hives. The effects on Windows registry hive values are provided in the following tables: Table 3, Table 4, Table 5, Table 6. The tables are arranged according to the contents of rows in Table 2.

Windows registry hive HKEY_USERS\USER SID\SOFTWARE collects and stores all the available information about BitTorrent application (Table 5). This registry hive is especially important since it allows knowing what application is installed. Table 5 is large, but it is very significant, since Table 5 reveals all the information stored about application.

Table 3. HKLM\SYST

<table>
<tr><th>Registry path</th><th>Registry values</th></tr>
<tr><td>HKLM\SYST\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\</td><td>{82DC8AFA-E652-400B-892B-87722CAA7EEB}: "v2.22|Action=Allow|Active=TRUE|Dir=In|Protocol=6|App=C:\Users\Eugenijus\AppData\Roaming\BitTorrent\BitTorrent.exe|Name=BitTorrent (TCP-In)|Desc=Allow BitTorrent network traffic with Edge Traversal|Edge=TRUE|"</td></tr>
<tr><td>HKLM\SYST\ControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\</td><td>{82DC8AFA-E652-400B-892B-87722CAA7EEB}: "v2.22|Action=Allow|Active=TRUE|Dir=In|Protocol=6|App=C:\Users\Eugenijus\AppData\Roaming\BitTorrent\BitTorrent.exe|Name=BitTorrent (TCP-In)|Desc=Allow BitTorrent network traffic with Edge Traversal|Edge=TRUE|"</td></tr>
</table>

Table 4. HKLM\SW

Registry path	Registry keys	Registry values
HKLM\SW\Classes\MIME\Database\Content Type\	application/x-bittorrent	Extension: ".torrent"
	application/x-bittorrent-app	Extension: ".btapp"
	application/x-bittorrent-appinst	Extension: ".btinstall"
	application/x-bittorrent-key	Extension: ".btkey"
	application/x-bittorrent-skin	Extension: ".btskin"
	application/x-bittorrentsearchdescription+xml	Extension: ".btsearch"
HKLM\SW\Microsoft\Windows\CurrentVersion\UFH\	ARP	0: 'User SID\Software\Microsoft\Windows\CurrentVersion\Uninstall BitTorrent "C:\Users\User\AppData\Roaming\BitTorrent\BitTorrent.exe" /UNINSTALL'

5.2. Download

During download process, single registry hive HKEY_USERS\USER SID\SOFTWARE is modified. The modified values are provided in Table 7. The registry value provided for the key “torrent” differs in every experiment.

5.3. Uninstallation

To uninstall BitTorrent client application, we explored two modes: a) without remove settings and b) with remove settings. As it can be expected, uninstallation in both modes completely destroys all the Windows registry hive values created during installation and provided in Table 3, Table 4, Table 5, and Table 6. But both modes of uninstallation leave registry values created during download process and provided in Table 7. Thus, even after the uninstallation of BitTorrent client is carried out, forensic investigator can establish the fact of use of BitTorrent client application on the base of Windows registry hive HKEY_USERS\USER SID\SOFTWARE. This is very important finding for forensic investigator; uninstallation of BitTorrent client application does not completely remove evidence from Windows registry hive. Forensic investigator using established fact of the exploitation of BitTorrent client can provide deeper analysis to learn the purpose of the employment of the application. Such information can not be obtained from Windows registry. The analysis of the file system is needed.

