DSCI
PROMOTING DATA PROTECTION

KARNATAKA STATE POLICE
C.I.D
CRIMINAL INVESTIGATION DEPARTMENT

Infosys Foundation

CENTRE FOR CYBERCRIME INVESTIGATION TRAINING & RESEARCH

DARK & DEEP WEB: ADVANCED FORENSIC ANALYSIS OF TOR BROWSER AND IMPLICATIONS FOR LAW ENFORCEMENT AGENCIES

Technical Whitepaper

AUTHOR

Manjesh P Shetty,
Senior Analyst,
Data Security Council of India

DISCLAIMER

This research paper contains information that is Intellectual Property of CCITR.This paper represents the opinions of the authors. No part of this paper can be reproduced in any form whatsoever. The information contained here in has been obtained from sources, believed to be reliable. However, author expressly disclaims all warranties, express or implied, as to the accuracy, completeness or adequacy of the information. CCITR shall have no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof. The research work demonstrated in the paper is the current results as of the date appearing on the material only.

Published by CCITR

TABLE OF CONTENTS

1. Introduction:

The Internet can be broadly divided into three categories, namely Surface web, Deep web and Dark web. The Surface web is the internet information that is readily accessible (indexable) using different search engines. Deep web refers to any internet information or data that is not crawled by search engine robots, which is intentionally or unintentionally made hidden or not accessible to search engine crawlers, whereas Dark web refers to the website which is hosted within overlay networks and accessible only with specialized software like the Tor Browser.

The dark web is predominantly better known for illegal content. It can be accessed using specialized browsers like Tor which grants anonymity to users. hence the Dark Web has become a hotbed for criminal activity, and a challenging task for law enforcement and digital forensic experts to pinpoint the origin of traffic, location or to prove the ownership of the machine.

2. Problem Statement:

Millions of users use the Tor browser in day-to-day life which has made it a challenging task for Law Enforcement agencies across the globe to hunt down criminals, and the Tor project was implemented in such a way that it was designed to protect user's privacy and anonymity but on the contrary, it has made it quite challenging for Forensic Investigators and LEA to determine the website visited by the users as it keeps no footprints about the internet activity.

3. Solution:

In this whitepaper, we will be performing Forensic Analysis on Tor Browser, which is installed or executed live in Windows 11 machine. The analysis was split into different stages having different criteria. we would be focusing more on uncommon locations in Windows 11 system to find the artifacts, where we will be performing Disk Analysis, Memory Analysis & Network Analysis using free and open-source tools, so that LEA and Forensic Investigator can prove the ownership of the computer having more evidence where Tor browser was used for illegal activities.

Top Three Darkweb Networks

- Freenet
- I2P
- ToR

Freenet:

Freenet is a large storage device where it acts as a peer-to-peer platform for censorship-resistant, anonymous communication. It uses a decentralized distributed data store to keep and deliver information and when you upload any files it will chop data into the piece and encrypt it and distribute it among peer nodes and the uploader is provided with a key to retrieve the uploaded file.

To access Freenet, you can download software from freenetproject.org. The software supports Windows, macOS & Linux systems and works on two main nodes are opennet and darknet.

The Invisible Internet Project (I2P):

I2P uses one-way tunnels to communicate with each other systems where it can be either be outbound send traffic to a destination or inbound to accept the traffic. You can install I2P from I2P Anonymous Network (geti2p.net) which works on Windows, macOS, and Linux computers.

4. Tor Browser Overview:

Tor Browser is an anonymous browser that works on TOR (The Onion Routing) network, called TOR circuits. It keeps users anonymous while surfing the website and bouncing user communication around distributed network relays run by volunteers also known as Tor Network. Tor Browser is Firefox ESR with some patches.

SOURCE:
1. *https://freenetproject.org/index.html*
2. *https://geti2p.net/en/*
3. *https://www.torproject.org/*

5. Tor hidden Services Names:

Tor uses .onion pseudo-top-level domain which is not valid in the surface web. Over the years Tor software used to use Version2 .onion at one point of time it was considered as vulnerable as v2 uses RSA1024 keypair and 80 bit SHA1 (truncated) addresses. It is crafted using SHA1 hash of first the SHA1 hash of the DER-encoded ASN.1 public key is calculated then the first half of the hash is encoded to Base32 and the suffix ".onion" is added to the address which will contain the Numerical Digits 2-7 and the lower case letters a-z and which are exactly 16 characters long. Also, there is no central repository of all .onion names.

On January 9, 2018, Tor version 0.3.2.9 was released which supports next-generation onion services and was the first tor version supporting onion service version 3 which are 56 bytes long instead of 16 and has better crypto which is replaced with SHA1/RSA1024 with SHA3/ed25519/curve25519 with better onion address security. As per the Onion Version planned deprecation timeline, Tor version 0.4.6.x: will no longer support v2 onion service and support will be removed from their code base on July 15, 2021, and from October 2021 Tor Browser (Stable) will stop supporting version 2 onion services very soon.

6. Forensic Analysis of Tor Browser & other Programs:

In this paper, mainly we will be focusing on artifacts related to Tor Browser and other anti-forensics tools like SDelete.

SOURCE:
1. *https://lists.torproject.org/pipermail/tor-dev/2020-June/014365.html*
2. *https://blog.torproject.org/tors-fall-harvest-next-generation-onion-services*

6.1.1 Installation of OS for Test Case

We will be installing Windows 11 OS in virtual machine to perform Disk Forensics and XPS 15 Laptop Pre-Installed with Windows 11 for the Live Memory Acquisition.

System Summary of installed Operating System (Virtual Machine) for Disk Forensics:

OS: Windows 11 Pro
Version: 21H2 | 22000.376
System Name: LUFFY
Local Account Administrator Name: Strawhat Luffy
RAM Allocated: 8 GB
Hard Disk Allocated: 20 GB
Virtual Machine Software: VMware Workstation 15 Pro (Licensed Version: 15.5.1 build 15018445)

System Summary of installed Operating System (XPS 15) for Memory Forensics:

Device: Dell XPS 15 9500
OS: Windows 11 Home Single Language
Version: 21H2 | 22000.434
System Name: DESKTOP-GT6AAE4
Local Account Administrator Name: Dell
RAM: 32 GB
Hard Disk: 1 TB SSD

SOURCE: 1. *https://www.vmware.com/in/products/workstation-pro.html*

6.1.2: Overview of the Experimental Methodology

a) Disk Forensics

The operating system was installed with default settings and values without any modification, and we have taken a base snapshot during the initial installation to be able to revert to default settings. We have turned on the default Windows defender features.

b) Memory Forensics

The Memory Acquisition is performed on the Live System running Windows 11 OS. All the Windows Default Settings were turned on including Windows Defender and the system was running Kaspersky End Point Security.

c) Network Forensics

The Network Forensics is performed on the Live System running Windows 11 OS. All the Windows Network Default Setting were preserved and the Machine was connected to the Internet using Wi-Fi Network.

6.1.3 Program Installed for the Experiment:

a) Tor Browser:

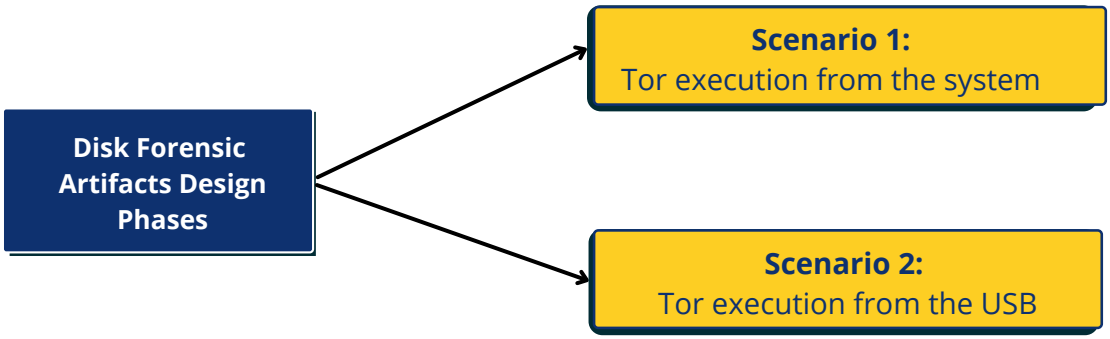
We have installed the latest version of Tor Browser 11.0.4 updates Firefox to 91.5.0esr and NoScript to the latest release (11.2.14). Tor Browser doesn't install itself in the program files, the software is installed into a directory as a whole (default Location is Desktop) and a relevant file for running the software resides inside the directory. The user can simply delete the folder named "Tor Browser" to remove it from their system.

b) SDelete:

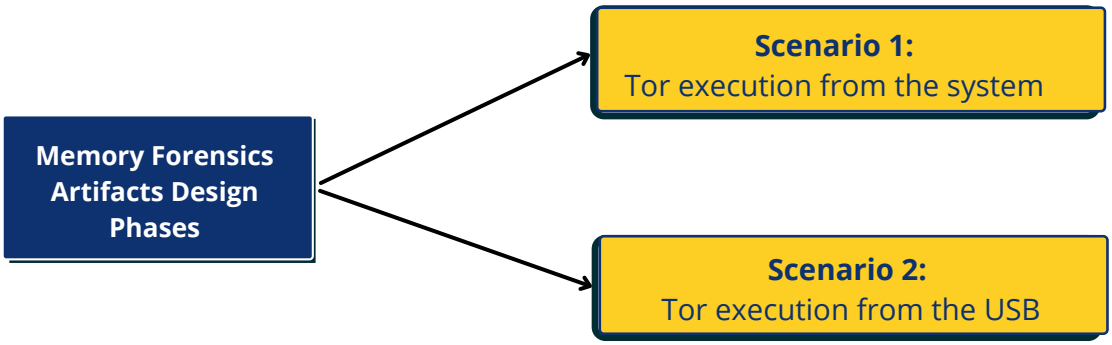
SDelete is a free command-line tool that you can use to delete files securely.

7. Creation of Artifacts: Design Consideration

Disk Forensics: Disk forensics artifacts design consideration has been divided into two case scenario as shown in Figure 1 &2. All the artifacts are created based on our requirements and a stable version of the Tor Browser were installed in this experiment as shown in figure 1 &2 for Disk Forensics. As mentioned in the figure, all the programs were downloaded from the Edge in Windows 11 VM and installed. All the browser history, cache, cookies were cleared and downloaded files were deleted.



Memory Forensics: Memory Forensics design consideration has been divided into two case scenarios as well.



a) Running Tor Browser from system:

As show in below figure, Tor Browser was installed in C Drive Location of the Windows 11 system and later it was deleted by SDelete Anti-Forensic Command Line Tool.

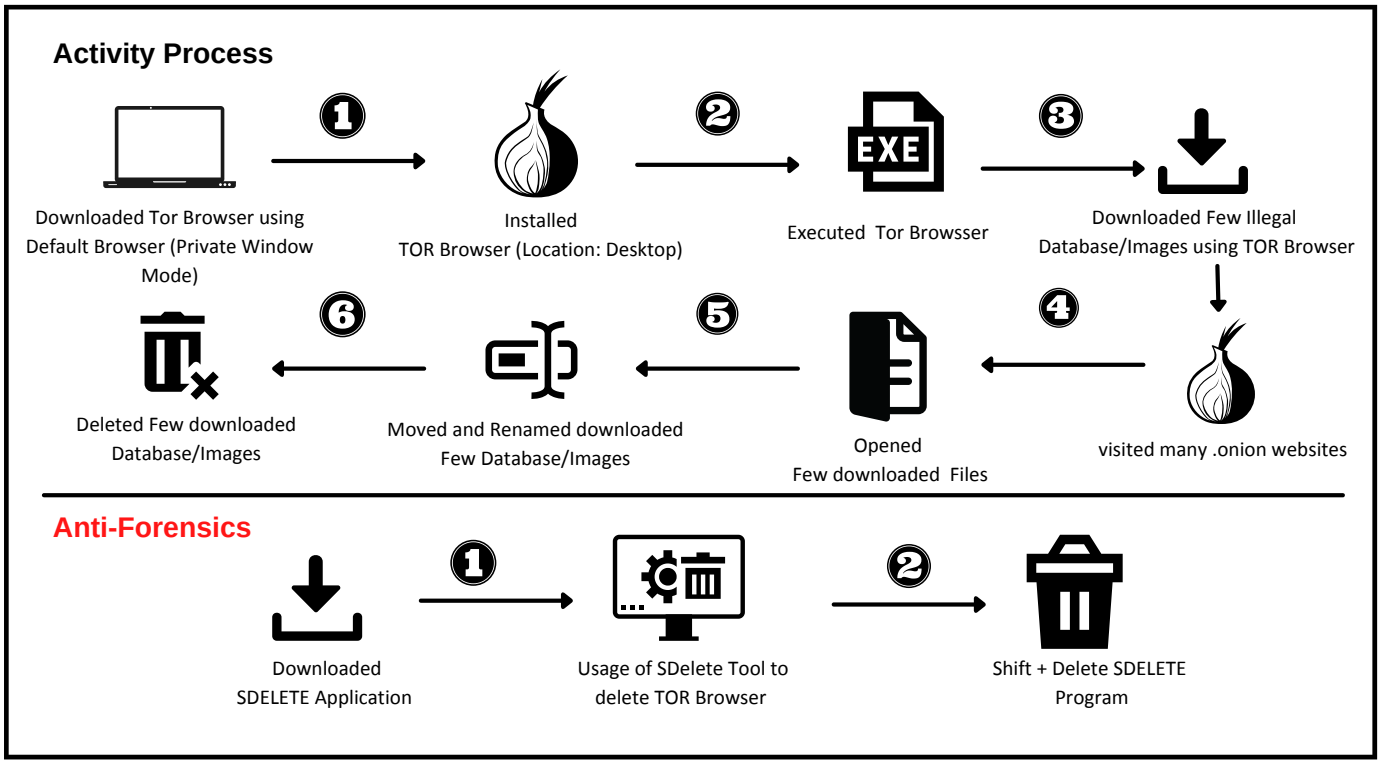


Figure 1: Scenario1 - Running Tor Browser from System

b) Running Tor Brower from USB Flash Drive (Portable Execution)

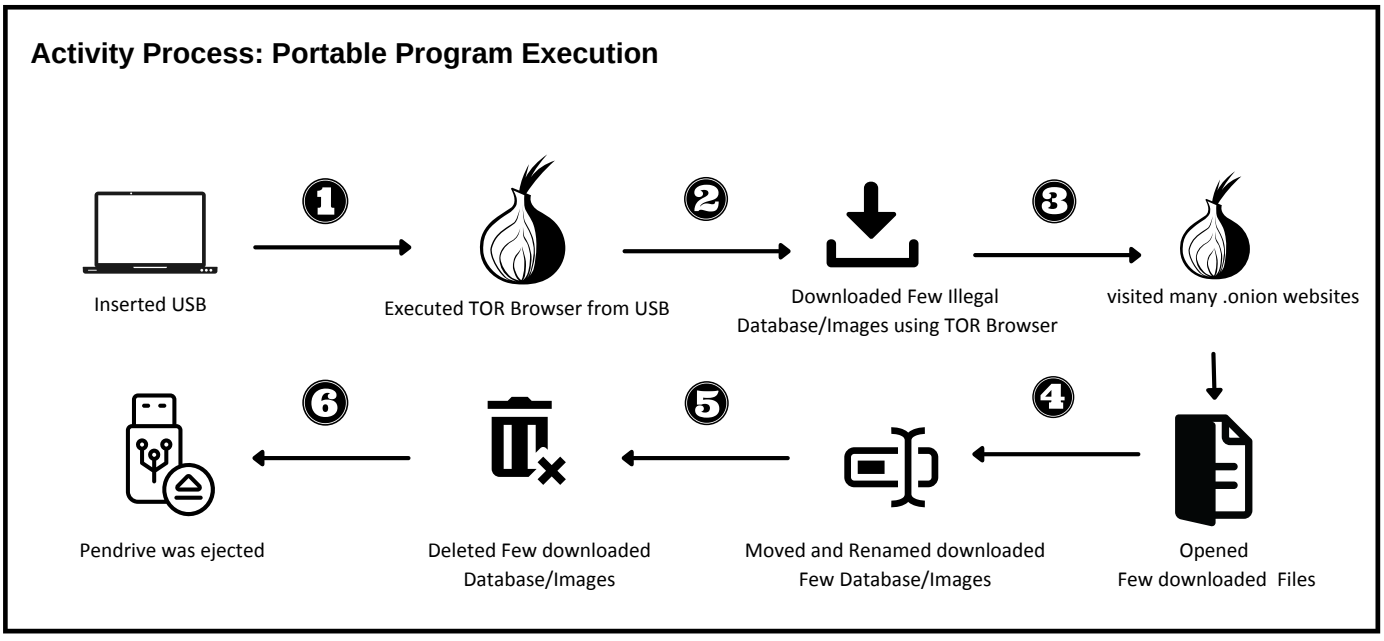


Figure 2: Scenario2 - Running Tor Browser from USB

8. Acquisition Phase:

Figure 3: Forensic Acquisition

Tools Used

a) FTK Imager version 4.3.1.1: We have installed the latest version of FTK Imager version in the default location (Program Files) and copied Copy the entire FTK Imager installation folder (typically "C:\Program Files\AccessData\FTK Imager") to our flash drive.

Note: FTK Imager Lite Version 3.1.1 will not work on the latest Operating System as it will throw below permission error to the user when executing it.

> **This app has been blocked for your protection.**
> **An administrator has blocked you from running this app.**
> **For more information, contact the administrator.**

b) Network Miner V2.7.2: Network Miner is an open-source Network Forensic Analysis Tool (NFAT) for Windows used as a passive packet capturing tool.

c) Rawcap: It is a command-line network sniffer for Windows that uses raw sockets. In our experiment, we are using it to capture Tor browser localhost traffic.

