Problem Statement

In the past few decade internet has become an essential part of life. Browsers are used to access the Internet. Concern for privacy and anonymity is increasing day by day due to many reasons. In the meantime, popularity of browsers that promises to maintain privacy and keep anonymity of internet activity is also increasing. Tor browser is one of such applications. It is popular among different user groups. It is used by user to carryout both normal and illegal activities on the Internet. The Tor browser allows to hide identity while doing the online activity, it is built in such a way that it leaves very few traces of digital evidence also known as artifacts in the accused computer. It creates much difficulty while gathering and analyzing artifacts in the accused computer to provide forensically sound findings. A forensic scenario may occur differently from ideal scenarios of browsing the Internet using the Tor browser as the suspect may have attempted to alter the past activity carried out in it. So it becomes tough to find out artifacts in cases where alteration has been done by the accused individual in the computer i.e. deleting visited website history, uninstalling the browser, etc.

Abstract

The Tor system is a favorite, encrypted, global, anonymizing digital system available since 2002 and is traditionally used by most factors of society like privacy advocates, journalists, authorities, and offenders. This analysis will offer a forensic investigation of this Tor Browser latest variant client on a Windows-10 server for someone or group thinking about remnants made by this computer software. This study will utilize various free and commercial tools to provide a detailed analysis of registry artifacts as well as a comparison between pre- and post-connection to the Tor network using registry analysis. This study will try further to emphasize on registry rebuilding as a method to find out artefacts that are lost due to registry modification.

Introduction

Web Browsers are on the list of most frequently used software to get into the internet from any stage now. With recent electronic episodes regarding violation of information, users are getting to be more aware of the hazard posed by malicious celebrities using personal data in addition to susceptible software, which might undermine their information. For this reason, users are increasingly being offered solitude retaining solutions for hope adulthood. The onion (Tor) browser is also just one such application that not just ensures that the privacy preservation targets but in addition provides assuring anonymity. As a result of the feature, better part of the users utilize Tor browser to get ordinary utilization in addition to malign pursuits. As a way to confirm the claims of Tor browser and also help digital forensic researchers and research workers, we generated different cases to forensically analyze the Tor browser solitude and anonymity. As a consequence of the findings, it might be reasoned that the Tor browser renders various sensitive electronic artifacts onto the system, which is further utilized to undermine user data.

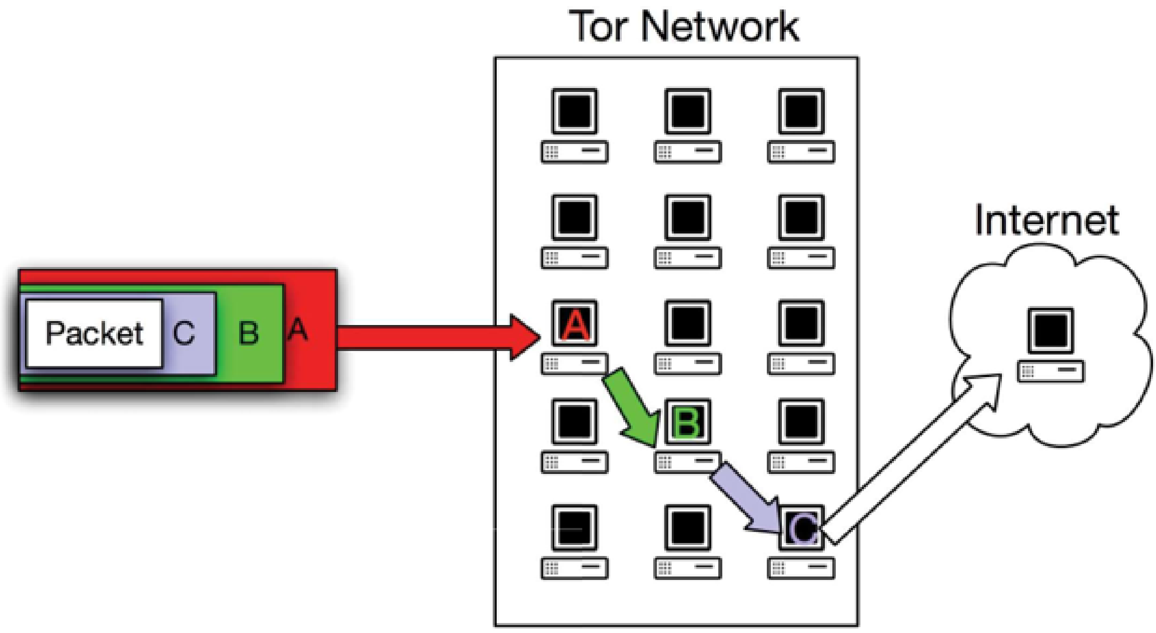
In Order to safeguard sensitive details, users have begun to effect changes within their usually missed surfing habit. The Tor browser is thought of as one among the methods that supply the much-desired consumer solitude. Yet it introduces a fantastic challenge to forensic researchers that attempts to rebuild the previous surfing heritage, in the event there is any computer occurrence. This study assesses the remaining traces of left-handed by the TOR browser. Additionally, it suggests a methodology that helps researchers to effortlessly test activities connected with a Tor browser related to prevalence response. What's more, it assesses the possibility of registry rebuild because of its own evidential potential. The renovation of remaining artifacts left to the victim computer at this browser that may function as evidence that's admissible in the court of law will also be discussed.

The rising usage of Encrypted data inside file storage and also in system communications leaves researchers that have many challenges. Probably one of the hardest is that the Tor protocol, even because its principal focus is always to guard the privacy of their user, in either its community footprint in just a server and above a network connection [1]. Even the Tor browser, even however, can render behind digital artifacts that may be employed by an investigator. This paper summarizes an experimental procedure and supplies consequences for signs paths that might be used within real-time investigations.

Browsers are widely used on Computers, laptops, and mobile devices. Within this phase, we want to find out and compare that which forensic artifacts might also be retrieved from TOR. Our investigation has been largely run with registry application so as to reproduce the method and abilities of an electronic digital forensics laboratory with limited tools. After indistinguishable statistics creation across all browsers and also manners of surfing in a controlled digital setting, forensic graphics were recorded subsequently examined. This study not just expands the present area of digital forensics where artifacts are available by which areas but additionally affirms various claims as it pertains to the solitude of private browsing manners [2]. Just as expected, all data had been retrieved from routine surfing styles, very nominal data from browsing, and nearly evident artifacts out of TOR .

Internet crime is now a severe issue. Cyber-criminals make use of the Darknet to market several applications tools from the marketplace, such as DDOS-attack applications, ransom-ware, Crimeware-as-a-service (CaaS), and also other cybercrime tools. Users can utilize the Tor browser using incognito works to join into the Darknet and run trades in the black market [3]. In any case, you can find a few anonymous plugins with the purposes of concealing the page activities of all users. Even though these browsers can't be used for connecting into this Darknet right, and they are able to let a criminal hook up into the net anonymously and then hide all of the criminal pursuit. Hence, the analysis of digital signs from the used recordings of browsers that are anonymous is filled with significant challenges. Within this paper, we demonstrate the way that programs and tools can be utilized in the forensic investigation of browsers that are anonymous. The experimental results reveal the capacity for these programs and tools from the analysis of digital signs.