Table 5. HKU\US\SW

Registry path	Registry keys	Registry values
HKU\US\SW\Classes\MIME\Database\Content Type\\	application/x-bittorrent	Extension: ".torrent"
	application/x-bittorrent-app	Extension: ".btapp"
	application/x-bittorrent-appinst	Extension: ".btinstall"
	application/x-bittorrent-key	Extension: ".btkey"
	application/x-bittorrent-skin	Extension: ".btskin"
	application/x-bittorrentsearchdescription+xml	Extension: ".btsearch"
HKU\US\SW\Microsoft\Windows\CurrentVersion\Uninstall\	BitTorrent	DisplayIcon: "C:\Users\User\AppData\Roaming\BitTorrent\BitTorrent.exe,0"'
		DisplayName: "BitTorrent"
		DisplayVersion: "7.9.3.40634"
		UninstallString: ""C:\Users\User\AppData\Roaming\BitTorrent\BitTorrent.exe" /UNINSTALL"
		InstallLocation: "C:\Users\User\AppData\Roaming\BitTorrent"
		MajorVersion: 0x00000007
		MinorVersion: 0x00000009
		URLInfoAbout: "http://www.bittorrent.com"
		Publisher: "BitTorrent Inc."
		HelpLink: "http://www.bittorrent.com/btusers/guides"
HKU\US\SW\Classes\	.btapp	:"BitTorrent" Content Type: "application/x-bittorrent-app"
	.btinstall	:"BitTorrent" Content Type: "application/x-bittorrent-appinst"
	.btkey	:"BitTorrent" Content Type: "application/x-bittorrent-key"
	.btsearch\OpenWithProgids	BitTorrent: ""
	.btsearch	:"BitTorrent" Content Type: "application/x-bittorrentsearchdescription+xml"
	.btskin	:"BitTorrent" Content Type: "application/x-bittorrent-skin"
	.torrent\OpenWithProdigs	BitTorrent: ""
	.torrent	:"BitTorrent" Content Type: "application/x-bittorrent"
HKU\US\SW\Classes\Applications	BitTorrent.exe\shell	: "open"
	BitTorrent.exe\shell\open\command	:""C:\Users\User\AppData\Roaming\BitTorrent\BitTorrent.exe" "%1" /SHELLASSOC"

Table 6. HKU\USCL

Registry path	Registry keys	Registry values
HKU\USCL\MIME\Database\Content Type\	application/x-bittorrent	Extension: ".torrent"
	application/x-bittorrent-app	Extension: ".btapp"
	application/x-bittorrent-appinst	Extension: ".btinstall"
	application/x-bittorrent-key	Extension: ".btkey"
	application/x-bittorrent-skin	Extension: ".btskin"
	application/x-bittorrentsearchdescription+xml	Extension: ".btsearch"
HKU\USCL\	.btapp	:"BitTorrent" Content Type: "application/x-bittorrent-app"
	.btinstall	:"BitTorrent" Content Type: "application/x-bittorrent-appinst"
	.btkey	:"BitTorrent" Content Type: "application/x-bittorrent-key"
	.btsearch\OpenWithProgids	BitTorrent: ""
	.btsearch	:"BitTorrent" Content Type: "application/x-bittorrentsearchdescription+xml"
	.btskin	:"BitTorrent" Content Type: "application/x-bittorrent-skin"
	.torrent\OpenWithProdigs	BitTorrent: ""
	.torrent	:"BitTorrent" Content Type: "application/x-bittorrent"
HKU\USCL\Applications	BitTorrent.exe\shell	: "open"
	BitTorrent.exe\shell\open\command	:""C:\Users\User\AppData\Roaming\BitTorrent\BitTorrent.exe" "%1" /SHELLASSOC"

Table 7. Effects of download

Registry path	Registry keys	Registry values
HKU\US\SW\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\	torrent	0: 14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 32 00 2E 80 53 16 DD 3A 32 EB B0 4C BB D7 DF A0 AB B5 AC CA 1E 00 00 00 25 00 EF BE 11 00 00 00 31 5A 28 65 32 B7 D0 01 98 BA A3 86 0C C3 D0 01 14 00 8A 00 32 00 06 08 00 00 F4 46 78 7E 20 00 45 55 47 45 4E 49 7E 31 2E 54 4F 52 00 00 6E 00 09 00 04 00 EF BE F4 46 9C 86 F4 46 9C 86 2E 00 00 00 A6 01 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0B 0B 18 00 45 00 75 00 67 00 65 00 6E 00 69 00 6A 00 75 00 73 00 20 00 44 00 53 00 43 00 30 00 34 00 39 00 36 00 37 00 2E 00 6A 00 70 00 67 00 2E 00 74 00 6F 00 72 00 72 00 65 00 6E 00 74 00 00 00 1C 00 00 00
		MRUListEx: 00 00 00 00 FF FF FF FF
HKU\US\SW\ Microsoft\Windows\CurrentVersion\Explorer\FileExts\.torrent	OpenWithList	a: "BitTorrent.exe"
		MRUList: "a"