SOURCE: 1. *https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager*
2. https://www.netresec.com

9. Analysis Phase:

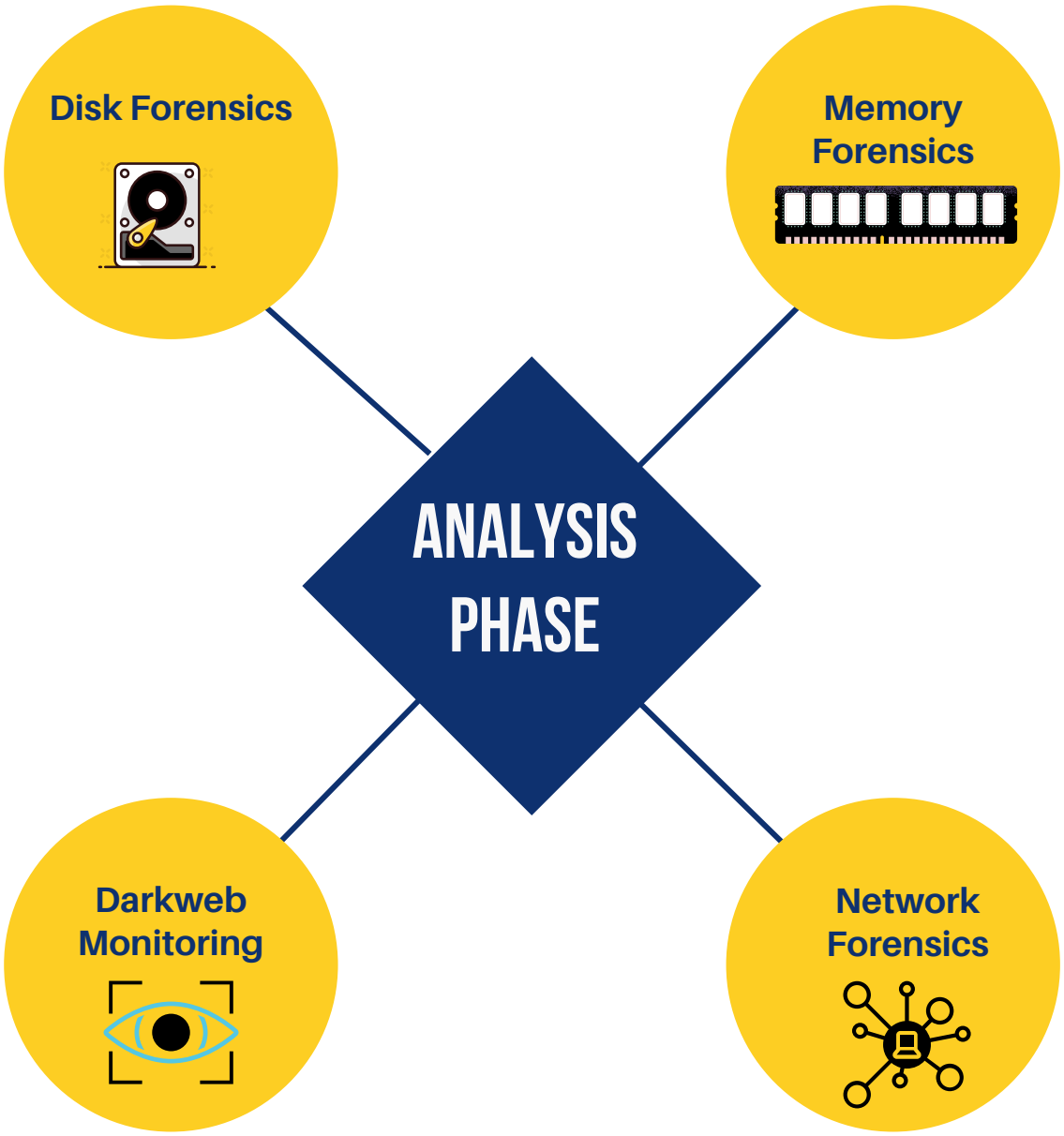
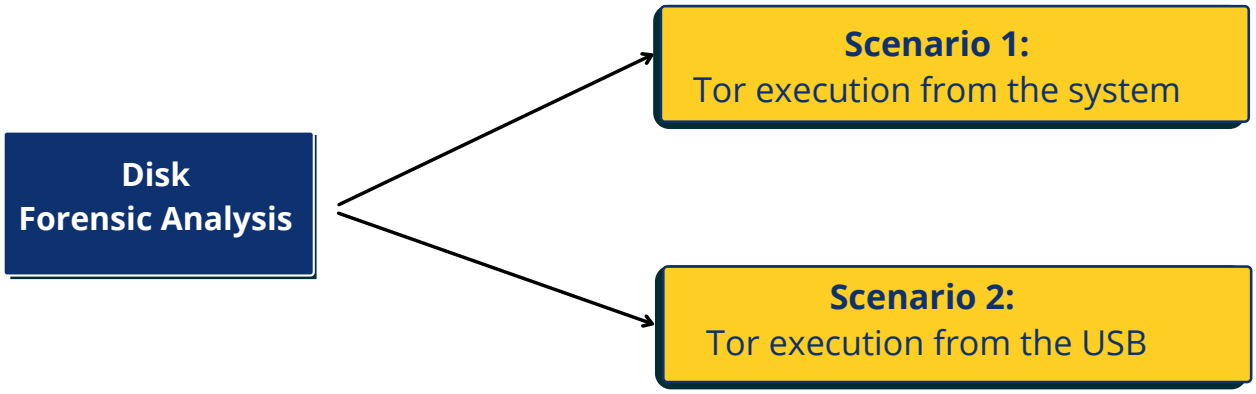


Figure 4: Forensic Analysis Phase

9.1 Disk Forensics

We will be performing disk forensics using free & open source tools, all the tools used in the analysis phase are free and available on the internet. The disk image used in this experiment will be Windows 11 64-bit OS which is acquired by the FTK imager as shown in figure 3. Analysis of the whole disk is done using free & open source Forensic Tools.

Disk Forensics Analysis is Divided into Two Phases



Scenario 1: Disk Forensic Analysis (Executed from the system)

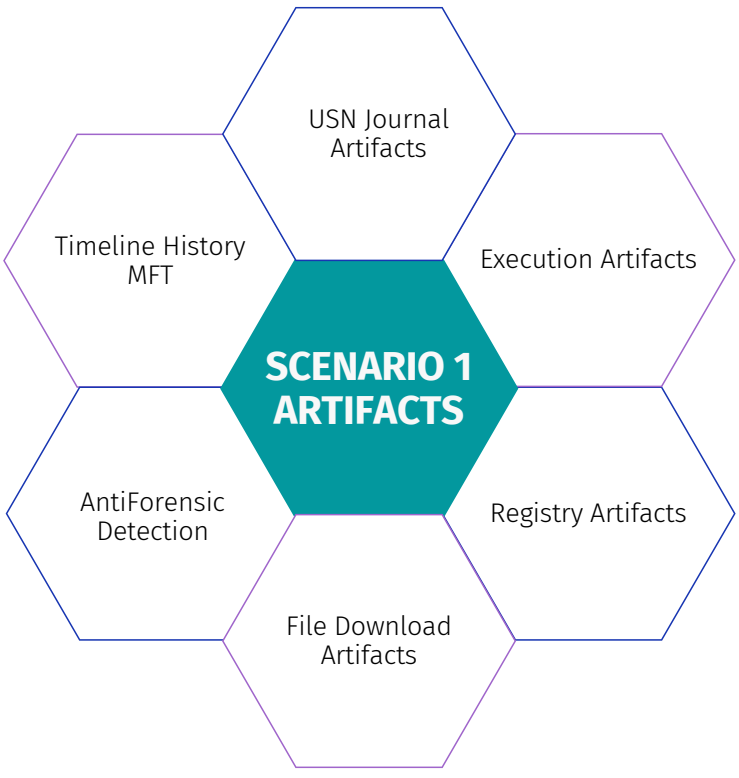


Figure 5: Artifacts List

9.1.2 Artifacts extracted by different Free & Open Source Tools.

Program Execution Artifacts

Jumplist: It allows users to "jump" or access a list of items they frequently or recently used by the user and this feature is available on Windows 7 and later versions in the taskbar button. For the forensic investigator, it is yet another location of the artifacts to trace down the execution of the programs, and it also provides the exact path of the executed program. By default, jumplist is enabled in windows. There are two forms of jumplist created, namely automatic and custom.

Default Location of the Artifacts:
\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent

Tool Used: JLECmd version 1.5.0.0

Result: Jumplist entries indicates Few Images were opened.

3	2022-01-11 09:47:04	2022-01-11 09:47:04	2022-01-11 09:59:32	My Computer\C:\Users\starwhat luffy\Documents\sinaloacartel.jpg	2	1
2	2022-01-11 09:58:46	2022-01-11 09:58:48	2022-01-11 09:59:29	My Computer\C:\Users\starwhat luffy\Documents\243288577_1...	2	1
1	2022-01-11 09:49:22	2022-01-11 09:49:22	2022-01-11 09:59:26	My Computer\C:\Users\starwhat luffy\Documents\120.jpg	2	1

o group by that column

	Target Created On	Target Modified On	Target Accessed On	Absolute Path
	=	=	=	ABC
9	2022-01-11 10:58:25	2022-01-11 10:58:37	2022-01-11 10:58:37	My Computer\E:\New folder (2)
7	2022-01-11 20:29:02	2022-01-11 10:01:27	2022-01-11 10:01:27	My Computer\C:\Windows\addins
3	2022-01-11 07:15:45	2022-01-11 09:58:52	2022-01-11 09:59:32	My Computer\Documents
1	2022-01-11 07:15:45	2022-01-11 07:16:14	2022-01-11 07:16:38	My Computer\Desktop
2	2022-01-11 07:15:45	2022-01-11 07:16:14	2022-01-11 07:16:14	My Computer\Downloads
6	2022-01-11 07:15:45	2022-01-11 07:16:14	2022-01-11 07:16:14	My Computer\Videos
5	2022-01-11 07:15:45	2022-01-11 07:16:14	2022-01-11 07:16:14	My Computer\Music
4	2022-01-11 07:15:45	2022-01-11 07:16:14	2022-01-11 07:16:14	My Computer\Pictures

Figure 6: Jumplist Output

Note: C:\Windows\Addins path was accessed, you can add as the pivot point, in the USNJRNL session we will cover the same.

Prefetch: When the application is executed for the first time, OS creates prefetch which will help to pre-load a piece of data, files and code into memory. This is a great artifact for the forensic investigator to prove the application executed in the system and it would help the malware investigator to identify the malicious DLL loaded by the application. There can be up to 1024 files in the prefetch folder in Windows 8-10 OS.

In our experiment, we export the selected prefetch files from the image disk as per the artifacts design consideration Figure 1, and it will be analyzed using free & open source Tool.

Prefetch File Location: *C:\Windows\Prefetch*

Tool Used: PECMD (Prefetch Explorer Command Line v1.5.0.0) by Eric Zimmerman

```
Command line: -f G:\[root]\Windows\prefetch\TOR.EXE-9CEDC248.pf

Keywords: temp, tmp

Processing G:\[root]\Windows\prefetch\TOR.EXE-9CEDC248.pf

Created on: 2022-01-11 08:27:07
Modified on: 2022-01-11 10:02:39
Last accessed on: 2022-01-11 10:02:39

Executable name: TOR.EXE
Hash: 9CEDC248
File size (bytes): 75,252
Version: Windows 10 or Windows 11

Run count: 3
Last run: 2022-01-11 10:02:29
Other run times: 2022-01-11 09:59:47, 2022-01-11 08:26:57

Volume information:

#0: Name: \VOLUME{01d7f48026d4004b-7226ec21} Serial: 7226EC21 Created: 2021-12-19 02:28:47 Directories: 15 File references: 72

Directories referenced: 15

00: \VOLUME{01d7f48026d4004b-7226ec21}\USERS
01: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY
02: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP
03: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER
04: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER
05: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER
06: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER\DATA
07: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER\DATA\TOR
08: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER\TOR
09: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS
10: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\APPPATCH
11: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\GLOBALIZATION
12: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\GLOBALIZATION\SORTING
13: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32
14: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\EN-US

Files referenced: 55

00: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\C_1252.NLS
02: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\C_437.NLS
03: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\L_INTL.NLS
04: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER\TOR\TOR.EXE (Executable: True)
05: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\KERNEL32.DLL
06: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\KERNELBASE.DLL
```

Figure 7: PECMD Output

Note: Creation date and Last modification date (Filesystem Timestamp) of the prefetch file is always (-10 seconds) because application touches the files within 10 seconds of time.

Filtered Output of the Figure

Created on: 2022-01-11 08:27:07
Modified on: 2022-01-11 10:02:39
Last accessed on: 2022-01-11 10:02:39

Executable name: TOR.EXE
Hash: 9CEDC248
File size (bytes): 75,252
Version: Windows 10 or Windows 11

Run count: 3
Last run: 2022-01-11 10:02:29
Other run times: 2022-01-11 09:59:47, 2022-01-11 08:26:57

Volume information:

#0: Name: \VOLUME{01d7f48026d4004b-7226ec21} Serial: 7226EC21 Created: 2021-12-19 02:28:47 Directories: 15 File references: 72

Directories referenced: 15

06: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER\DATA
07: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER\DATA\TOR

Files referenced: 55

04: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER\TOR\TOR.EXE (Executable: True)

Figure 8: PECMD Output (Filtered Output)

Results:

The new version of the tool even indicates Windows Version as 11 and Executable True Flag. We can find files opened by the application (Tor.exe) within 10 seconds of it execution which includes the full path of executable and also extracts volume information, directory and files referenced, Last run times.

Full Path of the Tor: \USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER\TOR\TOR.EXE

Disk Volume ID: 7226EC21 | **Number of TOR executed**: 3

First Time Program Executed: 2022-01-11 08:26:57 **Last Run:** 2022-01-11 10:02:39

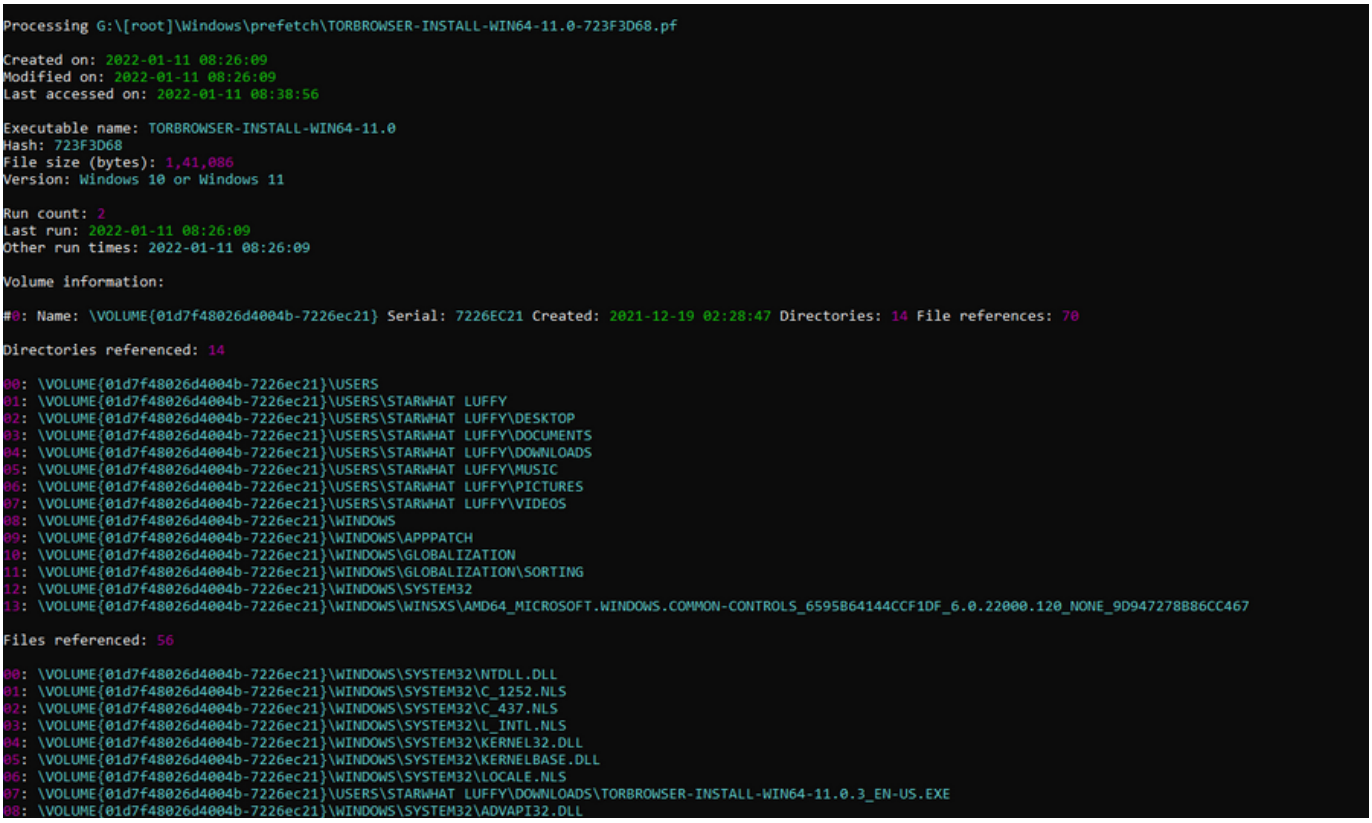


Figure 9: PECMD Output of TORBROWSER-INSTALL-WIN64-11.0

Created on: 2022-01-11 08:26:09
Modified on: 2022-01-11 08:26:09
Last accessed on: 2022-01-11 08:38:56

Filtered Output of the Figure

Executable name: TORBROWSER-INSTALL-WIN64-11.0
Hash: 723F3D68
File size (bytes): 1,41,086
Version: Windows 10 or Windows 11

Run count: 2
Last run: 2022-01-11 08:26:09
Other run times: 2022-01-11 08:26:09

Volume information:

#0: Name: \VOLUME{01d7f48026d4004b-7226ec21} Serial: 7226EC21 Created: 2021-12-19 02:28:47 Directories: 14 File references: 70

Directories referenced: 14
00: \VOLUME{01d7f48026d4004b-7226ec21}\USERS

Files referenced: 56

07: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DOWNLOADS\TORBROWSER-INSTALL-WIN64-11.0.3_EN-US.EXE

Figure 10: PECMD Output of TORBROWSER-INSTALL-WIN64-11.0 (Filtered Output)

Results: The Tor installation executable was deleted by the user after installation but we have found deleted executable in the prefetch folder. We can conclude from above figure TORBROWSER-INSTALL-WIN64-11.0.exe which was downloaded on 2022-01-11 08:26:09

ShimCache: Shimcache also known as AppCompatCache was created by Microsoft (beginning in Windows XP) and used by the operating system to identify application compatibility issues. It keeps track of the application execution including file path, and last modification in Win10/11 Machine.

***ProTip**: Even though attackers wipes prefetch and shimcache using anti-forensic tool, current shimcache entries are stored in the memory and new entries of the shimcache are only written after the shutdown of the system. If the attackers rename the application then the application will be shimmed again with new entries.*

Shimcache File Location:
HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache

Tool Used: AppCompatCache Parser version 1.5.0.0 and Timeline Explorer V 2.0.0.0 by Eric Zimmerman

```
C:\Tools\net6>AppCompatCacheParser.exe -f G:\[root]\Windows\System32\config\SYSTEM --csv C:\Tools
AppCompatCache Parser version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AppCompatCacheParser

Command line: -f G:\[root]\Windows\System32\config\SYSTEM --csv C:\Tools

Processing hive 'G:\[root]\Windows\System32\config\SYSTEM'

Two transaction logs found. Determining primary log...
Primary log: G:\[root]\Windows\System32\config\SYSTEM.LOG2, secondary log: G:\[root]\Windows\System32\config\SYSTEM.LOG1
Replaying log file: G:\[root]\Windows\System32\config\SYSTEM.LOG2
At least one transaction log was applied. Sequence numbers have been updated to 0x00D8. New Checksum: 0x5CC2BFEC
Found 138 cache entries for Windows10Creators in ControlSet001

Results saved to 'C:\Tools\20220130213428_Windows10Creators_SYSTEM_AppCompatCache.csv'
```

Figure 11: AppcompatCacheParser Output

Entry Po…	Execut…	Last Modified Time UTC	Path
1	NA		00000009 5660057900020000 0000000000000000 8664 Microsoft.WindowsStore 8wekyb3d8bbwe
27	NA	2000-01-01 00:00:00	C:\Users\starwhat luffy\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe
30	NA	2000-01-01 00:00:00	C:\Users\starwhat luffy\Desktop\Tor Browser\Browser\firefox.exe
32	NA	2022-01-11 08:26:00	C:\Users\starwhat luffy\Downloads\torbrowser-install-win64-11.0.3_en-US.exe

Figure 12: Output of AppcompatCacheParser Analyzed using Timeline Explorer

Results: The Tor installation executable and Tor.exe was found in the shimcache entries as shown in the above figure and we have observed these entries were written to the SYSTEM hive (Disk) only after the shutdown .