Tor Browser works on the concept of connecting to the Internet via multi-layer encryption with multiple hops. There is a network of Tor hopes running as a node called a Tor network [4]. When a user request for a website (indexed and non-indexed), multiple layers of encryption is added to the request packet data, and it passes through many hops in the middle as represented below in the diagram. These hops are also known as a node. Each hop removes previous outer layer encryption and uses its own encryption while passing the packets to the next nodes [5]. At the last node, these encryptions are removed, and naked packets are delivered to the server where the website is hosted. This first node and last node, here represented as A and B is called as entry relay and exit relay respectively [5]. As the server replies with the resources the same procedure is followed to send it back to the end-user. In this way, the server never knows who was the original requester of the resources [5].



(Fig- 1 Picture credit: Aron Warren [6])

Internet security has turned into an important and growing issue for several decades. Really, Internet internet explorer has been daily used by the majority of individuals and will be seen on laptops, mobile devices, mobile devices, gaming consoles, smart televisions, and in wrist-watches, cars, and appliances. Along with clearing their surfing history, end users may even prevent the storage of such advice using 'private browsing' features and applications. Clients might decide to make use of private browsing tools and features for a number of reasons, for example, internet gift purchasing, analyzing and debugging sites, and obtaining computers that are public. In any case, offenders are using numerous procedures to obtain data in the exceptionally lucrative cyber-crime enterprise.

Registry artifacts consult with pieces of information an operating system records, as soon as a user has been using their computer. These pieces of data have been user/session special and offer all advice concerning using a specific application or application in addition to the essential period stamps [7]. An electronic digital forensic analyst should know about such artifacts as a way to do a legally satisfactory, precise, and tool-independent investigation of a system that is contested. This study gives a thorough guide for most forensic artifacts out there at a windows-10 environment [6]. These artifacts provide both qualitative and probative evidence to an investigator and sort vital preliminaries of episode response at an electronic digital offense scenario.

Forensic artifacts of the Tor usage

Forensic artifacts can be defined as the bit of information that an operating system keeps records regarding the usage of different applications and programme [8]**.**

As Tor browser's primary focus is to protect the privacy of the user and maintain its anonymity, in both its local footprint within a host and over a network connection. It follows different installation procedures compared to other applications and stores files in separate directories [9]. Very few traces are left in the host computer when it is uninstalled after use. The Registry is one of such a place where artifacts about tor usage can be found. Registry is a database storing information, settings, options, and other values for both software and hardware installed on an operating system [10]. When an application is installed in the operating system, a new subkey is created in the Registry for that application.

The Registry contains five major subfolders inside which all the keys and subkeys are stored. These subfolders are known as Hives [5]. Details about these hives are given below.

SI. NO	Key Class Name (WIN 10)	Remarks
01	HKEY_CLASSES_ROOT	Contains file extension association information, as well as a programmatic identifier (ProgID), Class ID (CLSID), and Interface ID (IID) data
02	HKEY_CURRENT_USER	It contains subkeys corresponding to the HKEY_CURRENT_USER keys for each user profile actively loaded on the machine, though user hives are usually only loaded for currently logged-in users.
03	HKEY_LOCAL_MACHINE	contains the majority of the configuration information for the software you have installed, as well as for the Windows operating system itself.
04	HKEY_USERS	It contains registry information about the user's application settings, desktop, environment, network connections, and printers.
05	HKEY_CURRENT_CONFIG	Acts as a pointer, or a shortcut, to a registry key that keeps the information about the hardware profile currently being used.

Table 1: Major registry hives, Credit (Windows official Blog)

All of this can be useful for a forensic investigator to carry out relevant and conclusive findings in a forensic investigation.

Review of litrature

As technology becomes incorporated into our everyday lives and people are dependent on the worldwide web, lots of men and women are getting to be more conscious of these digital footprints and also the associated demand for solitude. No matter how you connect into the Web if from desktop, notebook, or mobile device--a browser is often demanded. Browsers enable users to get into news sites, pay invoices, see videos, and send emails. For several, this system traffic might be sensitive. The release of 1000s of top-secret NSA records in overdue 2013 resulted in a gigantic interest in people's information security and also the right to solitude [11]. Input the growth of browsing capacities. Private browsing enables the consumer to navigate the Web without departing evidence behind that which websites were seen (history), reports used stored passwords files downloaded, etc.. Predicated on the browser and settings used, a few of the data can remove or change. While some private-browsing features started showing up in the early 2000s, the leaked NSA documents led to the explosive development of privacy-focused plugins, and even add ons. These features are rather appealing to ordinary hackers, users, or offenders for a variety of factors. Nevertheless, the use of Tor browsers may complicate signs collecting methods and procedures employed by forensic investigators.

Motivated by the anxiety about privacy-intrusion members of the general public and cyber-criminals alike increasingly switched into the Tor Browser, enticed with its own anonymizing capabilities. A brand new influx of users and growing media focus induce academic research to the efficacy of both Tor and its own capacity to protect user privacy [12]. All these artefacts are conducive to a specific user, uniquely recognize the Tor Browser, and then continue through Uninstallation and log out.

What's more, user actions within Tor is composed of the Windows Registry as due to recent upgrades to Windows-10. This permits a forensic adversary to ascertain the names of pages seen with the browser.

The publication way of anonymous media that Tor is (in) famous for has drawn attention from the cyber security community, chiefly leading to research regarding de-anonymization of users by a networking perspective. But, it's the aim of this Tor Project to secure an individual from the local and network adversaries. That is reached via the execution of design and features choices meant to obfuscate network actions and employ anti-forensics tactics to protect against browsing session data from being written to the disc drive. Unlike routine web surfing, this obfuscates an individual's IP, ensuring their identity isn't revealed to the internet sites they see. By assessing the traffic through encrypted stations, data can also be shielded from passive traffic investigation. Using this system does not guarantee anonymity, which makes the Tor Browser Bundle (TBB) that an essential component from the privacy-oriented structure. The TBB can be an elongated service release (ESR) of all Mozilla's Firefox browser, also bundled using compulsory add-ons that protect user-friendliness. The browser design doctrine says that the TBB should protect an individual from famous web attacks created to show an individual's individuality and minimize the sum of surfing data written to the disc drive. To allow this, plugins like no script that protects an individual from malicious code websites are used automatically since is Firefox's Personal Browsing manner. Forcing Private Browsing style means that history isn't stored to disc by the browser, which ought to allow it to be hard to get a forensic adversary to see internet sites seen.

Anonymity and privacy are two major elements to protect freedom of language. Goal of anonymity is always to protect all of the information which could reveal real identification of consumer information like name, location, ip etc.. The goal of privacy is to be certain any company or entity doesn't collect or save any personal or private information like user browser record, location info, account details without user's knowledge. Currently Tor project is working together with the intention to protect user anonymity and privacy over the web. Tor job premiered in 1995 by US Naval Research Laboratories [10]. The main objective of their project was to split up identification advice from routing and also to design an anonymous communication system for military communication. After general disclosure, it was profoundly studied and extensive research was completed contributing to various revisions of this endeavor. Based on the latest report released by Tor metrics, there are more than 2.5 million busy Tor users with 6000+ nodes carrying their traffic and providing 25.5 Gbps bandwidth to your own Tor network. Tor browser is the easiest way to get in touch into the Tor overlay network to track users' traffic. Tor browser is just a modified variant of Mozilla Firefox with some additional features for privacy and solitude. Several of those features are the Tor launcher, Tor button, No-script and HTTPS-Everywhere. Automatically, browsing is configured to get private style with the possibility to clear browsing activity and also its own related artifacts such as snacks and other browsing related data after final of the browser. According to a study, local DNS resolver and exchange partition utilized for memory card swapping are two big challenges to browsing [10]. Private browsing can leave lots of artifacts on host machine plus it does not supply the degree of solitude maintained by its own vendors. The investigation demonstrated that artifacts might be recovered out of memory if the browser which is used for browsing is available at the time of acquisition.