The mode of the uninstallation “with remove settings” leaves additional undestroyed values in Windows registry hive in comparison with the mode “without remove settings”. These values are provided in Table 8 and Table 9. Table 8 contains the values left in Windows registry hives HKEY_CLASSES_ROOT\Local Settings\Software and in HKEY_USERS\USER SID_Classes.

Table 9 holds the values left in Windows registry hives HKEY_CURRENT_USER and in HKEY_USERS\USER SID_Classes.

Table 8. Information left in USER SID Classes

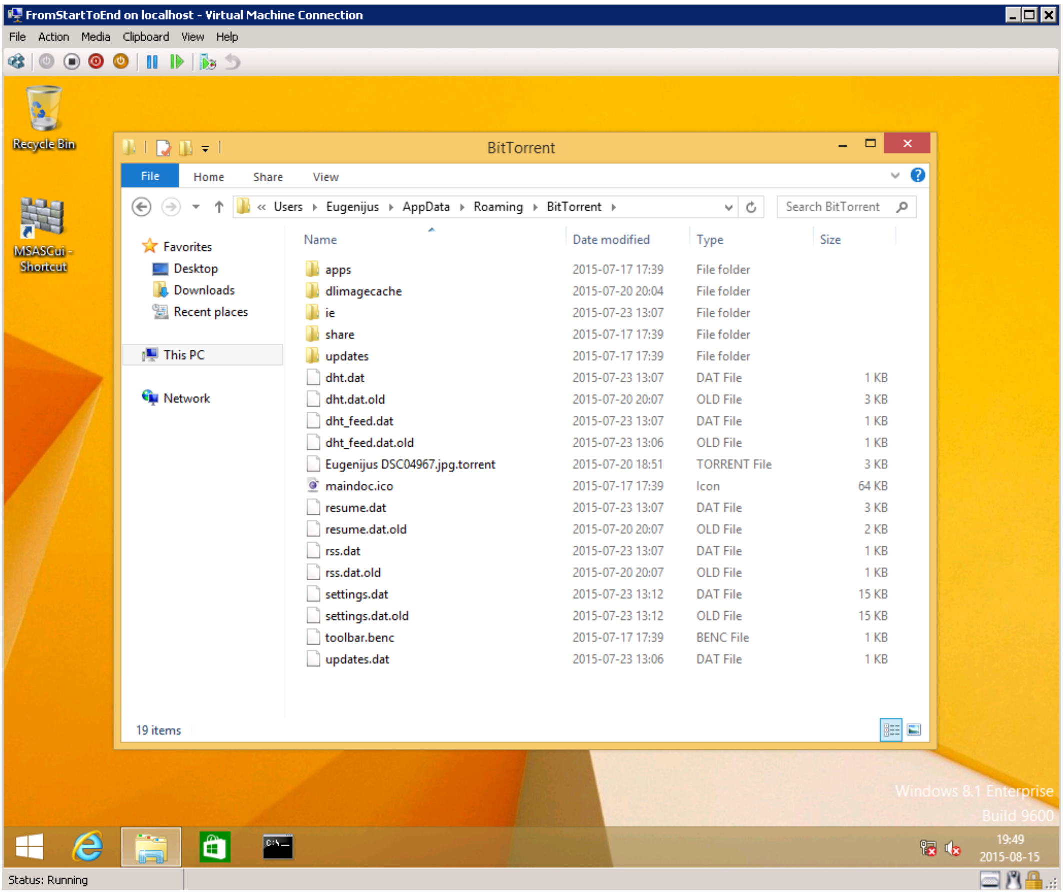
Registry path	Registry keys	Registry values
Microsoft\Windows\Shell\MuiCache \	C:\Uers\User\Downloads\ BitTorrent.exe.ApplicationCompany	BitTorrent Inc.
	C:\Uers\User\Downloads\ BitTorrent.exe.FriendlyAppName	BitTorrent