SOURCE: 1. *https://andreafortuna.org/2017/10/16/amcache-and-shimcache-in-forensic-analysis/*

Amcache: It stores the execution of the program. It is yet another location for the forensic investigator to find the timeline of the execution of the program as it tracks installed applications, Programs executed and driver loaded which includes full path location, file size, SHA1 Hashes of the executable and last modified date etc.,

Tool Used: AmcacheParser 1.5.1.0 and Timeline Explorer

Location: C:\Windows\AppCompat\Programs\Amcache

```
C:\Tools\net6>AmcacheParser.exe -i -f G:\[root]\Windows\appcompat\Programs\Amcache.hve --csv C:\Tools\
AmcacheParser version 1.5.1.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser

Command line: -i -f G:\[root]\Windows\appcompat\Programs\Amcache.hve --csv C:\Tools\

Two transaction logs found. Determining primary log...
Primary log: G:\[root]\Windows\appcompat\Programs\Amcache.hve.LOG1, secondary log: G:\[root]\Windows\appcompat\Programs\Amcache.hve.LOG2
Replaying log file: G:\[root]\Windows\appcompat\Programs\Amcache.hve.LOG1
At least one transaction log was applied. Sequence numbers have been updated to 0x0013. New Checksum: 0x7812BCAB
Two transaction logs found. Determining primary log...
Primary log: G:\[root]\Windows\appcompat\Programs\Amcache.hve.LOG1, secondary log: G:\[root]\Windows\appcompat\Programs\Amcache.hve.LOG2
Replaying log file: G:\[root]\Windows\appcompat\Programs\Amcache.hve.LOG1
At least one transaction log was applied. Sequence numbers have been updated to 0x0013. New Checksum: 0x7812BCAB

G:\[root]\Windows\appcompat\Programs\Amcache.hve is in new format!

Total file entries found: 73
Total device containers found: 15
Total device PnPs found: 191

Found 59 unassociated file entry and 14 program file entries (across 15 program entries)

Results saved to: C:\Tools\

Total parsing time: 0.164 seconds
```

Figure 13: Output of Amcache Parser

File Key Last Writ…	SHA1	Full Path
2022-01-11 08:26:56	266b9fcf61aa5c838ce472df83d950…	c:\users\starwhat luffy\desktop\tor browser\browser\firefox.exe
2022-01-11 08:26:27	4b8e45ba45e234757933bb01fedd56…	c:\users\starwhat luffy\downloads\torbrowser-install-win64-11.0.3_en-us.exe

Figure 14: Output of Amcache Parser is analyzed using Timeline Explorer

In the above output, amcache parser has parsed Application Unassociated Entries which contains the full path of the executable and Hash of the Program along with file size, file version number, Last Modified Date, USN Journal Entry Number.

***ProTip**: Malware or evil executable can be indentified its renamed using SHA1 Algorithm.*

Filtered Output

File Key Last Write Timestamp	SHA1	Full Path
2022-01-11 08:26:27	4b8e45ba45e23475793 3bb01fedd56ea00688b 44	c:\users\starwhat luffy\downloads\ torbrowser-install-win64-11.0.3_en-us.exe
2022-01-11 08:26:56	266b9fcf61aa5c838ce4 72df83d95091aff94ff3	c:\users\starwhat luffy\desktop\tor browser\browser\firefox.exe

Figure 15: Output of Amcache (Filtered Verison)

Result: We have identified Full Path location of the Tor Browser including Hash of the Program and in above results were part of UnassociatedFileEntries of the Amcache where executable may not be part of installation packages.

Note: Entries in the Amcache doesn't necessarily indicate that program was executed from the system, It also indicate that executable was present as shown in above figure **torbrowser-install-win64-11.0.3_en-us.exe** was downloaded from the internet.

Registry Artifacts

As the definition goes, a registry is a collection of databases of configuration settings for Windows OS and at the same time, it is a treasure box for the forensic investigator.

In our experiment, we have exported Registry Hive namely 'NTUSER.DAT', 'System' & 'Software' from the Acquired image using FTK Imager and was analysed by free Registry Forensic Tool.

Tool Used: Registry Explorer V 2.0.0.0 by Eric Zimmerman's

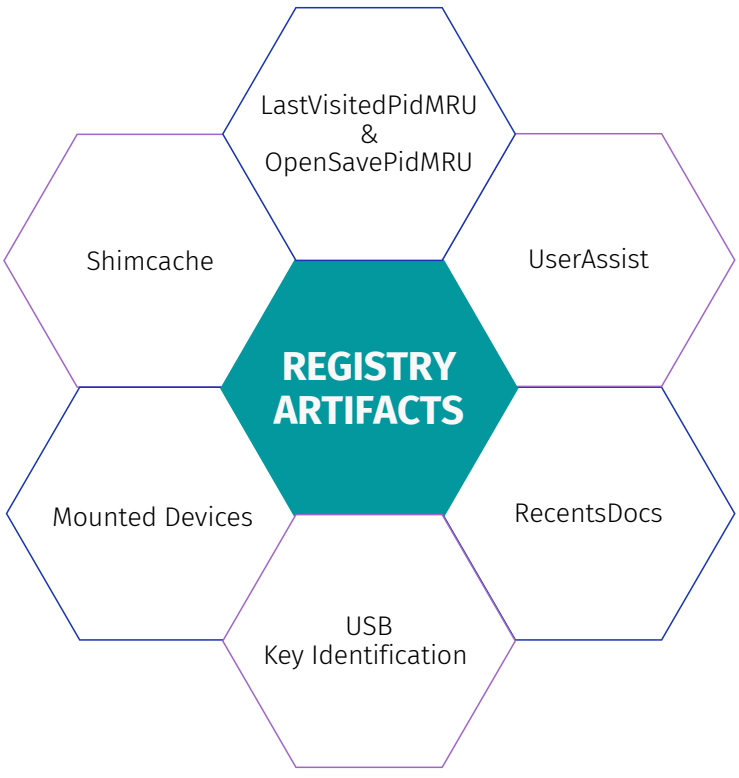


Figure 16: Registry Artifacts

a) LastVisitedPidMRU & OpenSavePidMRU: OpenSavePidMRU registry key tracks files that have been opened or saved from the Windows shell dialog box by the user and LastVisitedPidMRU tracks the specific program used by the user to open the files (which are stored in OpenSavePidMRU).

Registry Location:
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\

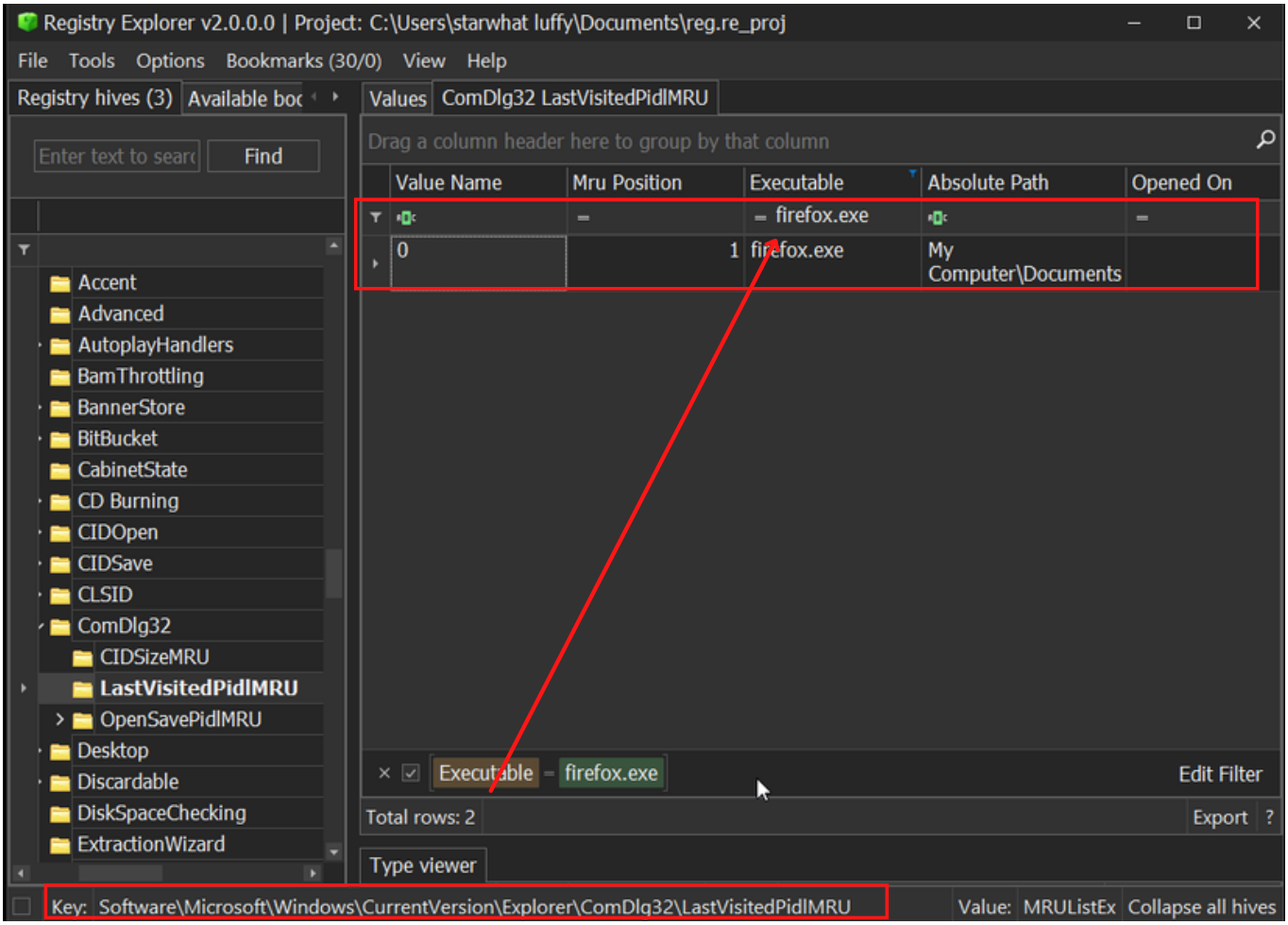


Figure 17: LastVisitedPIDMRU Output

We can observe in the above figure 17, any traces related to the Tor browser are not found in OpenSavePidMRU registry key, but the execution of the Tor/Firefox is found in LastVisitPidMRU Key.

b) UserAssist: This key contains the execution of the programs in the system, which is yet another location for the forensic examiner. Unlike other artifacts, userAssist will include information on whether the application was run from a shortcut link or directly from the installed location.

Registry location:
NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count

CEBFF6CD: This key in the registry indicates Executable File Execution.

F4E57C4B: This key indicates Shortcut File Execution

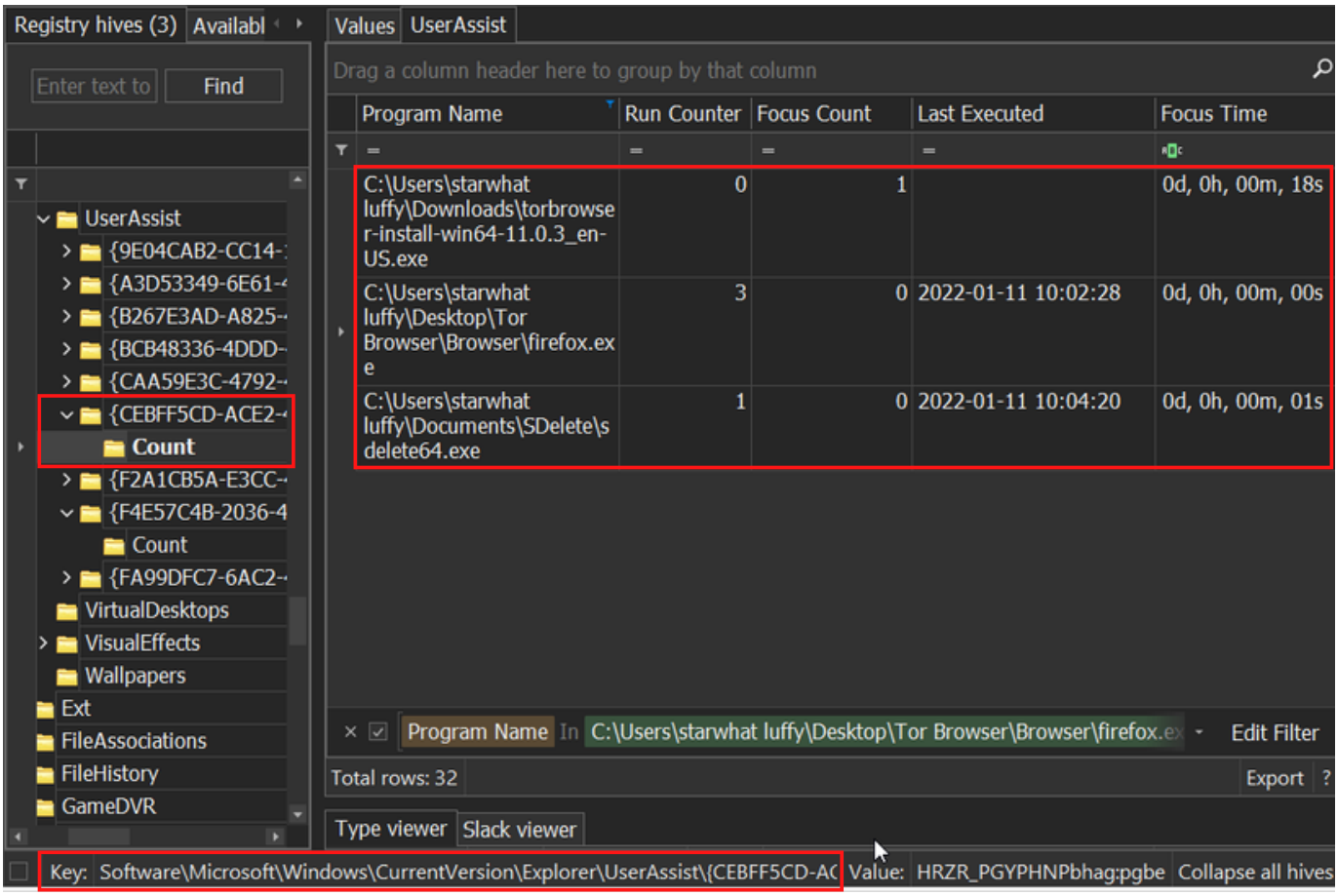


Figure 18: UserAssist Output (Execution from the Installed Location)

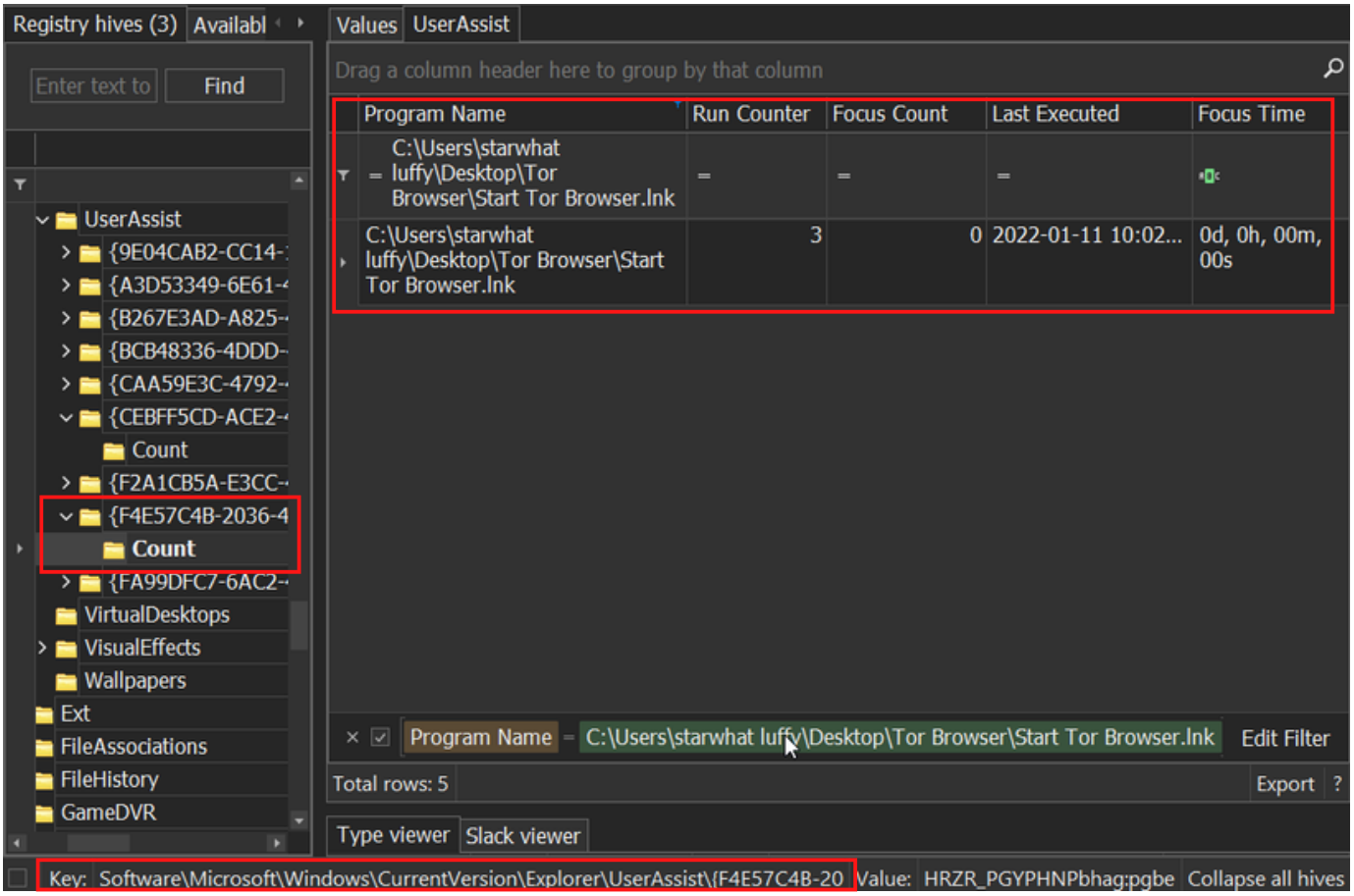


Figure 19: UserAssist Output (Shortcut Execution)

As shown in figure 18 & 19, we can observe that all the artifacts related to Tor Browser Execution and Tor Installer Program has been found and also Run Counter indicates the number of times application was executed.

Note: SDelete is an Anti-Forensic Tool which was executed and captured by Userassist Entries in figure 18, we will analyze in-depth on SDelete Tool in Anti-Forensic Detection Phase.

c. RecentDocs: This key tracks the recent documents opened by the programs.