There has been studies that have a fantastic investigation of Tor Browser, but there remain a few locations which aren't properly addressed. Tor working methodology Tor is made up of worldwide overlay system of relays which aids in the success of solitude and anonymity to get user traffic. For every single communicating, the Tor system creates a digital circuit containing no less than three sequential, randomly selected relays. Hence, the vertical layer of protection is protected from the entrance node where as the inner most level of encryption is intended for its flow node to decrypt [13]. Every relay node decrypts the received package with its decryption key so as to find the next-hop speech for the received package. In this way, every Tor node gets got the understanding of relay nodes just 1 jump away from that point. At the departure node, the inner most coating of encryption is encrypted as well as the un-encrypted data package is forwarded towards its ultimate destination [14]. Ergo, the solitude of users' data is maintained before previous jump. In the instance of all https over Tor system, data between past destination and hop can be encrypted. Additional that the Tor browser varies its own course after every couple minutes. To be sure the consumer's anonymity. Routing of information through Tor system is portrayed in Fig. inch. Anonymity on the flip side, is supplied by the Tor system by ensuring even the relay structures of the overlay have understanding of the predecessor and successor relay nodes at the complete digital circuit [15]. To further improve the anonymity land, every brand new digital circuit has been created with a newly selected pair of relay structures.

Suggested approach on literature review

There are many research articles published in different journals focusing on registry analysis to find artifacts regarding Tor usage. Tor does not write browsing data to disk [11]. Earlier studies show that analyzing in the system and user hives in windows 7 computer system, SID and location path can be found in the Registry [11]. In close Tor browser instance and open Tor browser instance, two keys are found in Registry while the third was missing [8]. It suggests that registry data is not cleared after the uninstallation. Registry analysis using Regshot in windows 10 system with an old version of the tor browser was carried out by the researcher and found the installation location of the tor browser [5]. This indicates to proceed further and to look dipper on the Registry to find relevant artifacts. It is worth enough to mention that different registry analysis tool has a different capacity as mentioned in the tool section. So multiple tools for registry analysis can be considered. Registry analysis tool with key rebuilding capacity and deleted key recovery ability may enhance the result.

Registry analysis on the latest version of Tor can be carried out as older versions are obsolete now (No longer people are using it). Only a few forensic situations and their effect on the Registry are studied so far. So going for more forensic scenarios inside the same operating system may allow us to note the minute changes in the Registry, which are may not be direct evidence but can support the evidence more accurately.

Objective

To find and analyze artifacts related to Tor usage in windows system from registry analysis in different simulated forensic scenarios.

Methodology

Assumption

1. The computer is working correctly without any anomalies.
2. There is no programme running on the computer, which may execute registry modification commands at any time period.
3. No ongoing remote administration session in the computer system.
4. The Tor browser is installed on the operating system Windows 10 (x64 bit, kernel-10.0.18363.592) on the computer.
5. The investigator or researcher has access to windows registry hives.

Scope

1. The operating system may not be installed with default settings and values, but the user does not modify the Registry.

2. It is considered that artifacts that are not directly related to the Tor Browser Bundle but supports facts regarding Tor browser usage are under observation.

3. Traces are considered that left after using the Tor Browser Bundle due to the presence of the files related to it or system is not shut down after usage.

4. It is possible to occur that a different scenario would reveal additional traces of the Tor Browser Bundle on the user's system.

Forensic Scenario

1. Installation of Tor browser and uninstalling it without any usage.
2. Installation of Tor browser with usage and left the browser installed on the host machine.
3. Installed Tor browser and uninstalled after usage.

Tool

Includes free and open-source tools.

Specification of these tools are given below:

Forensic Functionality: Windows Registry, Tool host OS/runtime environment: windows, Input data type(s): any, Automated hive extraction and parsing: any, Registry rebuilding: any, Deleted key recovery: any, Key and value instance display: any, Pre-built reports: any.

1. Regshot (Open source)
2. Regedit (Inbuilt in windows)

Limitations

There are few limitations exists with the experiment

1. It is only focused on a specific operating system (Windows 10 Pro) and a specific browser based on Tor protocol.
2. There are few assumptions regarding the state of the computer during analysis.

Forensic Approach

The disk images that will be used in the analysis are snapshots that were created using VMWare pro version 8.5.3. The Operating System (OS) used was a clean 64-bit installation to a 64-bit Windows 10 Pro. The OS was patched to kernel version 10.0.18363.592. The researcher seen throughout this study was a user account with administrative privileges.

To make the analysis easier, a full clone of the VM was made to have a clean starting point with the snapshots. The first snapshot of the VM was made immediately after the installation was performed. The second snapshot was taken was after the Tor Browser software was installed. Third snapshot was taken after uninstallation of the browser without using it. A fourth snapshot was made again reinstalling it while a connection to the Tor network was established and few websites are browsed.

The computer used to perform the analysis was a Lenovo laptop (purchased on October 2017) with Windows 10 STUDENT Edition latest version. The open source tools Regshot and Reg edit was used throughout this study. The version of the Tor Browser installed was version 9.0.10_en-US.

Technical changes compared to synopsis

1. Kernel version mentioned in synopsis changed to latest kernel upgrade by windows.
2. Paid tool Arsenal Recon was earlier mentioned for use in synopsis but not used for this study due to transactional reason.

Procedure

1. Installation of Regshot

A basic Windows forensic step is to obtain the registry settings. The registry before and after installation of the Tor Browser software can yield an understanding of how the software installation changes the system. Regshot, shown in Figure 2, is open source software that performs registry snapshots (regshot, 2016). HAL9000 says that we “simply create the 1st shot, install the software or run the program you want to watch, and then press 2nd shot” (Hal9000, 2016).

2. Installation of Tor Browser

Older versions of the Tor Browser are difficult to find but can be obtained from https://www.torproject.org/dist/torbrowser/9.0.10/torbrowser-install-win64-9.0.10_en-US.exe. Pretty Good Privacy (PGP) was used, as shown in Figure below, to verify the software signatures and ensure the version downloaded is a verified package (“How to verify signatures for packages,” n.d.).

```
-----BEGIN PGP SIGNATURE-----

iQIcBAABCgAGBQJesJrRAAoJEOt3RJHZ/wbifbsP/j2WoEhZexhGrM8mGOn66M6g
jmL4kbT8sK5eCe+m0XcDbaAFIuH39JSA1hKamO1wOTZmCSTqBz8Tm/hZq5N2Pjoa
Us9QNG3lxQGdeHPRw/M0EvQBt5BuHYAj1Uj9Eg4qnuKyHrZ74CNHqwxe/hnt2gaB
ByGzg8Z+YjiDjYucF7ZYaGySgg/9/wyoXnaEB43oRJARsV0zcmTEc2v5a27L/mtC
G3rWlqQCL8zydcNmBqBVMTTdzf593utBrm5pXx0r6aOD23xuZ5ZwOZB06/djAp4I
F6Vzpe1yAKZacTKwUrimYnfeK2DwifM8C6qgZSCIuFlkRhfdrtdYbF4V4hnYwZAZ
LgDe3tzXvXEXyww8UmPn8TMb1rkzMDSGKpSa+V0me9auzQKtwoEnfELcHExzpGsS
5uoNhs0z/AI6AVfOpxM2/XxlBjG8I688rmBGpXcHtDMn8kDtxt7a9Mp38JIfSOXv
rrautz/L/DpdKx9Jkjm0A1Xj3fNnCLKB2/qMUvZcv7yIZ1GP1PssEAYTKpIHVB2H
UtMPt0LhoH+GmesWVqR/Bj9YCxAvRn4x7f/rBpEt2RbHevKoRHvfO4cAGrcJxXae
kiRfyONSSL+SKKs8CXaPu8yNUnfbOTAI0wX2ljyEgbGGmKWVCTsZhN2CBv79kyzV
C+UOcNQTePp8uas1WhMP
=VR5V
-----END PGP SIGNATURE-----
```