Table 9. Current user information

Registry path	Registry keys	Registry values
Software\Microsoft\Internet Explorer\DOMStorage\bittorrent.com	NumberOfSubdomain	0x00000001
	Total	0x000001bf
Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BROWSER_EMULATION	BitTorrent.exe	0x00002328
Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SCRIPTURL_MITIGATION	BitTorrent.exe	0x00000001

So, the mode of the uninstallation “with remove settings” leaves more information in Windows registry.

The explored modes of uninstallation demonstrate quite a different behavior for the file system. The mode of the uninstallation “with remove settings” completely removes all the files related to BitTorrent client application. The mode of the uninstallation “without remove settings” deletes executable file BitTorrent.exe only (Figure 1).



Name	Date modified	Type	Size
apps	2015-07-17 17:39	File folder	
dlimagecache	2015-07-20 20:04	File folder	
ie	2015-07-23 13:07	File folder	
share	2015-07-17 17:39	File folder	
updates	2015-07-17 17:39	File folder	
dht.dat	2015-07-23 13:07	DAT File	1 KB
dht.dat.old	2015-07-20 20:07	OLD File	3 KB
dht_feed.dat	2015-07-23 13:07	DAT File	1 KB
dht_feed.dat.old	2015-07-23 13:06	OLD File	1 KB
Eugenijus DSC04967.jpg.torrent	2015-07-20 18:51	TORRENT File	3 KB
maindoc.ico	2015-07-17 17:39	Icon	64 KB
resume.dat	2015-07-23 13:07	DAT File	3 KB
resume.dat.old	2015-07-20 20:07	OLD File	2 KB
rss.dat	2015-07-23 13:07	DAT File	1 KB
rss.dat.old	2015-07-20 20:07	OLD File	1 KB
settings.dat	2015-07-23 13:12	DAT File	15 KB
settings.dat.old	2015-07-23 13:12	OLD File	15 KB
toolbar.benc	2015-07-17 17:39	BENC File	1 KB
updates.dat	2015-07-23 13:06	DAT File	1 KB

Figure 1. The files left after uninstallation in the mode “without remove settings”

Consequently, if the mode of uninstallation “without remove settings” was used, the forensic investigator can quite easy learn the purpose and the contents of BitTorrent client session since almost all the files of BitTorrent are left undestroyed. The more difficult situation for forensic investigator is in the case of usage of the mode of the uninstallation “with remove settings”. In the latter situation, the forensic investigator has to use utility to restore file system.

6. Conclusion

BitTorrent client application is a popular tool to download large files from Internet. The application was created having good intentions in mind but this application is quite frequently used for illegal activities that are some sort of cybercrimes. In order to fight this type of cybercrime we carried out the research, during which we investigated the evidences left by BitTorrent client application under Windows 8 operating system. The experiment was carried out in three steps: installation, download, and uninstallation. The snapshots of registry were taken and compared prior and after each step.

To remove the evidence of the usage of the application, the performed actions by uninstallation procedure are very important. Therefore, we have carried out the experiment and explored the uninstallation procedure in two modes: a) without remove settings and b) with remove settings. Both modes leave evidence in Windows registry. The mode “with remove settings” leaves more artefacts in Windows registry, but this mode completely removes files related to BitTorrent application. Meanwhile, the uninstallation mode “without remove settings” leaves files related to BitTorrent application almost untouched, except executable file.

We can conclude that BitTorrent client application creates Windows registry artefacts that can contain information which might be used as evidence during an investigation. It also has been shown that the evidence remains in the registry even after the removal of the application, although it can really prove the fact of usage of the application only. Therefore, the investigation of registry allows making the decision about the need for further directed analysis of the other software on the particular computer. The investigation of file system can really reveal whether the cybercrime using BitTorrent client application was committed.