Location:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

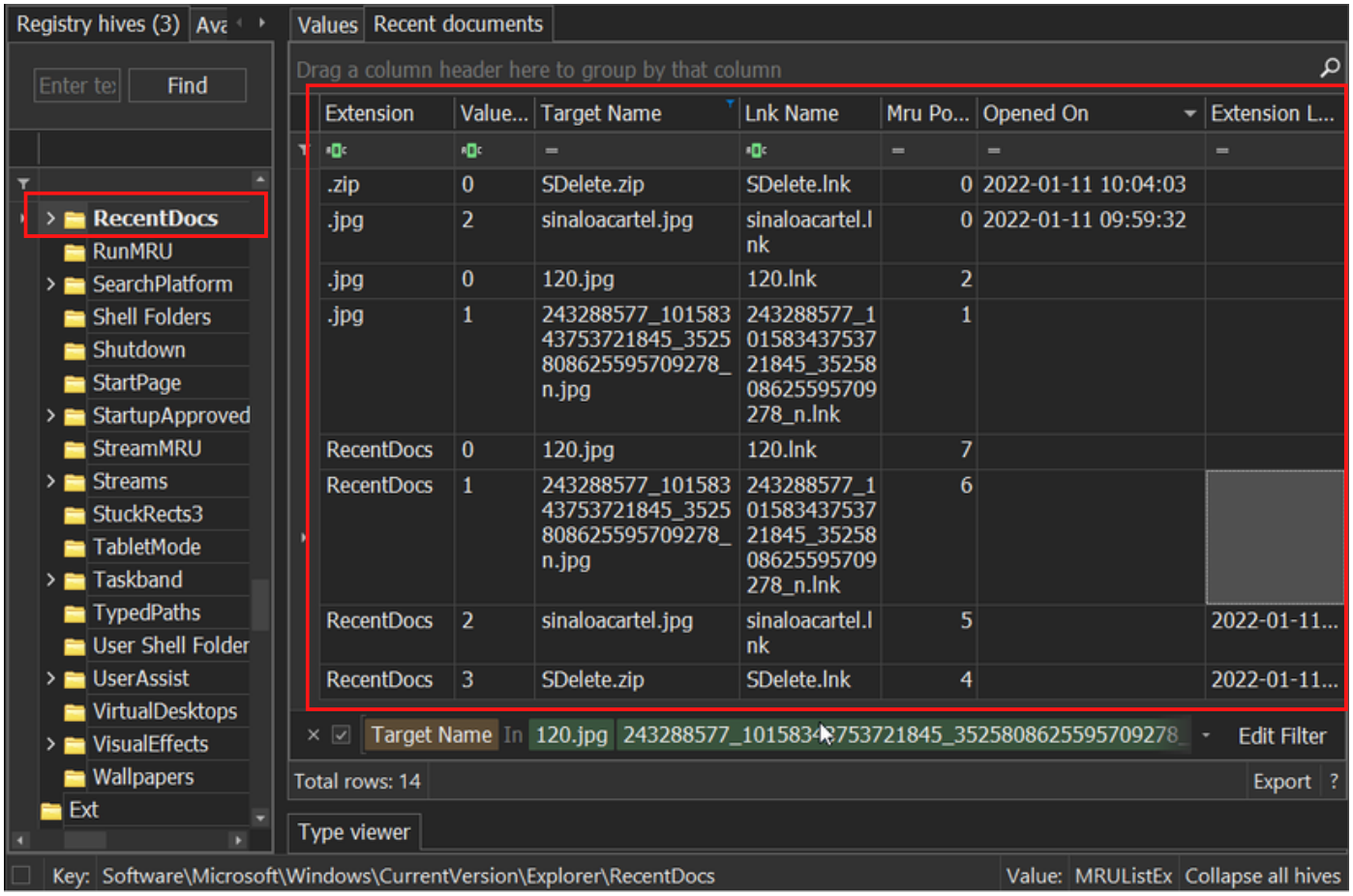


Figure 20: RecentDocs Output

As shown in the figure, we can conclude that many images downloaded/opened and a few files (SDelete.zip) are subjected to permanent delete since the file is missing from the acquired image.

Note: SDelete is an Anti-Forensic Tool, we will analyze in-depth on SDelete Tool in Anti-Forensic Detection Phase.

Download Execution Artifacts

Zone Identifier Artifacts: When the files are downloaded from the internet a zone Identifier Alternate Data Stream are tagged. If the Zone is “dangerous” a warning dialog may be presented to the user (Windows SmartScreen) when the file is executed.

Most common Zone Identifier:

-1 = NOZONE
0 = LOCAL MACHINE ZONE
1 = INTRANET ZONE
2 = TRUSTED
3 = INTERNET
4 = UNTRUSTED

Note: The Alternate Data Stream travels with the file between NTFS disks, but ADS will be lost if the file is copied or moved to other file system like FAT32 as ADS is not supported.

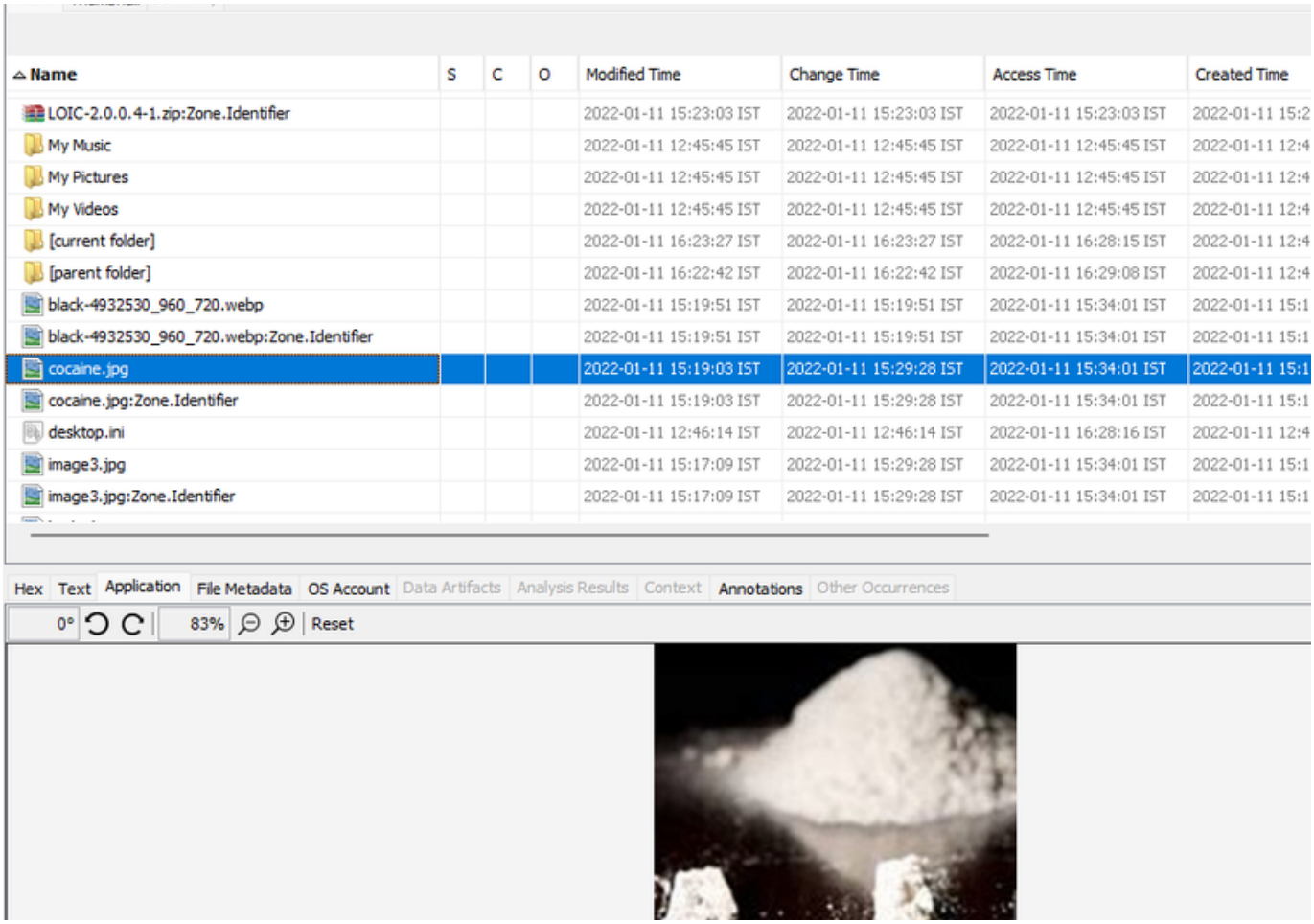


Figure 21: Autopsy Tool Results (Filesystem Analysis)

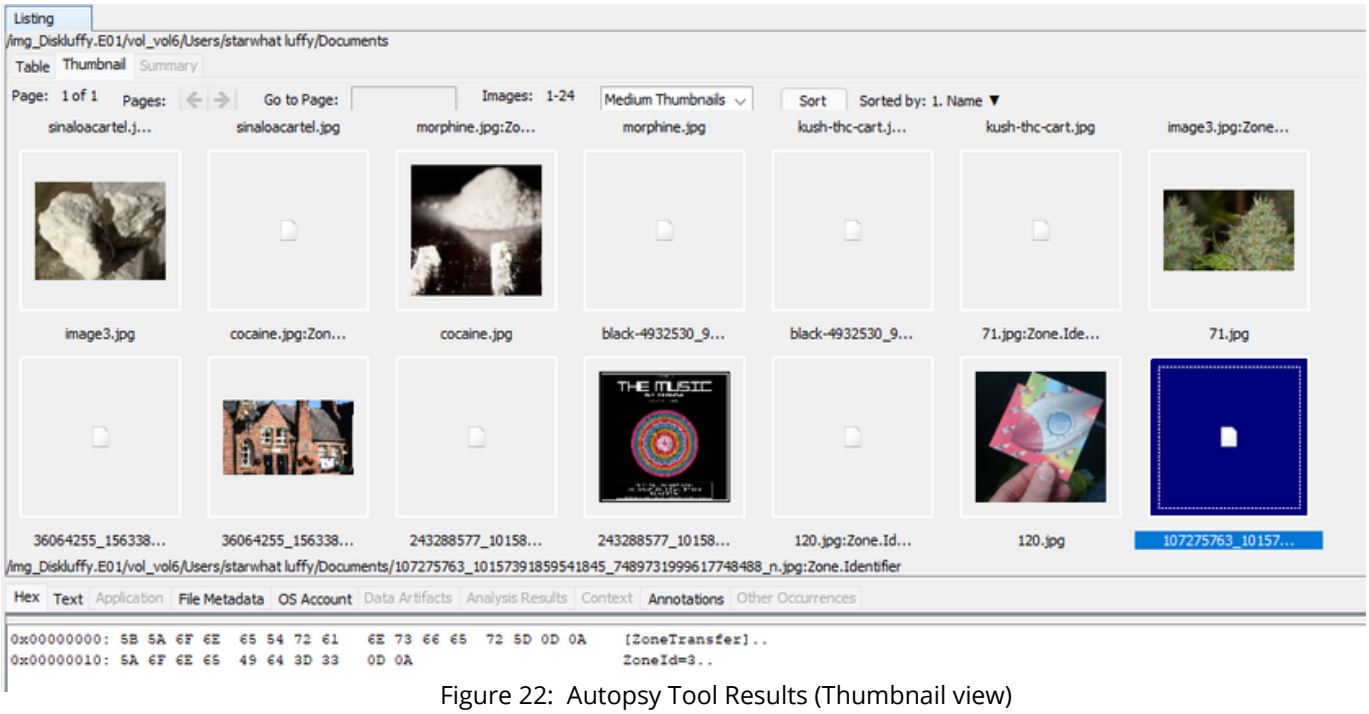


Figure 22: Autopsy Tool Results (Thumbnail view)

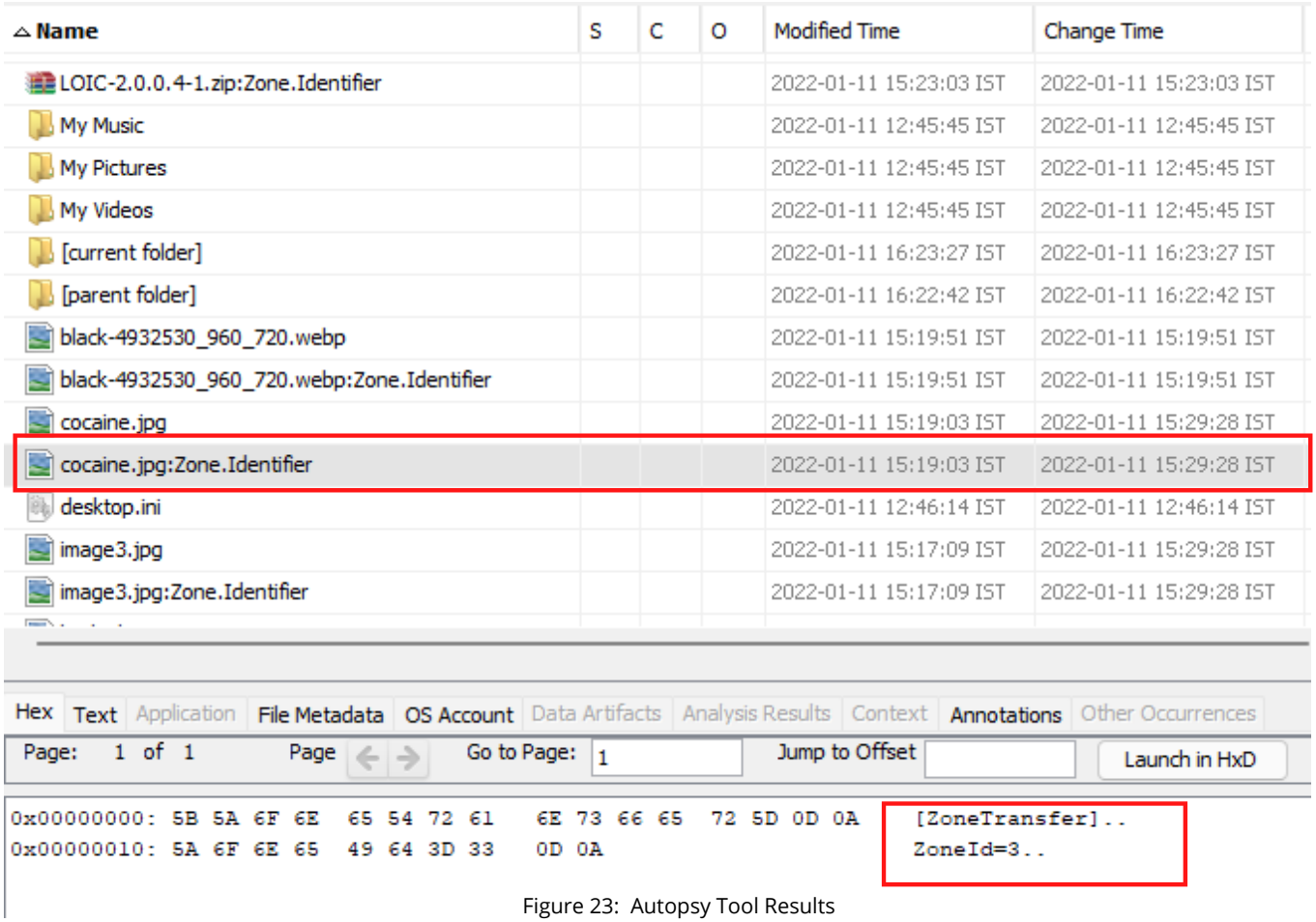


Figure 23: Autopsy Tool Results

We can conclude from the figure 21,22 & 23 drug images and files which are tagged with **Zone.Identifier =** 3 are downloaded from the Internet source. As Tor is based on Firefox, so we have only the zone, the referrerUrl is absent in ZoneID ADS.

SOURCE: 1. *http://cyberforensicator.com/2018/06/26/where-did-it-come-from-forensic-analysis-of-zone-identifier/*
2. *https://www.autopsy.com/download/*

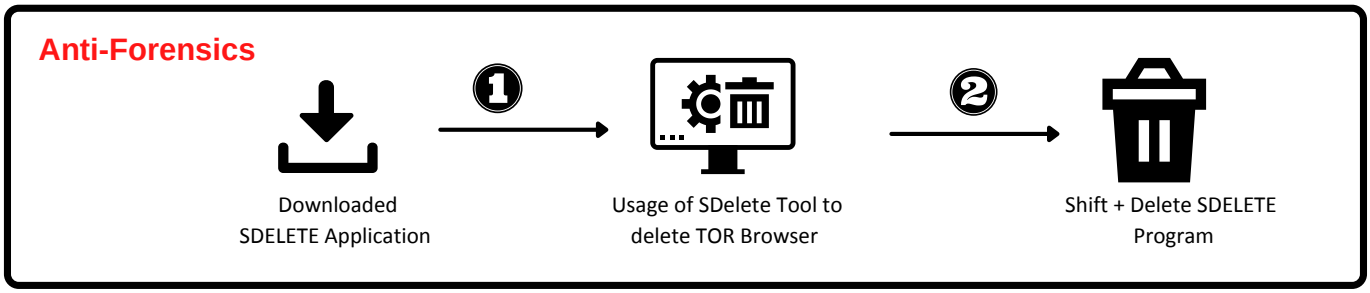
Anti-Forensics Detection

Anti-Forensic

Anti-Forensic is widely used by attackers to cover their tracks and use different techniques, tools to wipe their activity in windows OS but destroying all the references and artifacts is almost impossible.

We have seen a program called SDelete in the prefetch folder at the beginning and in the recentdocs artifacts (Ref Figure 20).

As per the Artifacts creation (Ref Figure: 1) the attacker has downloaded SDelete Program to wipe the TorBrowser Folder from the Windows OS as SDelete repeatedly overwrites the deleted data with random characters recovering files is impossible but we can find the references or artifacts related to his activity.



Objectives:

1. Find the Execution of SDelete Application.
2. Usage of SDelete Tool to Delete Tor Browser.

SDelete is a data wiping tool and an excellent Antiforensic tool as it is signed by Microsoft. SDelete is a tool that irrecoverably deletes files, conforming to U.S. Department of Defense standard DoD 5220.22-M for the handling of classified information.

SOURCE:
1. https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete
2. https://www.computerhope.com/issues/ch000038.htm