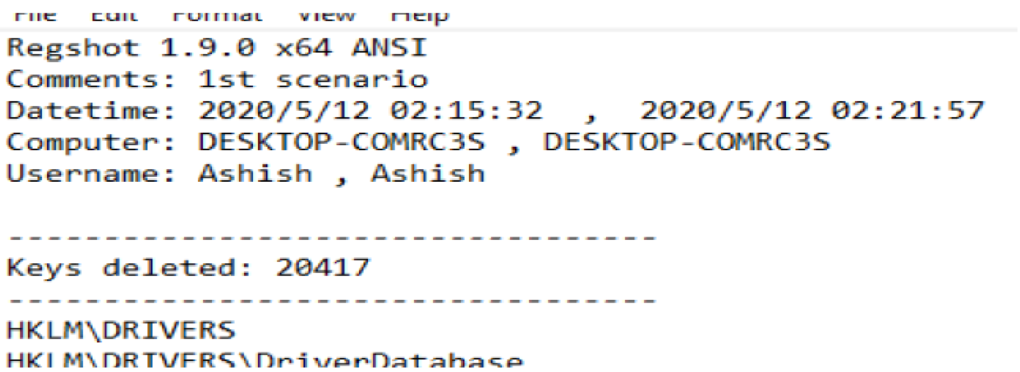
Figure 3. PGP verifies a file’s content against a signature signed by a key. This ensures that the file has not been altered.

3. Each scene was simulated and registry state are analyzed.

Observation

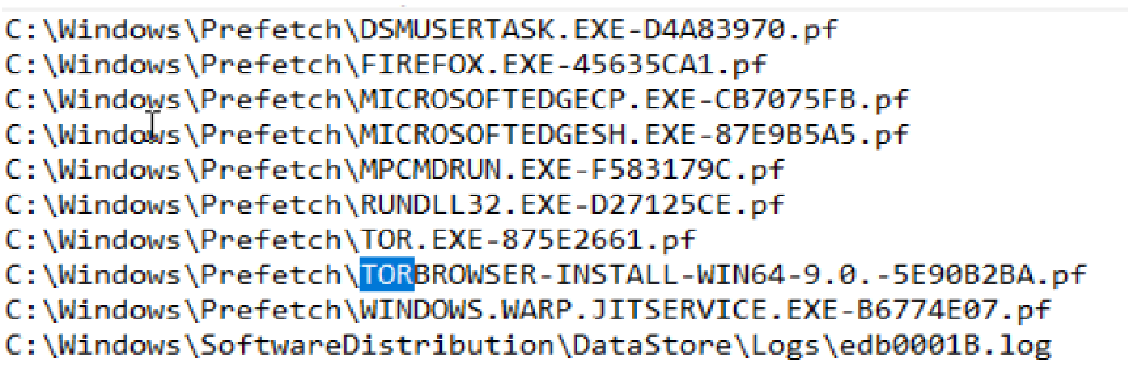
Since the package has been verified, as shown with the words “Good signature” in Figure3, the next step of installation was as easy as double-clicking the executable. For this installation, the user’s desktop was chosen to make it easy to find forensically. Regshot was used again and the second shot was taken. Then difference between both shots are compared.

Scenario 1



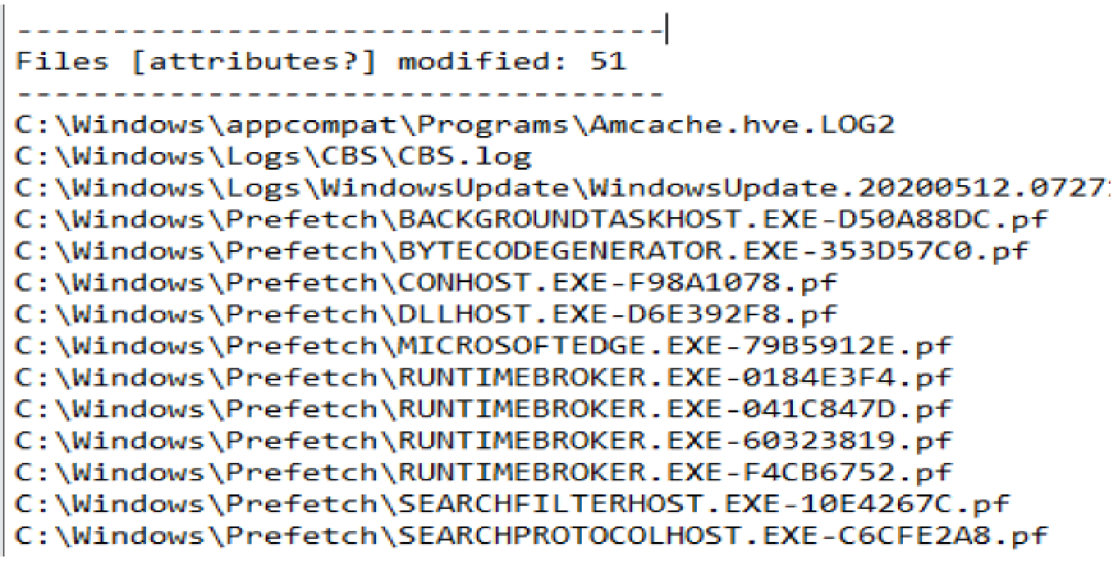
```
Regshot 1.9.0 x64 ANSI
Comments: 1st scenario
Datetime: 2020/5/12 02:15:32  ,  2020/5/12 02:21:57
Computer: DESKTOP-COMRC3S , DESKTOP-COMRC3S
Username: Ashish , Ashish

----------------------------------
Keys deleted: 20417
----------------------------------
HKLM\DRIVERS
HKLM\DRIVERS\DriverDatabase
```