Acknowledgement

The investigation presented in this paper has been carried out partially within the project “Lithuanian Cybercrime Centre of Excellence for Training, Research and Education”, Grant Agreement No HOME/2013/ISEC/AG/INT/4000005176, co-funded by the Prevention of and Fight against Crime Programme of the European Union.

References

[1] Horng, M.-F., Chen, C.-W., Chuang, C.-S. and Lin, C.-Y., "Identification and Analysis of P2P Traffic - An Example of BitTorrent,” in *Proceedings of First International Conference on Innovative Computing Information and Control.* 266-269. 2006.

[2] Park, S., Chung, H., Lee, C., Lee, S. and Lee, K., "Methodology and Implementation for Tracking the File Sharers using BitTorrent,” *Multimedia Tools Appl.* 74(1). 271-286. 2015.

[3] Schmidt, A. H., Antunes, R. S., Barcellos, M. P. and Gaspary, L. P., "Characterizing Dissemination of Illegal Copies of Content through Monitoring of BitTorrent Networks," in*: Proceedings of Network Operations and Management Symposium (NOMS)*, 327-334. 2012.

[4] Liberatore, M., Erdely, R., Kerle, T., Levine, B. N. and Shields, C., "Forensic investigation of peer-to-peer file sharing networks," *Digital Investigation*, 7, S95-S103. 2010.

[5] Farina, J., Scanlon, M. and Kechadi, M-T., "BitTorrent Sync: First Impressions and Digital Forensic Implications,” *Digital Investigation*, 11(S1), S77-S86. May 2014.

[6] Scanlon, M., Farina, J. and Kechadi, M-T., "BitTorrent Sync: Network Investigation Methodology," in *Proceedings of Ninth International Conference on Availability, Reliability and Security (ARES 2014)*, Fribourg, Switzerland, 21-29. September 2014.

[7] Cohen, B., “Incentives Build Robustness in BitTorrent,” in *Proceedings of the Workshop on Economics of Peer-to-Peer systems*, 6, 68-72. 2003.

[8] Mansilha, R. B., Bays, L. R., Lehmann, M. B., Mezzomo, A., Gaspary, L. P. and Barcellos, M. P., "Observing the BitTorrent Universe through Telescopes," in *Proceedings of International Symposium on Integrated Network Management*, 1-8. 2011.

[9] Wang, L. and Kangasharju, J., "Measuring Large-Scale Distributed Systems: Case of BitTorrent Mainline DHT," in: *Proceedings of IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P)*, 1-10. 2013.

[10] Adelstein, F. and Joyce, R. A., "File Marshal: Automatic extraction of peer-to-peer data,” *Digital Investigation*, 4 (S1). S43-S48. 2007.

[11] P2P Marshal. [Online]. Available: http://forensicswiki.org/wiki/P2PMarshal. [Accessed June 29, 2015].

[12] Woodward, A. J. and Valli, C., "Do Current Erasure Programs Remove Evidence of BitTorrent Activity?" in: *Proceedings of Conference on Digital Forensics, Security and Law*, 147-158. 2007.

[13] Woodward, A., "Do Current BitTorrent Clients running on Windows 7 beta leave behind meaningful data?" in: *Proceedings of International Conference on Security and Management*, 622-627. 2009.

[14] Lallie, H. S. and Briggs, P. J, "Windows 7 registry forensic evidence created by three popular BitTorrent clients," *Digital Investigation*, 7(3-4). 127-134. 2011.

[15] J. Acorn and J. Austin. "Forensic Studies in BitTorrent,” *Produced by the Information Security Group at Royal Holloway, University of London in conjunction with TechTarget*, 2008. [Online]. Available: http://cdn.ttgtmedia.com/searchSecurityUK/downloads/RH6_Acorn.pdf. [Accessed June 30, 2015].

[16] Sahoo, P.K., Chottray, R. K. and Pattnaiak, S., "Research Issues on Windows Event Log,” *International Journal of Computer Applications*, 41(19), 23-29. March 2012.