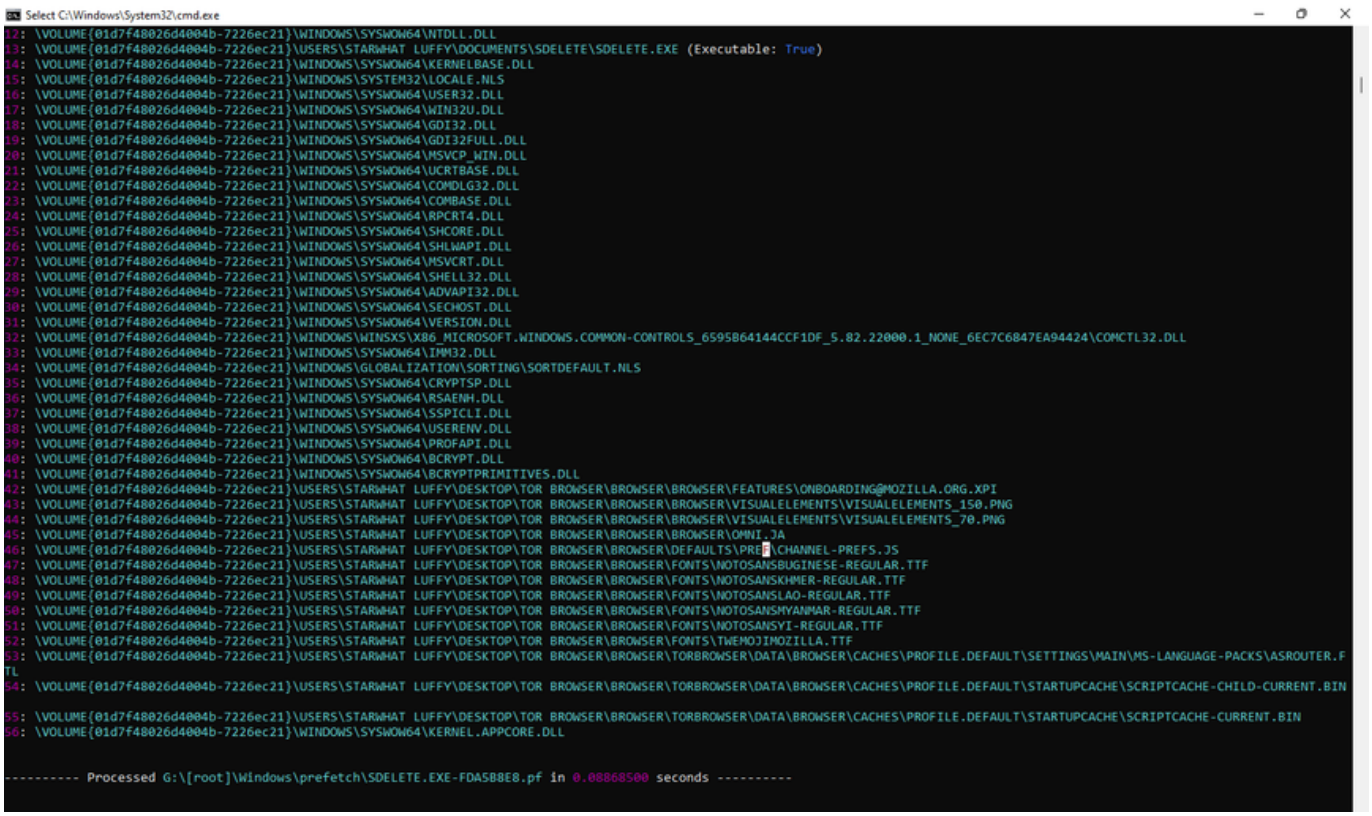


Figure 24: PECMD output for the Sdelete Prefetch File

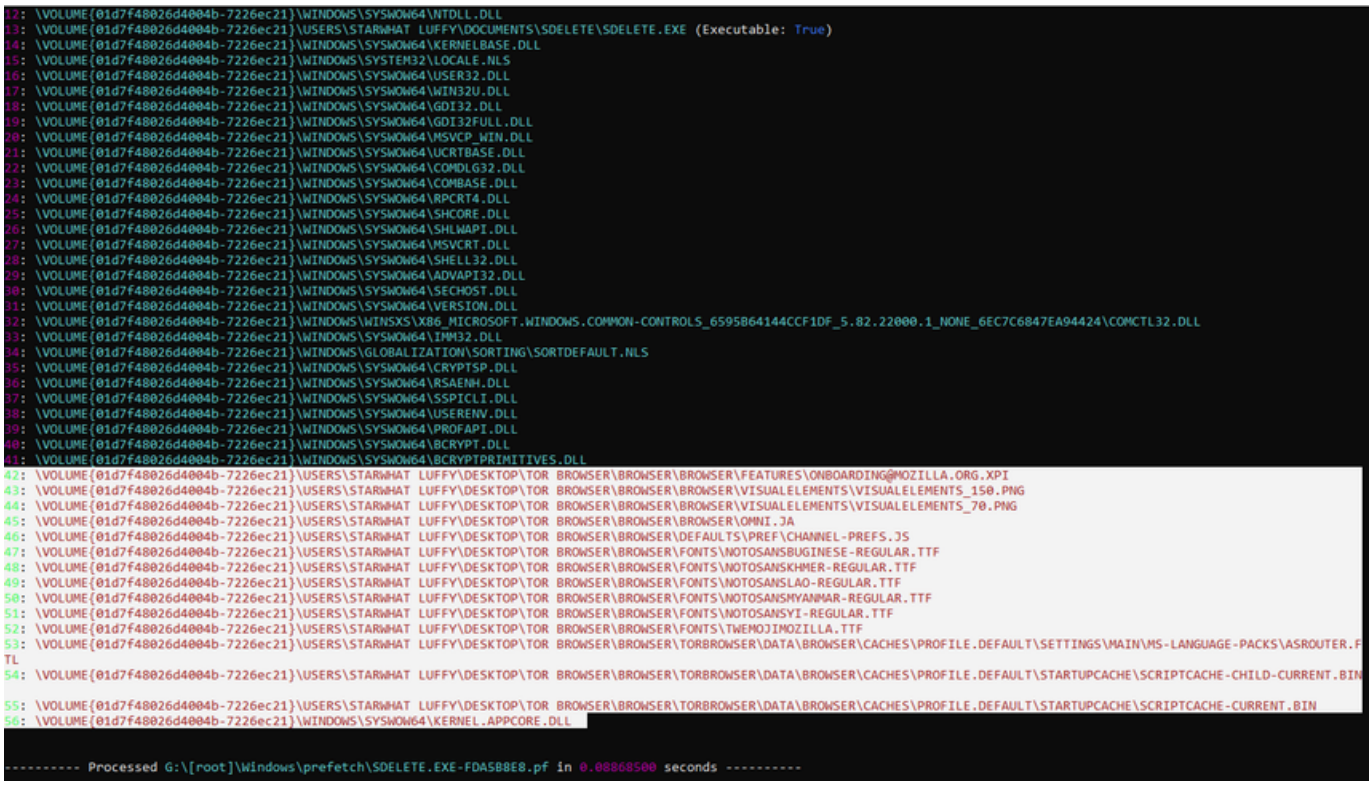


Figure 25: PECMD output for the Sdelete Prefetch File

Created on: 2022-01-11 10:04:34
Modified on: 2022-01-11 10:52:39
Last accessed on: 2022-01-11 10:52:39

Executable name: SDELETE.EXE
Hash: FDA5B8E8
File size (bytes): 75,250
Version: Windows 10 or Windows 11

Run count: 9
Last run: 2022-01-11 10:52:39
Other run times: 2022-01-11 10:49:40, 2022-01-11 10:47:47, 2022-01-11 10:47:20, 2022-01-11 10:47:15, 2022-01-11 10:47:02, 2022-01-11 10:05:56, 2022-01-11 10:05:42

Volume information:

#0: Name: \VOLUME{01d7f48026d4004b-7226ec21} Serial: 7226EC21 Created: 2021-12-19 02:28:47 Directories: 14 File references: 57

Directories referenced: 14

00: \VOLUME{01d7f48026d4004b-7226ec21}\$EXTEND
01: \VOLUME{01d7f48026d4004b-7226ec21}\USERS
02: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY
03: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP
04: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER
05: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER
06: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DOCUMENTS
07: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DOCUMENTS\SDELETE

Files referenced: 57

13: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DOCUMENTS\SDELETE\SDELETE.EXE (Executable: True)
42: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\BROWSER\FEATURES\ONBOARDING@MOZILLA.ORG.XPI
43: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\BROWSER\VISUALELEMENTS\VISUALELEMENTS_150.PNG
44: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\BROWSER\VISUALELEMENTS\VISUALELEMENTS_70.PNG
45: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\BROWSER\OMNI.JA
46: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\DEFAULTS\PREF\CHANNEL-PREFS.JS
47: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\FONTS\NOTOSANSBUGINESE-REGULAR.TTF
48: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\FONTS\NOTOSANSKHMER-REGULAR.TTF
49: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\FONTS\NOTOSANSLAO-REGULAR.TTF
50: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\FONTS\NOTOSANSMYANMAR-REGULAR.TTF
51: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\FONTS\NOTOSANSYI-REGULAR.TTF
52: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\FONTS\TWEMOJIMOZILLA.TTF
53: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER\DATA\BROWSER\CACHES\PROFILE.DEFAULT\SETTINGS\MAIN\MS-LANGUAGE-PACKS\ASROUTER.FTL
54: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER\DATA\BROWSER\CACHES\PROFILE.DEFAULT\STARTUPCACHE\SCRIPTCACHE-CHILD-CURRENT.BIN
55: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DESKTOP\TOR BROWSER\BROWSER\TORBROWSER\DATA\BROWSER\CACHES\PROFILE.DEFAULT\STARTUPCACHE\SCRIPTCACHE-CURRENT.BIN

Figure 26: Filtered Results of the PECMD Output (Reference Fig 24 & 25)

We can observe in Figure 26 (Filtered Output of Fig 24 & 25), the results fetched by the PECMD command for the SDELETE.EXE-FDA5B8E8.pf prefetch file concludes that SDelete has touched File's and Directory of the Tor Browser (Installed Folder) within 10 seconds (i.e: SDelete has Wiped Tor Browser Installed Folder which was saved in the Desktop)

Overall Results:

SDelete Path: \VOLUME{01d7f48026d4004b-7226ec21}\USERS\STARWHAT LUFFY\DOCUMENTS\SDELETE\SDELETE.EXE (Executable: True)

Volume Serial Number:7226EC21 (Serial Number of the Disk where SDelete was executed)

Number of Times SDelete was Executed: 9

Created on: 2022-01-11 10:04:34 (Filesystem Time)
First Time Program Executed: 2022-01-11 10:05:42
Last accessed on: 2022-01-11 10:52:39

Anti-Forensic Detection of SDelete Tool in $UsnJrnl

USNJRNL

The NTFS change journal ($UsnJrnl) is an operating system file that records when changes are made to files and directories. It has wealth of information for the Forensic Investigator, which gives a better overview of what happened to a system.

…	Update Timestamp	Name	Exte…	Paren…	Entr…	Update Reasons
	=			=	=	
	2022-01-11 10:5…	TorBAAAAAAAAAAAAAAAAAAAAAAAA…	.AAA	3174	10569	RenameNewName
	2022-01-11 10:5…	TorBAAAAAAAAAAAAAAAAAAAAAAAA…	.AAA	3174	10569	RenameNewName|Close
	2022-01-11 10:5…	TorBAAAAAAAAAAAAAAAAAAAAAAAA…	.AAA	3174	10569	RenameOldName
	2022-01-11 10:5…	TorBBBBBBBBBBBBBBBBBBBBBBBB…	.BBB	3174	10569	RenameNewName
	2022-01-11 10:5…	TorBBBBBBBBBBBBBBBBBBBBBBBB…	.BBB	3174	10569	RenameNewName|Close
	2022-01-11 10:5…	TorBBBBBBBBBBBBBBBBBBBBBBBB…	.BBB	3174	10569	RenameOldName
	2022-01-11 10:5…	TorBCCCCCCCCCCCCCCCCCCCCCCCC…	.CCC	3174	10569	RenameNewName
	2022-01-11 10:5…	TorBCCCCCCCCCCCCCCCCCCCCCCCC…	.CCC	3174	10569	RenameNewName|Close
	2022-01-11 10:5…	TorBCCCCCCCCCCCCCCCCCCCCCCCC…	.CCC	3174	10569	RenameOldName
	2022-01-11 10:5…	TorBDDDDDDDDDDDDDDDDDDDDDDDD…	.DDD	3174	10569	RenameNewName
	2022-01-11 10:5…	TorBDDDDDDDDDDDDDDDDDDDDDDDD…	.DDD	3174	10569	RenameNewName|Close
	2022-01-11 10:5…	TorBDDDDDDDDDDDDDDDDDDDDDDDD…	.DDD	3174	10569	RenameOldName
	2022-01-11 10:5…	TorBEEEEEEEEEEEEEEEEEEEEEEEE…	.EEE	3174	10569	RenameNewName

Figure 27: Output of USNJRNL

We can observe for the Parent MFT Entry 3174 which is assigned for the Tor Browser is subjected to the renaming of the Tor Browser Directory as mentioned in the update reasons of the USNJRNL entries (Reference Figure 27) with successive alphabetic character naming scheme as mentioned in official Microsoft Page. This concludes the usage of the SDelete Tool to wipe the Tor Browser Program.

> *To overwrite file names of a file that you delete, SDelete renames the file 26 times, each time replacing each character of the file's name with a successive alphabetic character. For instance, the first rename of "foo.txt" would be to "AAA.AAA".*
>
> *-Microsoft*

Figure 28: Output of SystemIndex Log

You can find similar logs in Windows Search Index logs which is yet another location for the investigator to co-relate the evidence as shown in above Figure 28.

Location:
[root]\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex

The index store, called SystemIndex, contains all retrievable Windows IPropertyStore values for indexed items.

SOURCE:
1. https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete
2. https://www.hecfblog.com/search/label/usnjrnl?max-results=20

Update Timestamp	Name	Extension	Paren…	Entr…	Update Reasons
2022-01-11 10:03:58	SDelete.zip	.zip	3535	10459	FileCreate
2022-01-11 10:04:03	SDelete.lnk	.lnk	3550	10632	DataExtend|FileCreate
2022-01-11 10:04:16	sdelete.exe	.exe	5139	10348	FileCreate
2022-01-11 10:04:34	SDELETE.EXE-FDA5B8E8.pf	.pf	212098	10645	FileCreate
2022-01-11 10:49:40	SDELETE.EXE-FDA5B8E8.pf	.pf	212098	10645	DataTruncation
2022-01-11 10:49:44	CMD.EXE-0BD30981.pf	.pf	212098	10648	DataTruncation
2022-01-11 10:52:39	TorAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA…	.AAA	3536	10224	RenameNewName
2022-01-11 10:52:39	TorAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA…	.AAA	3536	10224	RenameNewName|Close
2022-01-11 10:52:39	TorAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA…	.AAA	3536	10224	RenameOldName
2022-01-11 10:52:39	TorBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB…	.BBB	3536	10224	RenameNewName
2022-01-11 10:52:39	TorBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB…	.BBB	3536	10224	RenameNewName|Close
2022-01-11 10:52:39	TorBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB…	.BBB	3536	10224	RenameOldName
2022-01-11 10:52:39	TorCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC…	.CCC	3536	10224	RenameNewName
2022-01-11 10:52:39	TorCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC…	.CCC	3536	10224	RenameNewName|Close
2022-01-11 10:52:39	TorCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC…	.CCC	3536	10224	RenameOldName
2022-01-11 10:52:39	TorDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD…	.DDD	3536	10224	RenameNewName
2022-01-11 10:52:39	TorDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD…	.DDD	3536	10224	RenameNewName|Close
2022-01-11 10:52:39	TorDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD…	.DDD	3536	10224	RenameOldName
2022-01-11 10:52:39	TorEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE…	.EEE	3536	10224	RenameNewName
2022-01-11 10:52:39	TorEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE…	.EEE	3536	10224	RenameNewName|Close

Figure 29: Anti-forensic Timeline Activity

Update Timestamp	Name	Extension	Paren…	Entr…	Update Reasons
2022-01-11 10:52:42	DeVVVVVVVVVVVVVVVVVVVVVVVVVVVVV.VVV	.VVV	3523	10164	RenameNewName|Close
2022-01-11 10:52:42	DeVVVVVVVVVVVVVVVVVVVVVVVVVVVVV.VVV	.VVV	3523	10164	RenameOldName
2022-01-11 10:52:42	DeWWWWWWWWWWWWWWWWWWWWWWWWWWWW.WWW	.WWW	3523	10164	RenameNewName
2022-01-11 10:52:42	DeWWWWWWWWWWWWWWWWWWWWWWWWWWWW.WWW	.WWW	3523	10164	RenameNewName|Close
2022-01-11 10:52:42	DeWWWWWWWWWWWWWWWWWWWWWWWWWWWW.WWW	.WWW	3523	10164	RenameOldName
2022-01-11 10:52:42	DeXXXXXXXXXXXXXXXXXXXXXXXXXXXX.XXX	.XXX	3523	10164	RenameNewName
2022-01-11 10:52:42	DeXXXXXXXXXXXXXXXXXXXXXXXXXXXX.XXX	.XXX	3523	10164	RenameNewName|Close
2022-01-11 10:52:42	DeXXXXXXXXXXXXXXXXXXXXXXXXXXXX.XXX	.XXX	3523	10164	RenameOldName
2022-01-11 10:52:42	DeYYYYYYYYYYYYYYYYYYYYYYYYYYYY.YYY	.YYY	3523	10164	RenameNewName
2022-01-11 10:52:42	DeYYYYYYYYYYYYYYYYYYYYYYYYYYYY.YYY	.YYY	3523	10164	RenameNewName|Close
2022-01-11 10:52:42	DeYYYYYYYYYYYYYYYYYYYYYYYYYYYY.YYY	.YYY	3523	10164	RenameOldName
2022-01-11 10:52:42	DeZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZ	.ZZZ	3523	10164	RenameNewName
2022-01-11 10:52:42	DeZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZ	.ZZZ	3523	10164	RenameNewName|Close
2022-01-11 10:52:42	DeZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZ	.ZZZ	3523	10164	RenameOldName
2022-01-11 10:52:42	000200000000027B4223339EF		29	10164	RenameNewName
2022-01-11 10:53:23	sdelete.exe	.exe	5139	10348	FileDelete|Close
2022-01-11 10:53:23	sdelete64.exe	.exe	5139	10551	FileDelete|Close
2022-01-11 10:53:23	sdelete64a.exe	.exe	5139	10555	FileDelete|Close
2022-01-11 10:53:23	SDelete		3535	5139	FileDelete|Close
2022-01-11 10:53:27	SDelete.zip	.zip	3535	10595	FileDelete|Close

Figure 30: Anti-Forensic Timeline Activity

We can conclude from figure 29 & 30, the Timeline Activity of the Anti-Forensic Process. The USNJRNL is an excellent Artifact to find out what happened in the system at a certain interval of time. We can refer to the timeline Process Activity of Anti-Forensic Detection in figure 31.

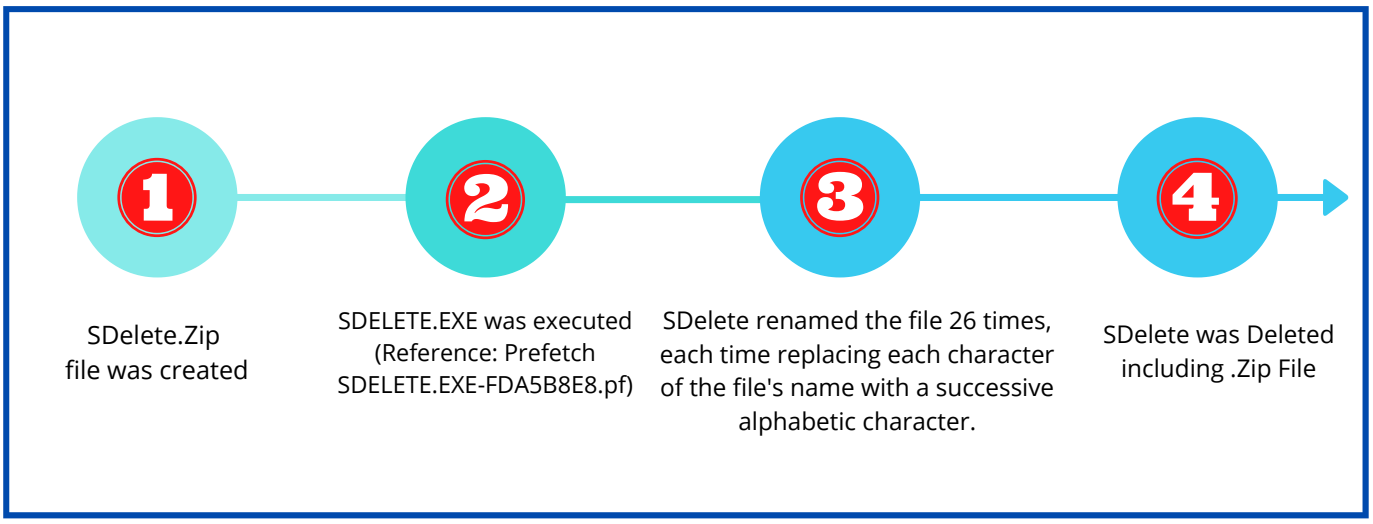


Figure 31: Anti-Forensic Tiimeline Process

We observe from the above figure 31, at the beginning Sdelete.Zip was downloaded by the Browser and it was executed (Reference Prefetch Figure Number: 26).

We have already observed in the prefetch phase, SDelete has touched the Tor Browser Installation directory within 10 seconds and in USNJRNL logs, soon after SDelete execution, Tor Browser was renamed with a successive alphabetic character naming scheme and SDelete has wiped the whole Tor Browser Directory. After the wiping process, Sdelete including SDelete.zip was subjected to deletion.

File System Timeline

Timeline analysis is an excellent analytical technique for a forensic investigator to examine the system activity at the time of the incident as adversaries leave footprints everywhere on the machine. This will help us know the story of what happened in the system at a certain interval of time.

Timeline analysis is the best technique to detect the anti-forensic techniques, as hackers leave a trace in the system after compromise and it's almost impossible for the hacker to wipe all the traces. The timeline analysis techniques are the key to exploring those hidden artifacts and a great method to know what happened in the system in a certain interval of time.

File system Analysis

It collects all the files, directories from allocated and unallocated sectors of the volume.In our process, MFTECmd Command will extract contents from $MFT (Master File Table)

Tools Used: MFTECmd V 1.1.0.0 / Mactime (Optional) and Timeline Explorer

During timeline analysis, we need to understand the basic concepts of MACB Timestamps.