Fig- 2



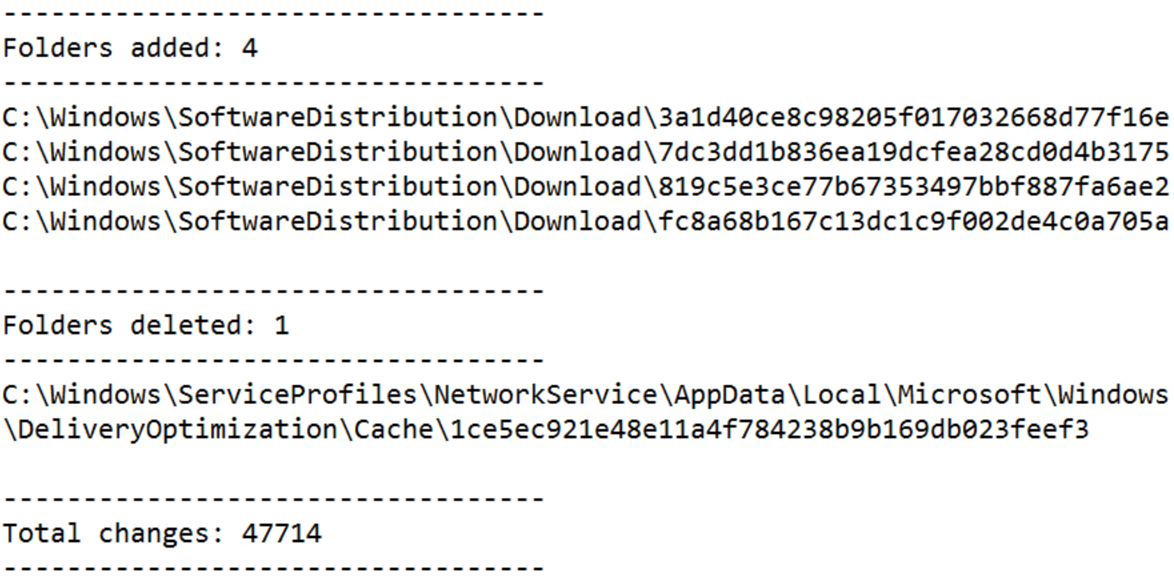
```
C:\Windows\Prefetch\DSMUSERTASK.EXE-D4A83970.pf
C:\Windows\Prefetch\FIREFOX.EXE-45635CA1.pf
C:\Windows\Prefetch\MICROSOFTEDGECP.EXE-CB7075FB.pf
C:\Windows\Prefetch\MICROSOFTEDGESH.EXE-87E9B5A5.pf
C:\Windows\Prefetch\MPCMDRUN.EXE-F583179C.pf
C:\Windows\Prefetch\RUNDLL32.EXE-D27125CE.pf
C:\Windows\Prefetch\TOR.EXE-875E2661.pf
C:\Windows\Prefetch\TORBROWSER-INSTALL-WIN64-9.0.-5E90B2BA.pf
C:\Windows\Prefetch\WINDOWS.WARP.JITSERVICE.EXE-B6774E07.pf
C:\Windows\SoftwareDistribution\DataStore\Logs\edb0001B.log
```

Fig- 3



```
----------------------------------
Files [attributes?] modified: 51
----------------------------------
C:\Windows\appcompat\Programs\Amcache.hve.LOG2
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20200512.0727
C:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-D50A88DC.pf
C:\Windows\Prefetch\BYTECODEGENERATOR.EXE-353D57C0.pf
C:\Windows\Prefetch\CONHOST.EXE-F98A1078.pf
C:\Windows\Prefetch\DLLHOST.EXE-D6E392F8.pf
C:\Windows\Prefetch\MICROSOFTEDGE.EXE-79B5912E.pf
C:\Windows\Prefetch\RUNTIMEBROKER.EXE-0184E3F4.pf
C:\Windows\Prefetch\RUNTIMEBROKER.EXE-041C847D.pf
C:\Windows\Prefetch\RUNTIMEBROKER.EXE-60323819.pf
C:\Windows\Prefetch\RUNTIMEBROKER.EXE-F4CB6752.pf
C:\Windows\Prefetch\SEARCHFILTERHOST.EXE-10E4267C.pf
C:\Windows\Prefetch\SEARCHPROTOCOLHOST.EXE-C6CFE2A8.pf
```

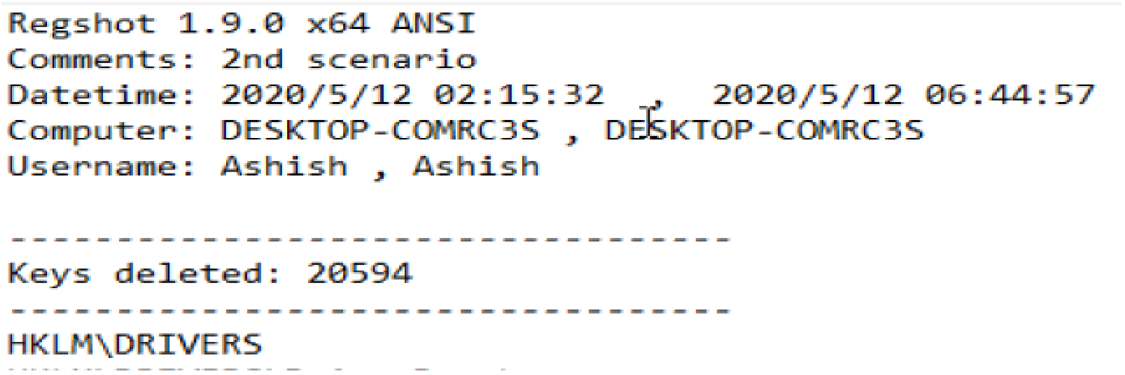
Fig- 4



```
----------------------------------
Folders added: 4
----------------------------------
C:\Windows\SoftwareDistribution\Download\3a1d40ce8c98205f017032668d77f16e
C:\Windows\SoftwareDistribution\Download\7dc3dd1b836ea19dcfea28cd0d4b3175
C:\Windows\SoftwareDistribution\Download\819c5e3ce77b67353497bbf887fa6ae2
C:\Windows\SoftwareDistribution\Download\fc8a68b167c13dc1c9f002de4c0a705a

----------------------------------
Folders deleted: 1
----------------------------------
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows
\DeliveryOptimization\Cache\1ce5ec921e48e11a4f784238b9b169db023feef3

----------------------------------
Total changes: 47714
----------------------------------
```

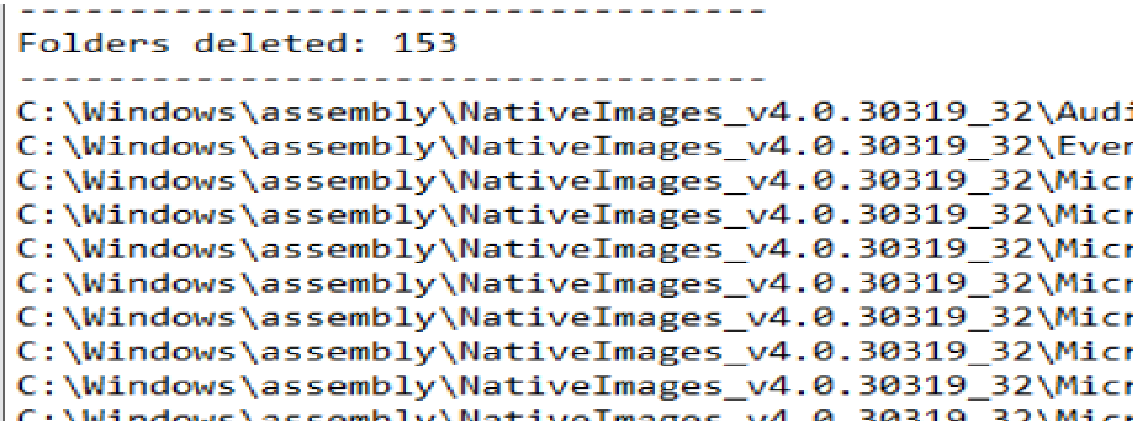
Fig- 5

Scenario 2



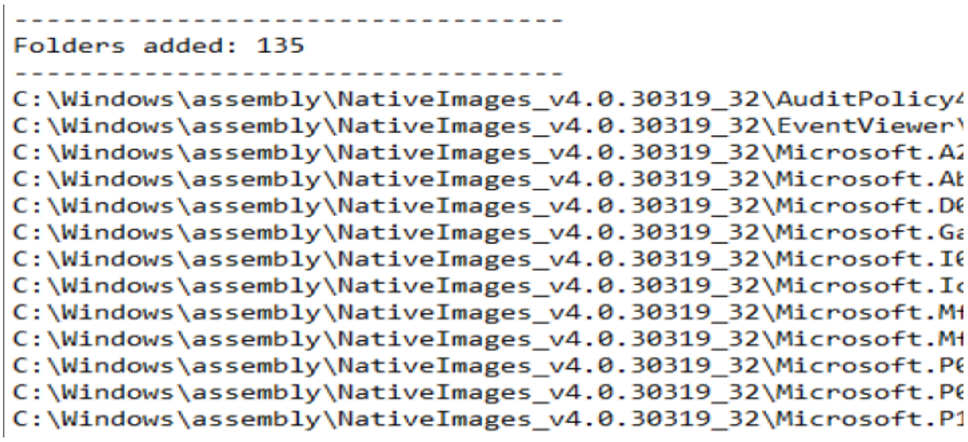
```
Regshot 1.9.0 x64 ANSI
Comments: 2nd scenario
Datetime: 2020/5/12 02:15:32  ,  2020/5/12 06:44:57
Computer: DESKTOP-COMRC3S , DESKTOP-COMRC3S
Username: Ashish , Ashish

----------------------------------
Keys deleted: 20594
----------------------------------
HKLM\DRIVERS
```

Fig- 6



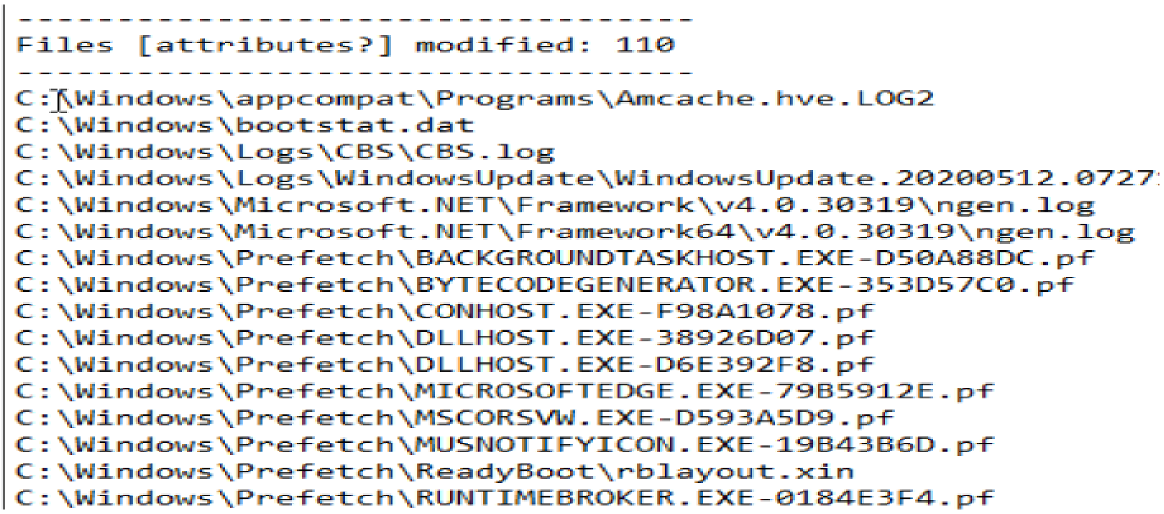
```
----------------------------------
Folders deleted: 153
----------------------------------
C:\Windows\assembly\NativeImages_v4.0.30319_32\Audi
C:\Windows\assembly\NativeImages_v4.0.30319_32\Ever
C:\Windows\assembly\NativeImages_v4.0.30319_32\Micr
C:\Windows\assembly\NativeImages_v4.0.30319_32\Micr
C:\Windows\assembly\NativeImages_v4.0.30319_32\Micr
C:\Windows\assembly\NativeImages_v4.0.30319_32\Micr
C:\Windows\assembly\NativeImages_v4.0.30319_32\Micr
C:\Windows\assembly\NativeImages_v4.0.30319_32\Micr
C:\Windows\assembly\NativeImages_v4.0.30319_32\Micr
```

Fig- 7



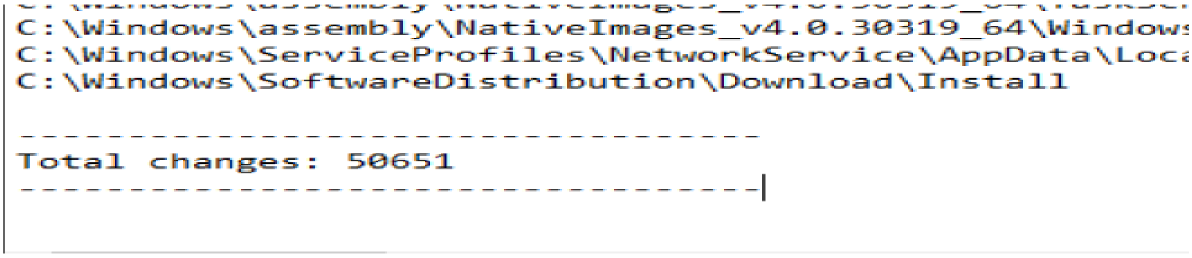
```
-----------------------------------
Folders added: 135
-----------------------------------
C:\Windows\assembly\NativeImages_v4.0.30319_32\AuditPolicy
C:\Windows\assembly\NativeImages_v4.0.30319_32\EventViewer
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.A
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Ab
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.D
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.G
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.I
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.I
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.M
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.M
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P
```

Fig- 8



```
-----------------------------------
Files [attributes?] modified: 110
-----------------------------------
C:\Windows\appcompat\Programs\Amcache.hve.LOG2
C:\Windows\bootstat.dat
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20200512.0727
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.log
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log
C:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-D50A88DC.pf
C:\Windows\Prefetch\BYTECODEGENERATOR.EXE-353D57C0.pf
C:\Windows\Prefetch\CONHOST.EXE-F98A1078.pf
C:\Windows\Prefetch\DLLHOST.EXE-38926D07.pf
C:\Windows\Prefetch\DLLHOST.EXE-D6E392F8.pf
C:\Windows\Prefetch\MICROSOFTEDGE.EXE-79B5912E.pf
C:\Windows\Prefetch\MSCORSVW.EXE-D593A5D9.pf
C:\Windows\Prefetch\MUSNOTIFYICON.EXE-19B43B6D.pf
C:\Windows\Prefetch\ReadyBoot\rblayout.xin
C:\Windows\Prefetch\RUNTIMEBROKER.EXE-0184E3F4.pf
```