The MACB times are derived from file system metadata, and they stand for:

Modified
Accessed
Changed ($MFT Modified)
Birth (file creation time)

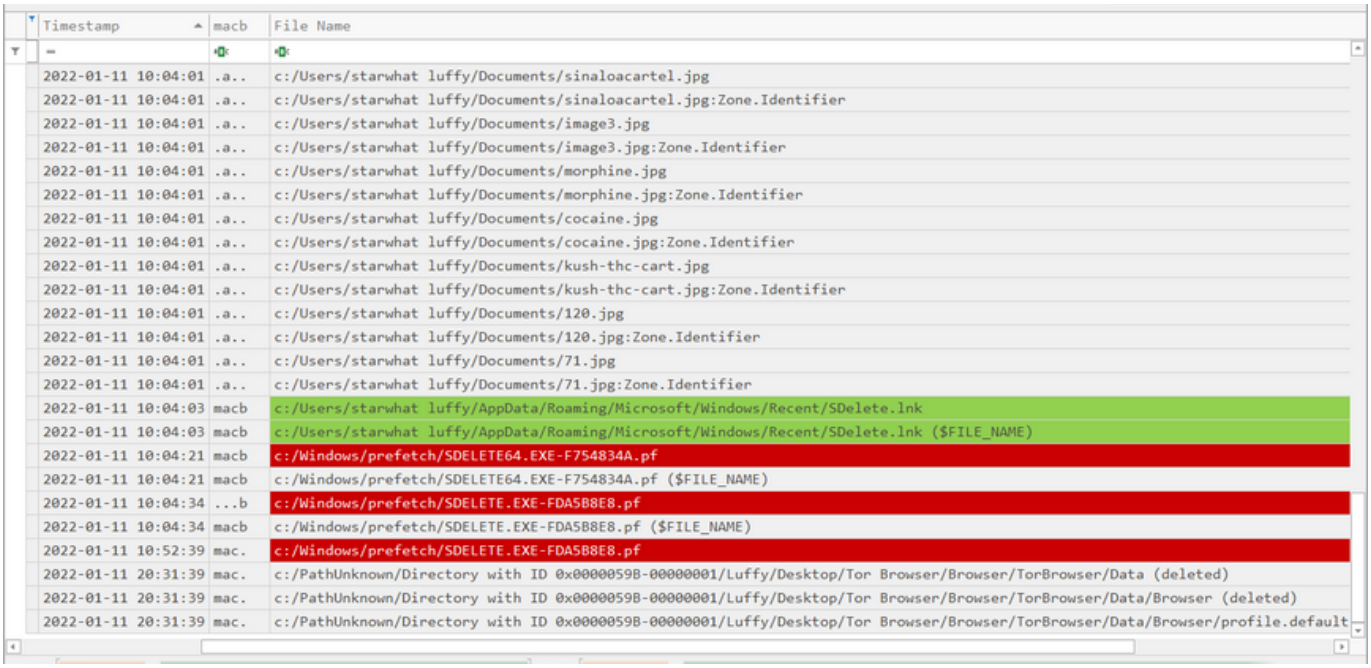
Note: Overwhelming procedure as there are too many artifacts found in the system which creates a lot of noise for the analyst while timeline analysis

Time Analysis Process:

Step1:Extract MFT Records into Bodyline Format using MFTECmd (By ericzimmerman) which is an MFT parser for NTFS file systems.

Step 2: Using the Mactime tool we can convert bodyfile Format into Human readable format and which can be easily analyzed by the Forensic Investigator. (mactime creates an ASCII timeline of file activity based on the output of the fls/MFTECmd tool)

Step 3: Finally using Timeline Explorer we parse the output file created by Mactime Tool



Timestamp	macb	File Name
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/sinaloacartel.jpg
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/sinaloacartel.jpg:Zone.Identifier
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/image3.jpg
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/image3.jpg:Zone.Identifier
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/morphine.jpg
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/morphine.jpg:Zone.Identifier
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/cocaine.jpg
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/cocaine.jpg:Zone.Identifier
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/kush-thc-cart.jpg
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/kush-thc-cart.jpg:Zone.Identifier
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/120.jpg
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/120.jpg:Zone.Identifier
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/71.jpg
2022-01-11 10:04:01	.a..	c:/Users/starwhat luffy/Documents/71.jpg:Zone.Identifier
2022-01-11 10:04:03	macb	c:/Users/starwhat luffy/AppData/Roaming/Microsoft/Windows/Recent/SDelete.lnk
2022-01-11 10:04:03	macb	c:/Users/starwhat luffy/AppData/Roaming/Microsoft/Windows/Recent/SDelete.lnk ($FILE_NAME)
2022-01-11 10:04:21	macb	c:/Windows/prefetch/SDELETE64.EXE-F754834A.pf
2022-01-11 10:04:21	macb	c:/Windows/prefetch/SDELETE64.EXE-F754834A.pf ($FILE_NAME)
2022-01-11 10:04:34	...b	c:/Windows/prefetch/SDELETE.EXE-FDA5B8E8.pf
2022-01-11 10:04:34	macb	c:/Windows/prefetch/SDELETE.EXE-FDA5B8E8.pf ($FILE_NAME)
2022-01-11 10:52:39	mac.	c:/Windows/prefetch/SDELETE.EXE-FDA5B8E8.pf
2022-01-11 20:31:39	mac.	c:/PathUnknown/Directory with ID 0x0000059B-00000001/Luffy/Desktop/Tor Browser/Browser/TorBrowser/Data (deleted)
2022-01-11 20:31:39	mac.	c:/PathUnknown/Directory with ID 0x0000059B-00000001/Luffy/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser (deleted)
2022-01-11 20:31:39	mac.	c:/PathUnknown/Directory with ID 0x0000059B-00000001/Luffy/Desktop/Tor Browser/Browser/TorBrowser/Data/Browser/profile.default

Figure 32: MFT Analysis via Timeline Explorer

USNJRNL Timeline

We have parsed USNJRNL using MFTCMD Tool and analyzed it via Timeline Explorer. As USNJRNL records all the activities of every individual file (CREATE, DELETE, RENAME etc.,) with Update reason codes so we have filtered our output in timeline explorer to remove repeated Names.

Update Timestamp	Name	Exte…	Paren…	Entr…	Update Reasons
2022-01-11 08:25:59	torbrowser-install-win64-11.0.3_en-US.exe	.exe	3534	2746	NamedDataExtend|RenameNewNan
2022-01-11 08:26:09	TORBROWSER-INSTALL-WIN64-11.0-723F3D68.pf	.pf	212098	10122	DataExtend|DataTruncation|Cl
2022-01-11 08:26:20	tor.exe	.exe	10204	10213	DataExtend|FileCreate|Basicl
2022-01-11 08:26:56	FIREFOX.EXE-FA36C190.pf	.pf	212098	10267	FileCreate
2022-01-11 08:27:07	TOR.EXE-9CEDC248.pf	.pf	212098	10345	FileCreate
2022-01-11 09:47:04	sinaloacartel.jpg	.jpg	3535	10502	FileCreate|FileDelete|Close
2022-01-11 09:47:09	image3.jpg	.jpg	3535	10526	NamedDataExtend|StreamChange
2022-01-11 09:48:39	morphine.jpg	.jpg	3535	10528	NamedDataExtend|StreamChange
2022-01-11 09:48:52	kush-thc-cart.jpg	.jpg	3535	10530	FileCreate
2022-01-11 09:49:03	cocaine.jpg	.jpg	3535	10529	FileCreate
2022-01-11 09:49:14	71.jpg	.jpg	3535	10532	FileCreate
2022-01-11 09:49:22	120.jpg	.jpg	3535	10531	FileCreate
2022-01-11 09:56:46	36064255_1563389080436628_4100650344030142464_n.jpg	.jpg	3535	10337	FileCreate
2022-01-11 09:58:46	243288577_10158343753721845_3525808625595709278_n.j…	.jpg	3535	10540	FileCreate
2022-01-11 09:58:51	107275763_10157391859541845_7489731999617748488_n.j…	.jpg	3535	10541	FileCreate
2022-01-11 09:59:27	120.jpg	.jpg	3535	10531	ObjectIdChange
2022-01-11 09:59:28	36064255_1563389080436628_4100650344030142464_n.jpg	.jpg	3535	10337	ObjectIdChange
2022-01-11 09:59:28	107275763_10157391859541845_7489731999617748488_n.j…	.jpg	3535	10541	ObjectIdChange
2022-01-11 09:59:28	71.jpg	.jpg	3535	10532	ObjectIdChange
2022-01-11 09:59:28	243288577_10158343753721845_3525808625595709278_n.j…	.jpg	3535	10540	ObjectIdChange|Close
2022-01-11 09:59:28	cocaine.jpg	.jpg	3535	10529	ObjectIdChange
2022-01-11 09:59:28	image3.jpg	.jpg	3535	10526	ObjectIdChange

Figure 33: USNJRNL Output 1

Update Timestamp	Name	Exte…	Paren…	Entr…	Update Reasons
2022-01-11 09:59:28	image3.jpg	.jpg	3535	10526	ObjectIdChange
2022-01-11 09:59:28	kush-thc-cart.jpg	.jpg	3535	10530	ObjectIdChange
2022-01-11 09:59:28	morphine.jpg	.jpg	3535	10528	ObjectIdChange
2022-01-11 09:59:28	sinaloacartel.jpg	.jpg	3535	10502	ObjectIdChange
2022-01-11 09:59:44	36064255_1563389080436628_4100650344030142464_n.jpg	.jpg	3535	10337	ObjectIdChange|Close
2022-01-11 09:59:49	FIREFOX.EXE-FA36C190.pf	.pf	212098	10267	DataTruncation
2022-01-11 09:59:58	TOR.EXE-9CEDC248.pf	.pf	212098	10345	DataTruncation
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	10294	FileCreate
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10551	FileCreate
2022-01-11 10:01:25	EMAIL and PASSWORD.txt	.txt	3535	2762	RenameOldName
2022-01-11 10:01:25	EMAIL and PASSWORD.txt	.txt	224014	2762	RenameNewName
2022-01-11 10:01:25	addins		1377	2240…	ObjectIdChange
2022-01-11 10:01:27	addins		1377	2240…	ObjectIdChange|Close
2022-01-11 10:01:27	Hack password.txt	.txt	3535	10294	RenameOldName
2022-01-11 10:01:27	Hack password.txt	.txt	224014	10294	RenameNewName
2022-01-11 10:01:39	EMAIL and PASSWORD.txt	.txt	224014	2762	RenameOldName
2022-01-11 10:01:39	readme1.txt	.txt	224014	2762	RenameNewName
2022-01-11 10:01:39	readme1.txt	.txt	224014	2762	RenameNewName|Close
2022-01-11 10:01:51	Hack password.txt	.txt	224014	10294	RenameOldName
2022-01-11 10:01:51	readme2.txt	.txt	224014	10294	RenameNewName
2022-01-11 10:01:51	readme2.txt	.txt	224014	10294	RenameNewName|Close
2022-01-11 10:02:30	FIREFOX.EXE-FA36C190.pf	.pf	212098	10267	DataTruncation

Figure 34: USNJRNL Output 2

Note: We have filtered a lot of Noise from the output to remove unwanted system files.

umn header here to group by that column

Enter text to search... Find

Update Timestamp	Name	Exte…	Paren…	Entr…	Update Reasons
2022-01-11 10:02:30	FIREFOX.EXE-FA36C190.pf	.pf	212098	10267	DataTruncation
2022-01-11 10:02:39	TOR.EXE-9CEDC248.pf	.pf	212098	10345	DataTruncation
2022-01-11 10:03:58	SDelete.zip	.zip	3535	10459	FileCreate
2022-01-11 10:04:03	SDelete.lnk	.lnk	3550	10632	FileCreate
2022-01-11 10:04:16	SDelete		3535	5139	FileCreate
2022-01-11 10:04:16	SDelete		3535	5139	FileCreate|Close
2022-01-11 10:04:16	sdelete.exe	.exe	5139	10348	FileCreate
2022-01-11 10:04:16	sdelete64.exe	.exe	5139	10551	FileCreate
2022-01-11 10:04:21	SDELETE64.EXE-F754834A.pf	.pf	212098	10644	FileCreate
2022-01-11 10:04:34	SDELETE.EXE-FDA5B8E8.pf	.pf	212098	10645	FileCreate
2022-01-11 10:49:44	CMD.EXE-0BD30981.pf	.pf	212098	10648	DataTruncation
2022-01-11 10:52:39	TorAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA…	.AAA	3536	10224	RenameNewName
2022-01-11 10:52:39	TorAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA…	.AAA	3536	10224	RenameNewName|Close
2022-01-11 10:52:39	TorAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA…	.AAA	3536	10224	RenameOldName
2022-01-11 10:52:39	TorBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB…	.BBB	3536	10224	RenameNewName
2022-01-11 10:52:39	TorBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB…	.BBB	3536	10224	RenameNewName|Close
2022-01-11 10:52:39	TorBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB…	.BBB	3536	10224	RenameOldName
2022-01-11 10:52:39	TorCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC…	.CCC	3536	10224	RenameNewName
2022-01-11 10:52:39	TorCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC…	.CCC	3536	10224	RenameNewName|Close
2022-01-11 10:52:39	TorCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC…	.CCC	3536	10224	RenameOldName
2022-01-11 10:52:39	TorDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD…	.DDD	3536	10224	RenameNewName
2022-01-11 10:52:39	TorDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD…	.DDD	3536	10224	RenameNewName|Close

Figure 35: USNJRNL Output 3

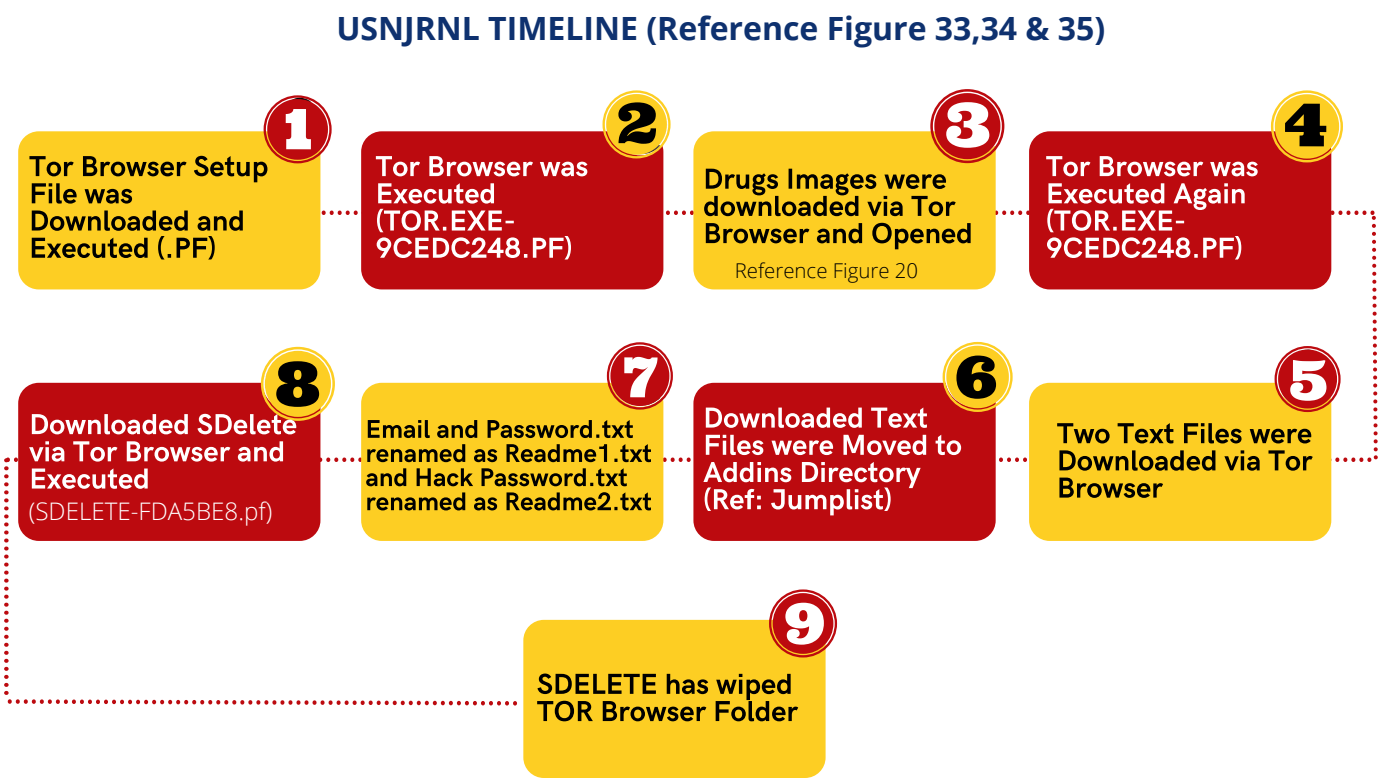


Figure 36: USNJRNL Timeline

We can conclude from the above timeline of the USNJRNL, our Artifacts Design Consideration Figure No 1 Matches with our USNJRNL Timeline.

USNJRNL Move and Rename Timeline Activity

We can refer to below the figure for the complete process of Move and rename Process of the files where update reason codes are displayed by the tool.

Update Timestamp	Name	Extension	Paren…	Entr…	Update Reasons
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	10294	FileCreate|FileDelete|Close
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	10294	FileCreate
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	10294	FileCreate|Close
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	10294	FileDelete|Close
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	2762	RenameNewName
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	2762	RenameNewName|Close
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	2762	SecurityChange
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	2762	SecurityChange|Close
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	2762	StreamChange
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	2762	NamedDataExtend|StreamChange
2022-01-11 10:00:33	EMAIL and PASSWORD.txt	.txt	3535	2762	NamedDataExtend|StreamChange|Close
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10551	FileCreate
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10551	FileCreate|FileDelete|Close
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10551	FileCreate
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10551	FileCreate|Close
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10551	FileDelete|Close
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10294	RenameNewName
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10294	RenameNewName|Close
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10294	SecurityChange
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10294	SecurityChange|Close
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10294	StreamChange
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10294	NamedDataExtend|StreamChange

Figure 37: USNJRNL Output 1 (Move and Rename Timeline)

Update Timestamp	Name	Exte…	Parent En…	Entry Nu…	Update Reasons
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10294	StreamChange
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10294	NamedDataExtend|StreamChange
2022-01-11 10:00:49	Hack password.txt	.txt	3535	10294	NamedDataExtend|StreamChange|Close
2022-01-11 10:01:25	EMAIL and PASSWORD.txt	.txt	3535	2762	RenameOldName
2022-01-11 10:01:25	EMAIL and PASSWORD.txt	.txt	224014	2762	RenameNewName
2022-01-11 10:01:25	EMAIL and PASSWORD.txt	.txt	224014	2762	RenameNewName|Close
2022-01-11 10:01:25	EMAIL and PASSWORD.txt	.txt	224014	2762	SecurityChange
2022-01-11 10:01:25	EMAIL and PASSWORD.txt	.txt	224014	2762	SecurityChange|Close
2022-01-11 10:01:25	addins		1377	224014	ObjectIdChange
2022-01-11 10:01:27	addins		1377	224014	ObjectIdChange|Close
2022-01-11 10:01:27	Hack password.txt	.txt	3535	10294	RenameOldName
2022-01-11 10:01:27	Hack password.txt	.txt	224014	10294	RenameNewName
2022-01-11 10:01:27	Hack password.txt	.txt	224014	10294	RenameNewName|Close
2022-01-11 10:01:27	Hack password.txt	.txt	224014	10294	SecurityChange
2022-01-11 10:01:27	Hack password.txt	.txt	224014	10294	SecurityChange|Close
2022-01-11 10:01:39	EMAIL and PASSWORD.txt	.txt	224014	2762	RenameOldName
2022-01-11 10:01:39	readme1.txt	.txt	224014	2762	RenameNewName
2022-01-11 10:01:39	readme1.txt	.txt	224014	2762	RenameNewName|Close
2022-01-11 10:01:51	Hack password.txt	.txt	224014	10294	RenameOldName
2022-01-11 10:01:51	readme2.txt	.txt	224014	10294	RenameNewName
2022-01-11 10:01:51	readme2.txt	.txt	224014	10294	RenameNewName|Close

Figure 38: USNJRNL Output 2 (Move and Rename Timeline)