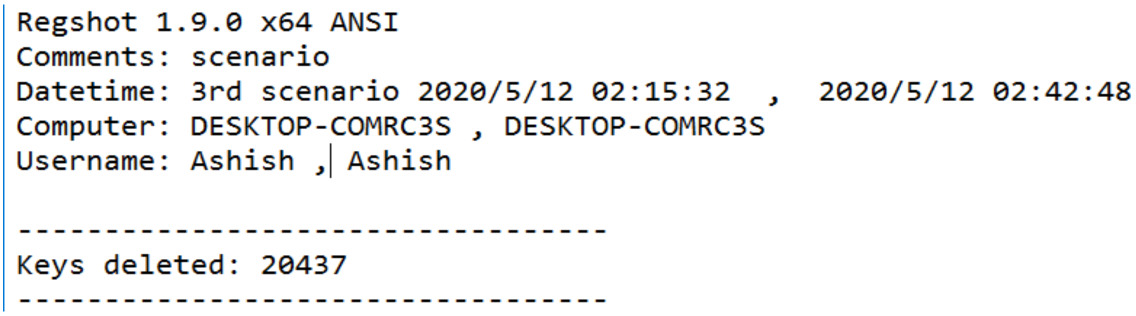
Fig- 9



```
C:\Windows\assembly\NativeImages_v4.0.30319_64\Window
C:\Windows\ServiceProfiles\NetworkService\AppData\Loc
C:\Windows\SoftwareDistribution\Download\Install

-----------------------------------
Total changes: 50651
-----------------------------------
```

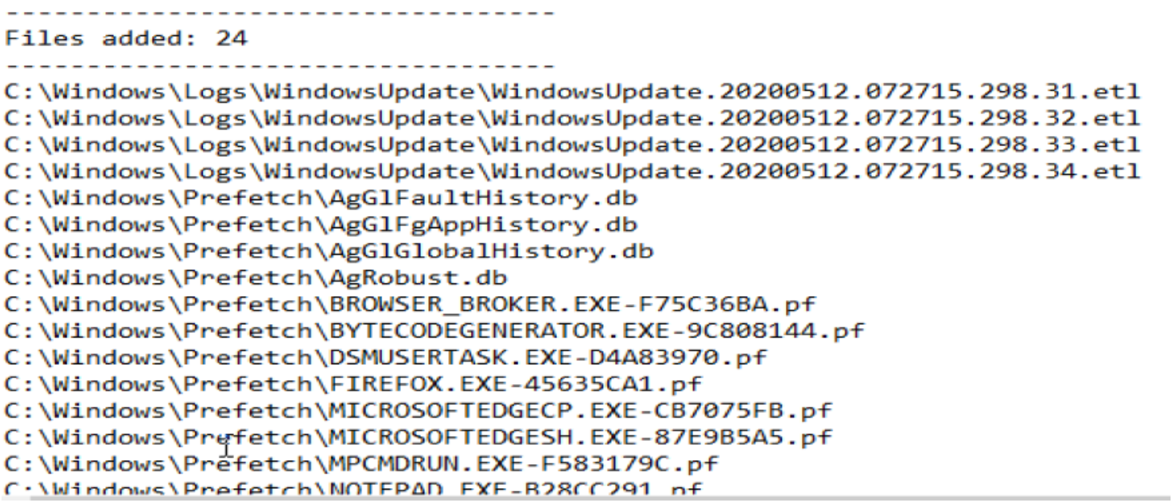
Fig- 10

Scenario 3



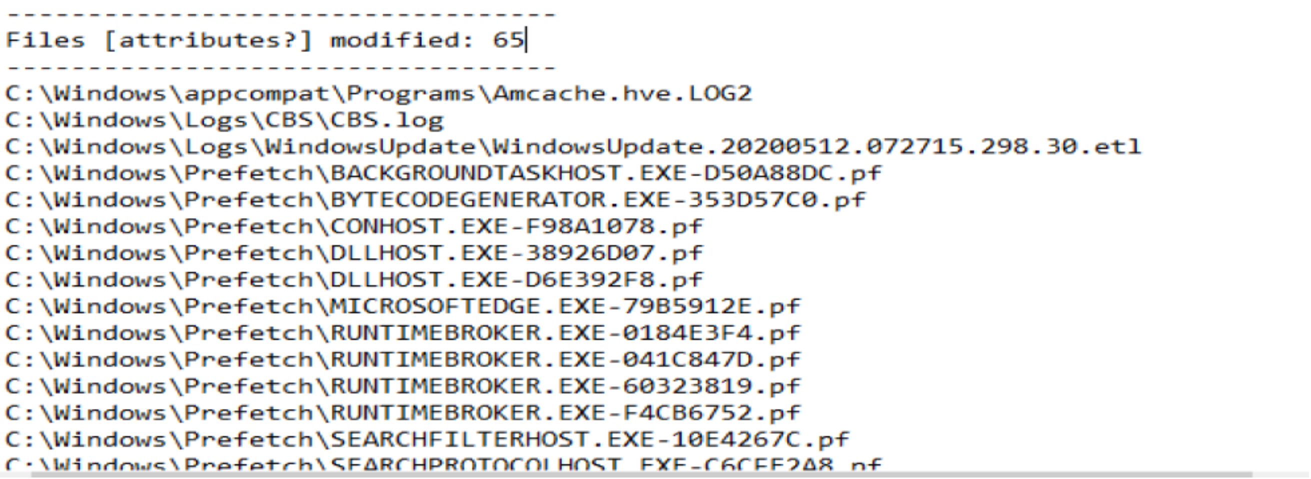
```
Regshot 1.9.0 x64 ANSI
Comments: scenario
Datetime: 3rd scenario 2020/5/12 02:15:32  ,  2020/5/12 02:42:48
Computer: DESKTOP-COMRC3S , DESKTOP-COMRC3S
Username: Ashish , Ashish

----------------------------------
Keys deleted: 20437
----------------------------------
```

Fig- 11



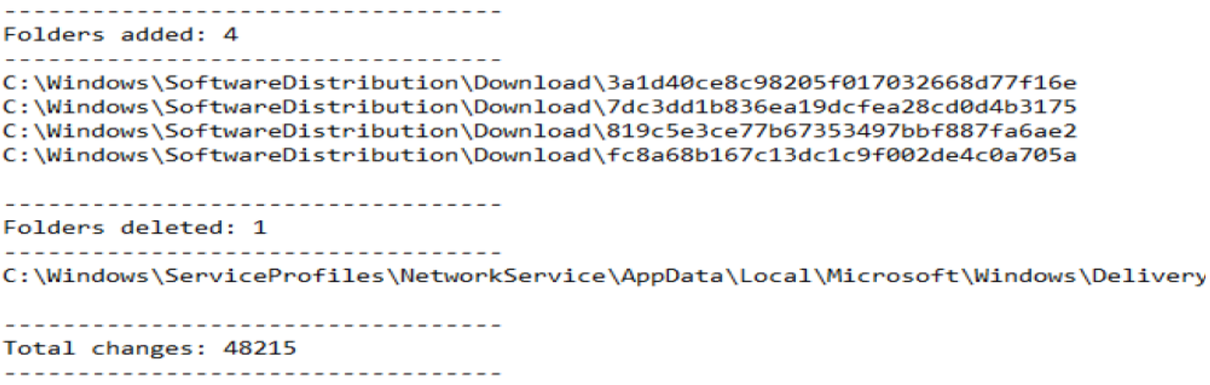
```
----------------------------------
Files added: 24
----------------------------------
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20200512.072715.298.31.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20200512.072715.298.32.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20200512.072715.298.33.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20200512.072715.298.34.etl
C:\Windows\Prefetch\AgGlFaultHistory.db
C:\Windows\Prefetch\AgGlFgAppHistory.db
C:\Windows\Prefetch\AgGlGlobalHistory.db
C:\Windows\Prefetch\AgRobust.db
C:\Windows\Prefetch\BROWSER_BROKER.EXE-F75C36BA.pf
C:\Windows\Prefetch\BYTECODEGENERATOR.EXE-9C808144.pf
C:\Windows\Prefetch\DSMUSERTASK.EXE-D4A83970.pf
C:\Windows\Prefetch\FIREFOX.EXE-45635CA1.pf
C:\Windows\Prefetch\MICROSOFTEDGECP.EXE-CB7075FB.pf
C:\Windows\Prefetch\MICROSOFTEDGESH.EXE-87E9B5A5.pf
C:\Windows\Prefetch\MPCMDRUN.EXE-F583179C.pf
C:\Windows\Prefetch\NOTEPAD.EXE-B28CC291.pf
```