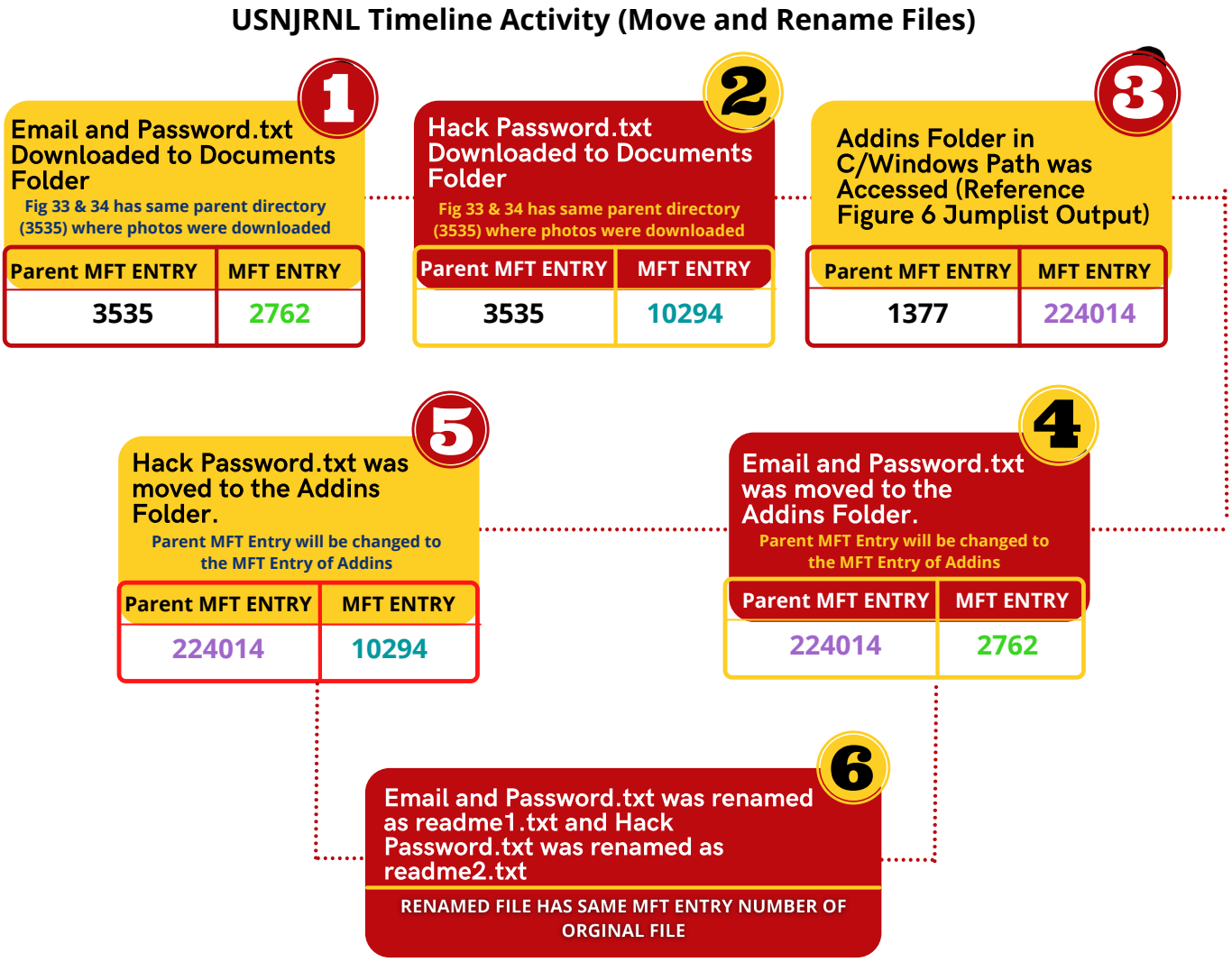


Figure 39: USNJRNL Move and Rename Timeline

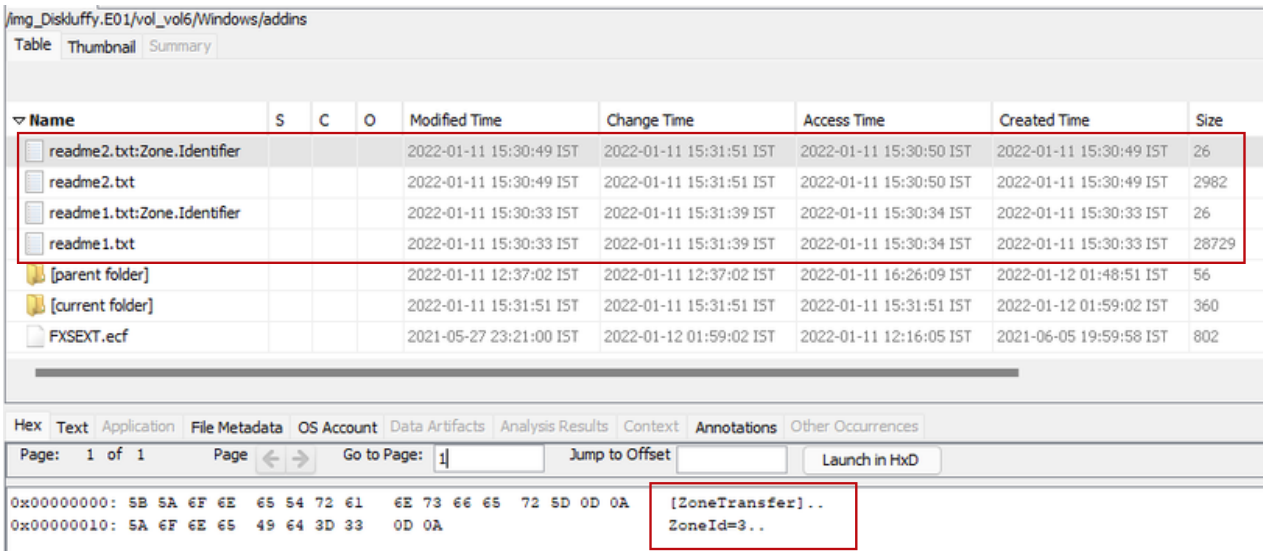


Figure 40: Autopsy Filesystem output

We observe in figure 40, renamed files readme1.txt and rename2.txt still have zone ID ADS tagged even after the file is moved from documents to Windows\Addins directory and renamed.

Scenario 2: Tor execution from the USB

In scenario 2, Tor Browser has been executed directly from the USB and the Disk Forensic analysis process will be carried out only on the system disk, not the Pendrive.

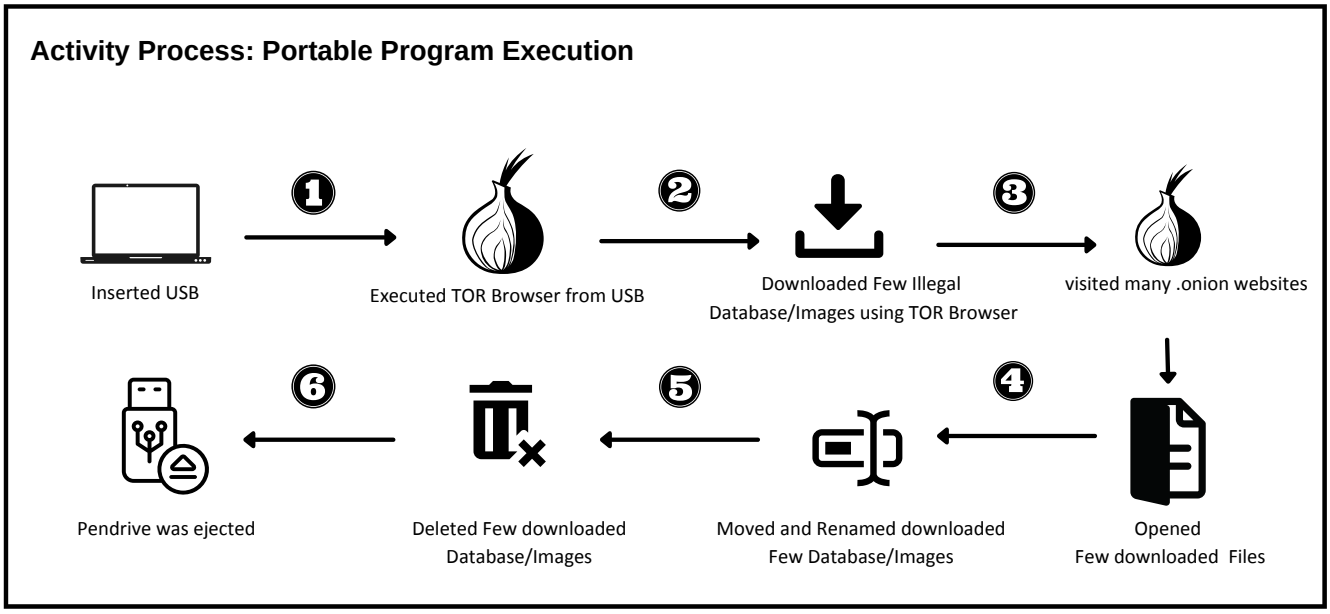


Figure 41: Scenario2 - Running Tor Browser from USB

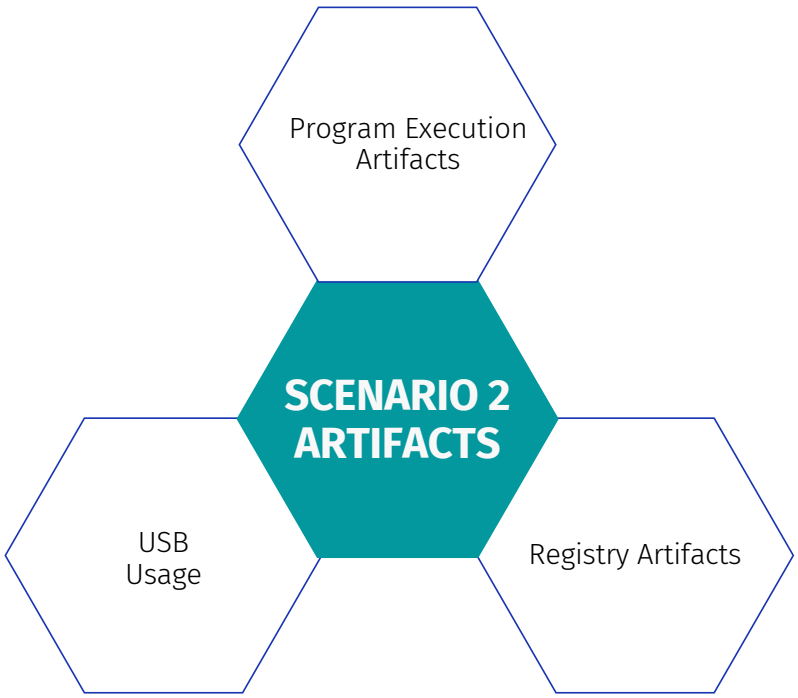


Figure 42: Scenario2 - Artifacts

Program Execution Artifacts

a. Jumplist

Default Location of the Artifacts:
\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent

Tool Used: JLECmd version 1.5.0.0 & Jumplist Explorer

Result: We observe in the output of the jumplist few drug images and files were directly opened in the USB Drive (E:\).

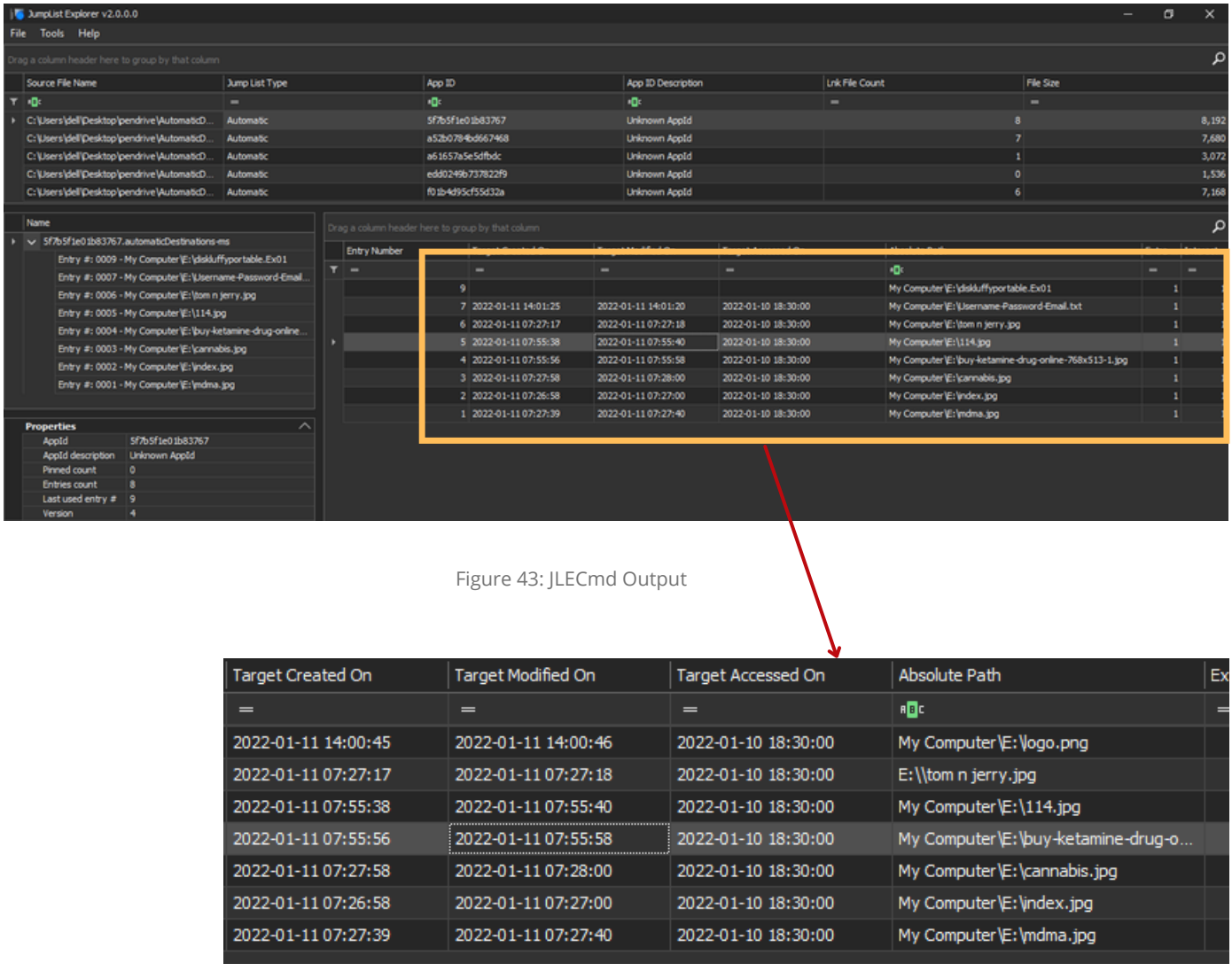


Figure 43: JLECmd Output

Target Created On	Target Modified On	Target Accessed On	Absolute Path	Ex
2022-01-11 14:00:45	2022-01-11 14:00:46	2022-01-10 18:30:00	My Computer\E:\logo.png	
2022-01-11 07:27:17	2022-01-11 07:27:18	2022-01-10 18:30:00	E:\\tom n jerry.jpg	
2022-01-11 07:55:38	2022-01-11 07:55:40	2022-01-10 18:30:00	My Computer\E:\114.jpg	
2022-01-11 07:55:56	2022-01-11 07:55:58	2022-01-10 18:30:00	My Computer\E:\buy-ketamine-drug-o...	
2022-01-11 07:27:58	2022-01-11 07:28:00	2022-01-10 18:30:00	My Computer\E:\cannabis.jpg	
2022-01-11 07:26:58	2022-01-11 07:27:00	2022-01-10 18:30:00	My Computer\E:\index.jpg	
2022-01-11 07:27:39	2022-01-11 07:27:40	2022-01-10 18:30:00	My Computer\E:\mdma.jpg	

b. Prefetch:

Prefetch File Location: *C:\Windows\Prefetch*

Tool Used: PECmd version 1.5.0.0 by Eric Zimmerman

Prefetch FileName: TOR.EXE-84EE9546.pf

```
Created on: 2022-01-11 07:24:05
Modified on: 2022-01-11 07:24:45
Last accessed on: 2022-01-11 07:24:45

Executable name: TOR.EXE
Hash: 84EE9546
File size (bytes): 78,858
Version: Windows 10 or Windows 11

Run count: 3
Last run: 2022-01-11 07:24:35
Other run times: 2022-01-11 07:24:06, 2022-01-11 07:23:59

Volume information:

#0: Name: \VOLUME{0000000000000000-5a27fd77} Serial: 5A27FD77 Created: 1601-01-01 00:00:00 Directories: 6 File references: 26
#1: Name: \VOLUME{01d7f48026d4004b-7226ec21} Serial: 7226EC21 Created: 2021-12-19 02:28:47 Directories: 6 File references: 42

Directories referenced: 12

00: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER
01: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER\BROWSER
02: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER\BROWSER\TORBROWSER
03: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER\BROWSER\TORBROWSER\DATA
04: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER\BROWSER\TORBROWSER\DATA\TOR
05: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER\BROWSER\TORBROWSER\TOR
06: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS
07: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\APPPATCH
08: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\GLOBALIZATION
09: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\GLOBALIZATION\SORTING
10: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32
11: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\EN-US

Files referenced: 56

00: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\C_1252.NLS
02: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\C_437.NLS
03: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\L_INTL.NLS
04: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER\BROWSER\TORBROWSER\TOR\TOR.EXE (Executable: True)
05: \VOLUME{01d7f48026d4004b-7226ec21}\WINDOWS\SYSTEM32\KERNEL32.DLL
```

Figure 44: Prefetch Output

Filtered Output of the Figure

Created on: 2022-01-11 07:24:05
Modified on: 2022-01-11 07:24:45
Last accessed on: 2022-01-11 07:24:45

Executable name: TOR.EXE
Hash: 84EE9546
File size (bytes): 78,858
Version: Windows 10 or Windows 11

Run count: 3
Last run: 2022-01-11 07:24:35
Other run times: 2022-01-11 07:24:06, 2022-01-11 07:23:59

Volume information:

#0: Name: \VOLUME{0000000000000000-5a27fd77} Serial: 5A27FD77 Created: 1601-01-01 00:00:00
Directories: 6 File references: 26
#1: Name: \VOLUME{01d7f48026d4004b-7226ec21} Serial: 7226EC21 Created: 2021-12-19 02:28:47
Directories: 6 File references: 42

Directories referenced: 12

00: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER
01: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER\BROWSER
02: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER\BROWSER\TORBROWSER

Files referenced: 56

04: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER\BROWSER\TORBROWSER\TOR\TOR.EXE (Executable: True)
26: \VOLUME{0000000000000000-5a27fd77}\TOR BROWSER\BROWSER\TORBROWSER\TOR\LIBCRYPTO-1_1-X64.DLL

Figure 45: Prefetch Filtered Output

Results:

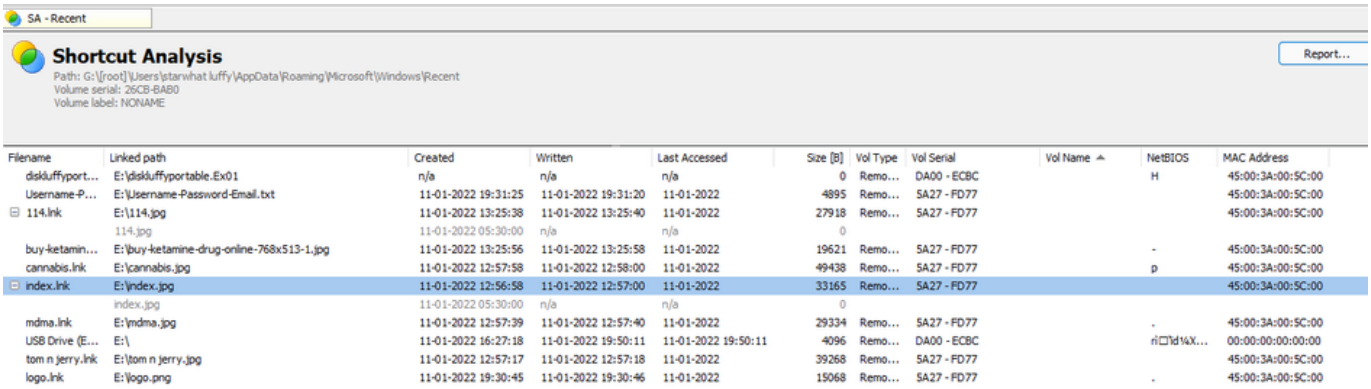
We can find files opened by the application within 10 seconds of its execution which includes the full path of executable and also extracts volume information, directory and files referenced, Last run times. We can observe TOR.exe was executed directly from an external USB Drive