Fig- 12



```
----------------------------------
Files [attributes?] modified: 65
----------------------------------
C:\Windows\appcompat\Programs\Amcache.hve.LOG2
C:\Windows\Logs\CBS\CBS.log
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20200512.072715.298.30.etl
C:\Windows\Prefetch\BACKGROUNDTASKHOST.EXE-D50A88DC.pf
C:\Windows\Prefetch\BYTECODEGENERATOR.EXE-353D57C0.pf
C:\Windows\Prefetch\CONHOST.EXE-F98A1078.pf
C:\Windows\Prefetch\DLLHOST.EXE-38926D07.pf
C:\Windows\Prefetch\DLLHOST.EXE-D6E392F8.pf
C:\Windows\Prefetch\MICROSOFTEDGE.EXE-79B5912E.pf
C:\Windows\Prefetch\RUNTIMEBROKER.EXE-0184E3F4.pf
C:\Windows\Prefetch\RUNTIMEBROKER.EXE-041C847D.pf
C:\Windows\Prefetch\RUNTIMEBROKER.EXE-60323819.pf
C:\Windows\Prefetch\RUNTIMEBROKER.EXE-F4CB6752.pf
C:\Windows\Prefetch\SEARCHFILTERHOST.EXE-10E4267C.pf
C:\Windows\Prefetch\SEARCHPROTOCOLHOST.EXE-C6CEE2A8.pf
```

Fig- 13



```
---------------------------------
Folders added: 4
---------------------------------
C:\Windows\SoftwareDistribution\Download\3a1d40ce8c98205f017032668d77f16e
C:\Windows\SoftwareDistribution\Download\7dc3dd1b836ea19dcfea28cd0d4b3175
C:\Windows\SoftwareDistribution\Download\819c5e3ce77b67353497bbf887fa6ae2
C:\Windows\SoftwareDistribution\Download\fc8a68b167c13dc1c9f002de4c0a705a

---------------------------------
Folders deleted: 1
---------------------------------
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\Delivery

---------------------------------
Total changes: 48215
---------------------------------
```

Fig- 14

Interpretation

Scenario 1

When registry changes are analysed for scenario 1, it was found that when Tor browser is installed in a computer and uninstalled without using, it still leaves traces in registry. These artefacts were found in comparison result. There were 20417 keys deleted, 4 folders added, 1 folder deleted, 51 modified and 47714 total changes. There are file attributes that shows the evidence as in fig. 3.

Scenario 2

In scenario 2 it was found that when Tor browser is installed in a computer and used for browsing different website, and browser is present in computer, it leaves traces in registry. These artefacts were found in comparison result. There were 20594 keys deleted, 135 folders added, 153 folder deleted, 110 modified and 50651 total changes.

Scenario 3

In scenario 3 it was found that when Tor browser is installed in a computer and used for browsing different website, and post use browser is uninstalled from computer, it still leaves traces in registry. These artefacts were found in comparison result. There were 20437 keys deleted, 4 folders added, 1 folder deleted, 65 modified, 48215 total changes and 4 files are added.

Conclusion

This study sought to identify the digital artifacts and their locations that could be recovered from a windows computer having Tor usage. We were able to successfully recover several artifacts of interest, that confirms the installation and usage of Tor browser. These findings provided the baseline used for the investigation into several browsing session scenarios. In the browsing sessions of Tor browser we were able to recover significantly less artefacts in case of uninstallation after browsing than the normal browsing sessions, validating several of the claims made by the producers of these programs. The Tor Browser Bundle excelled in minimizing the amount of information but still a lot of artefacts are there in registry that are useful for registry analysis.

Future Work

- Future research in the realm of web browser forensics should continue to analyze which artifacts can be recovered from registry hives along with registry rebuilding as a method to aid in digital forensic investigations.
- With the rise of mobile devices and seamless user experiences, research could focus on mobile Tor browsers.

Reference

[1] A. Kapadia, “Analysis of the Tor Browser and its Security Vulnerabilities,” pp. 1–9, 2014.

[2] B. Schneier, “Attacking Tor: how the NSA targets users’ online anonymity,” *Guard.*, p. 1, 2013.

[3] P. Winter *et al.*, “Spoiled onions: Exposing malicious Tor exit relays,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8555 LNCS, pp. 304–331, 2014.

[4] R. Hughes, “済無No Title No Title,” *J. Chem. Inf. Model.*, vol. 53, no. 9, p. 287, 2008.

[5] A. Warren, *Information Security Reading Room Tor Browser Artifacts in Windows 10 ________________________________ Th e In st itu te , A r R et ai ns ll Ri gh ts*. 2020.

[6] A. Warren, “Information Security Reading Room Tor Browser Artifacts in,” 2020.

[7] D. J. Farmer, “A Windows Registry Quick Reference : For the Everyday Examiner,” *Champlain Coll.*, pp. 1–14, 2008.

[8] M. Soni, “A Review of Forensic Artifacts in a Windows 8 Environment,” no. Cognition, pp. 20–24, 2015.

[9] K. Daimi, “Computer and network security essentials,” *Comput. Netw. Secur. Essentials*, pp. 1–618, 2017.

[10] A. K. Jadoon, W. Iqbal, M. F. Amjad, H. Afzal, and Y. A. Bangash, “Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web,” *Forensic Sci. Int.*, vol. 299, pp. 59–73, 2019.

[11] B. Mcfadden, E. Balasubramani, and W. E. Miebaka, *Digital Forensic Education*, vol. 61. Springer International Publishing, 2020.

[12] M. Muir, P. Leimich, and W. J. Buchanan, “A Forensic Audit of the Tor Browser Bundle,” *Digit. Investig.*, vol. 29, pp. 118–128, 2019.

[13] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, “Hiding routing information,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1174, pp. 137–150, 1996.

[14] T. Wang and I. Goldberg, “On Realistically Attacking Tor with Website Fingerprinting,” *Proc. Priv. Enhancing Technol.*, vol. 2016, no. 4, pp. 21–36, 2016.

[15] S.-Y. Teng and C.-Y. Wen, “A Forensic Examination of Anonymous Browsing Activities,” *Forensic Sci. J. Since*, vol. 17, no. 1, pp. 1–8, 2018.