Full Path of the Tor: \TOR BROWSER\BROWSER\TORBROWSER\TOR\TOR.EXE

Disk Volume ID: 5A27FD77 (USB) | **Number of TOR executed**: 3

First Time Program Executed: 2022-01-11 07:23:59 **Last Run:** 2022-01-11 07:24:35

Mapping of Volume Serial Number



Filename	Linked path	Created	Written	Last Accessed	Size [B]	Vol Type	Vol Serial	Vol Name	NetBIOS	MAC Address
diskluffyport...	E:\diskluffyportable.Ex01	n/a	n/a	n/a	0	Remo...	DA00 - ECBC		H	45:00:3A:00:5C:00
Username-P...	E:\Username-Password-Email.txt	11-01-2022 19:31:25	11-01-2022 19:31:20	11-01-2022	4895	Remo...	5A27 - FD77			45:00:3A:00:5C:00
114.lnk	E:\114.jpg	11-01-2022 13:25:38	11-01-2022 13:25:40	11-01-2022	27918	Remo...	5A27 - FD77			45:00:3A:00:5C:00
	114.jpg	11-01-2022 05:30:00	n/a	n/a	0					
buy-ketamin...	E:\buy-ketamine-drug-online-768x513-1.jpg	11-01-2022 13:25:56	11-01-2022 13:25:58	11-01-2022	19621	Remo...	5A27 - FD77		-	45:00:3A:00:5C:00
cannabis.lnk	E:\cannabis.jpg	11-01-2022 12:57:58	11-01-2022 12:58:00	11-01-2022	49438	Remo...	5A27 - FD77		p	45:00:3A:00:5C:00
index.lnk	E:\index.jpg	11-01-2022 12:56:58	11-01-2022 12:57:00	11-01-2022	33165	Remo...	5A27 - FD77			45:00:3A:00:5C:00
	index.jpg	11-01-2022 05:30:00	n/a	n/a	0					
mdma.lnk	E:\mdma.jpg	11-01-2022 12:57:39	11-01-2022 12:57:40	11-01-2022	29334	Remo...	5A27 - FD77		.	45:00:3A:00:5C:00
USB Drive (E...	E:\	11-01-2022 16:27:18	11-01-2022 19:50:11	11-01-2022 19:50:11	4096	Remo...	DA00 - ECBC		ri□'ld¼X...	00:00:00:00:00:00
tom n jerry.lnk	E:\tom n jerry.jpg	11-01-2022 12:57:17	11-01-2022 12:57:18	11-01-2022	39268	Remo...	5A27 - FD77			45:00:3A:00:5C:00
logo.lnk	E:\logo.png	11-01-2022 19:30:45	11-01-2022 19:30:46	11-01-2022	15068	Remo...	5A27 - FD77		.	45:00:3A:00:5C:00

Figure 46: Shortcut Analysis Output

Shortcut FIles

Shortcut Files automatically created by Windows Recent Items and opening local, external and remote data files and documents will generate a shortcut file (.lnk)

Location: C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\

Tools used: Windows File Analyzer

LNK File Information Fetched by the Tool:

- Modified, Access, and Creation times of the target file
- Volume Information (Name, Drive Letter, Type, Serial Number)
- Network Share information
- File Name and Size
- Original Location
- Name of System

In the above figure, we observe from the .lnk analysis results, volume serial number 5A27FD77 which is fetched by the prefetchparser tool in figure 45, are mapped with drive letter E in the .lnk analysis figure 46 and multiple files are opened from the external USB.

Amcache:

Tool Used: AmcacheParser 1.5.1.0 and Timeline Explorer

Location: C:\Windows\AppCompat\Programs\Amcache

	Is Os Component	Full Path
8f59b00baf644bfa9891662689a19	True	c:\windows\system32\mdmdiagnosticstool.exe
659ce7bd7891e5345217e0e0bba46	False	c:\program files (x86)\microsoft\edgeupdate\microsoftedgeupdate.exe
8efb9d1fd10e57500c3e52a56efe3	True	c:\windows\uus\amd64\mousocoreworker.exe
3ca175fb5a31ffefd384e4793ee76	True	c:\program files\windows defender\mpcmdrun.exe
09a131bc55c755bb7f85c0f0049a3	True	c:\program files\windows defender\msmpeng.exe
9ccd338c17130a3c4941471c3aa66	True	c:\windows\system32\oobe\msoobe.exe
d3788b6b66276de5206996c2187e4	True	c:\windows\microsoft.net\framework\v4.0.30319\ngen.exe
c8cb599ab8ff643f4d1765e111c2b	True	c:\windows\microsoft.net\framework64\v4.0.30319\ngen.exe
7ba51971b7b7094f0eed281b29223	False	c:\program files\windowsapps\microsoft.windowsnotepad_10.2102.13.0_x64__8wekyb3c
3435dfc8c2c631d17d3140493d1f3	False	c:\users\starwhat luffy\appdata\local\microsoft\onedrive\onedrive.exe
b5716ade6b895127d561299e7cafe	False	c:\users\starwhat luffy\appdata\local\microsoft\onedrive\update\onedrivesetup.ex
4b54516845d7c9927e09e63c30f47	True	c:\windows\syswow64\onedrivesetup.exe
5c8a8714f3ae259db8150ce6ab10c	True	c:\windows\system32\oobe\oobeldr.exe
55ca4ba19981404a6aa27418139e2	True	c:\windows\system32\relpost.exe
94ee508e42ede3010819134974375	True	c:\windows\system32\resetengine.exe
253b9e24eee4766553e26bf40a8fe	True	c:\windows\system32\searchindexer.exe
a129d68ce6b5ed1141109686b9a5a	True	c:\windows\system32\securityhealthservice.exe
b3399af6c1d37274bc1dcef94a422	True	c:\windows\system32\services.exe
717711cfd4bfba0e2723e400c2ee0	False	c:\$windows.~bt\sources\setupplatform.exe
70db8227dc50f9a481be466a0609f	True	c:\windows\system32\smss.exe
77b12c9da01a36c43d66557e2b465	True	c:\windows\system32\spoolsv.exe
19fbae200b728435af562d14f703a	True	c:\windows\system32\sppextcomobj.exe

Figure 47: Amcache Analysis Output

In the above output, amcache parser has parsed Application Unassociated Entries which doesn't contain any entries of Tor.exe.

Registry Artifacts

a) LastVisitedPidMRU & OpenSavePidMRU: OpenSavePidMRU registry key tracks files that have been opened or saved from the Windows shell dialog box by the user and LastVisitedPidMRU tracks the specific program used by the user to open the files (which are stored in OpenSavePidMRU).

Registry Location:
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\

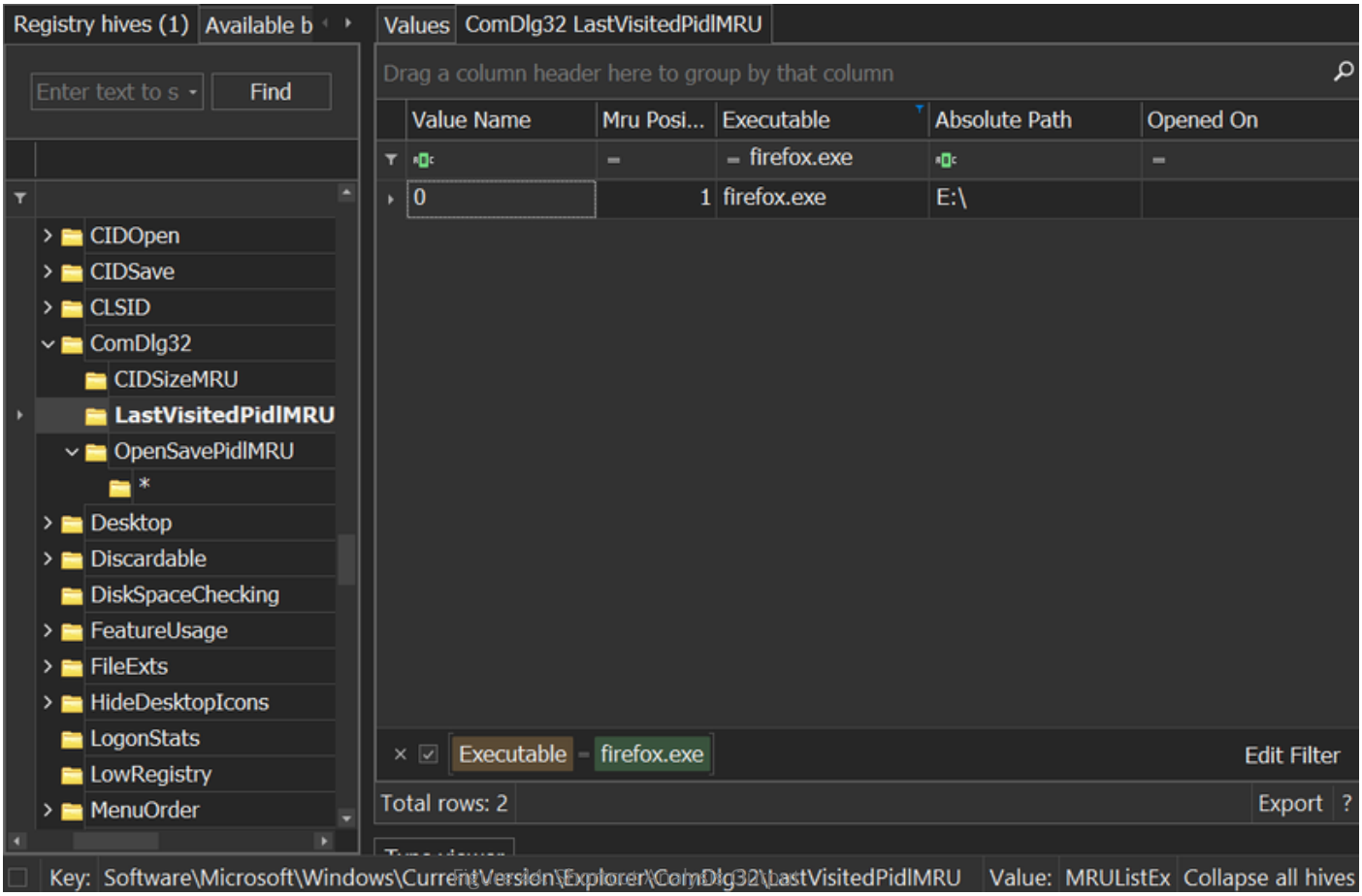


Figure 48: LastVisitedPIDMRU Output

We can observe in the above figure 48, any traces related to the Tor browser are not found in the OpenSavePidMRU registry key, but the execution of the Tor/Firefox is found in LastVisitPidMRU Key.

b) UserAssist: This key contains the execution of the programs in the system, which is yet another location for the forensic examiner. Unlike other artifacts, userAssist will include information on whether the application was run from a shortcut link or directly from the installed location.

Registry location:
NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count

CEBFF6CD: This key in the registry indicates Executable File Execution.

F4E57C4B: This key indicates Shortcut File Execution

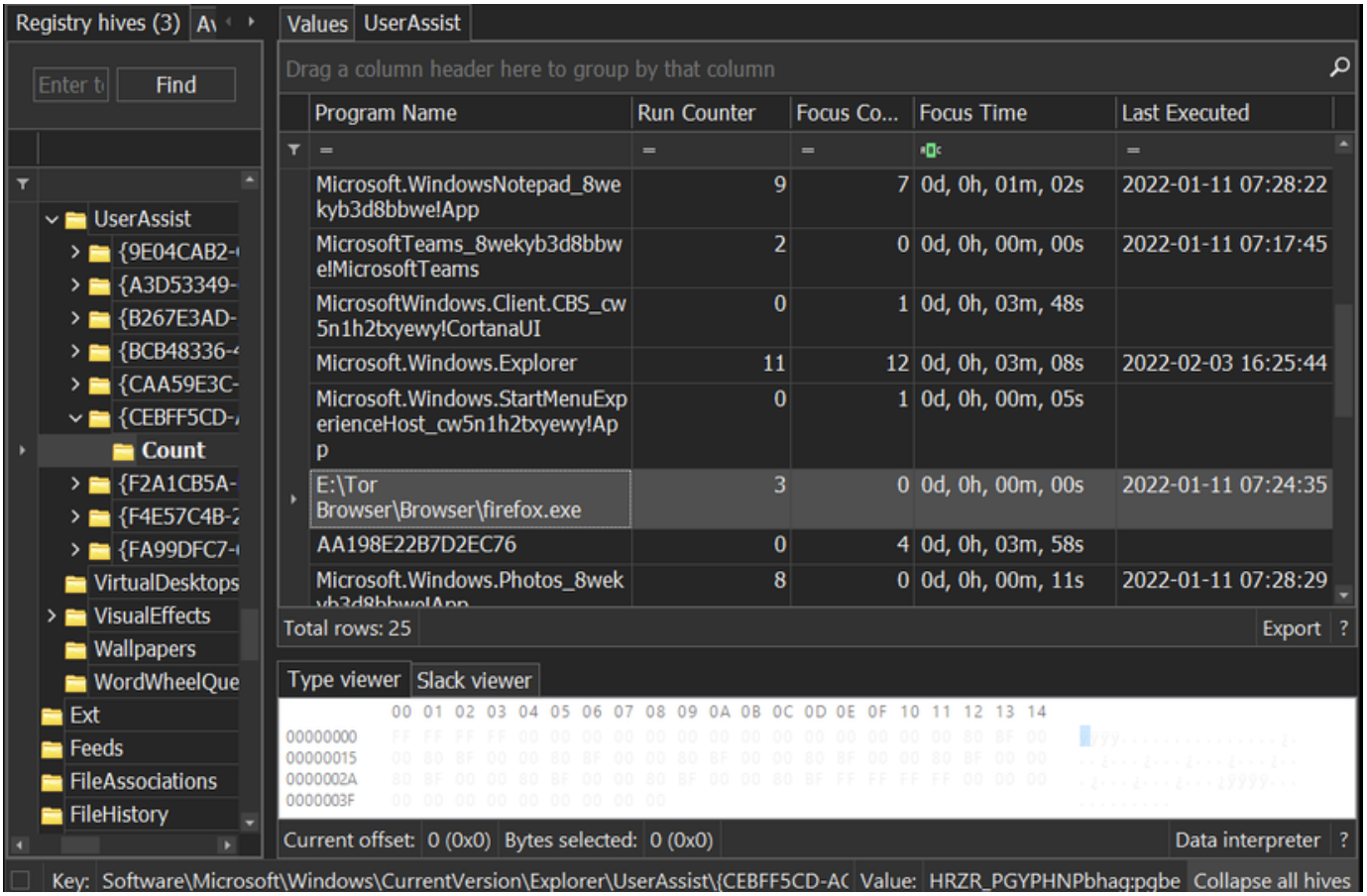


Figure 49: UserAssist Output (Execution from the Installed Location)

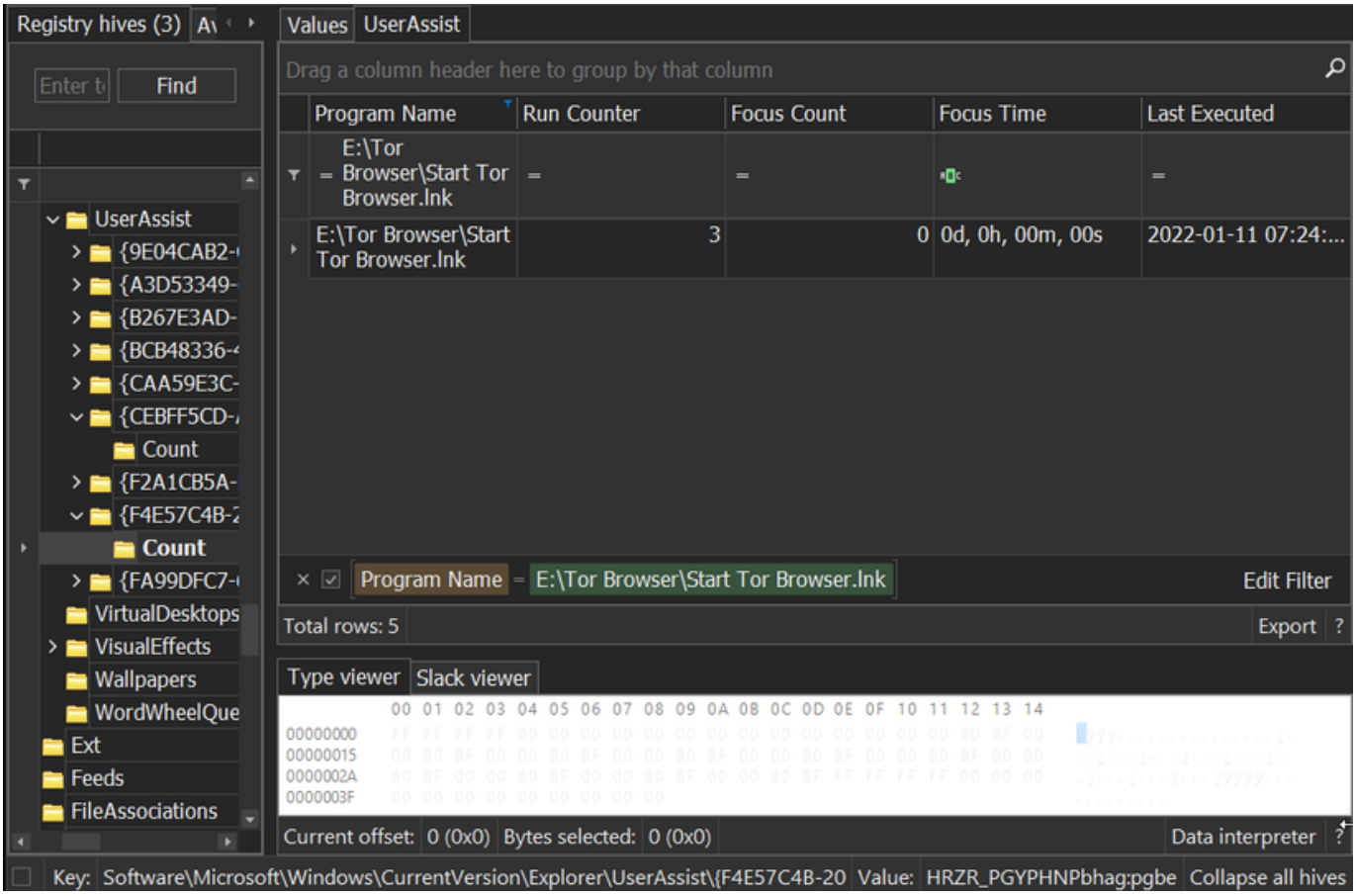


Figure 50: UserAssist Output (Execution from the Installed Location)

As shown in figure 49& 50, we can observe that all the artifacts related to Tor Browser Execution and Tor Installer Program including the program path has been found and also Run Counter indicates the number of times the application was executed and it matches with prefetch artifacts (Reference Figure: 45)

c. RecentDocs: This key will track the last files and folders opened and is used to populate data in the “Recent” menus of the Start menu.

Location:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

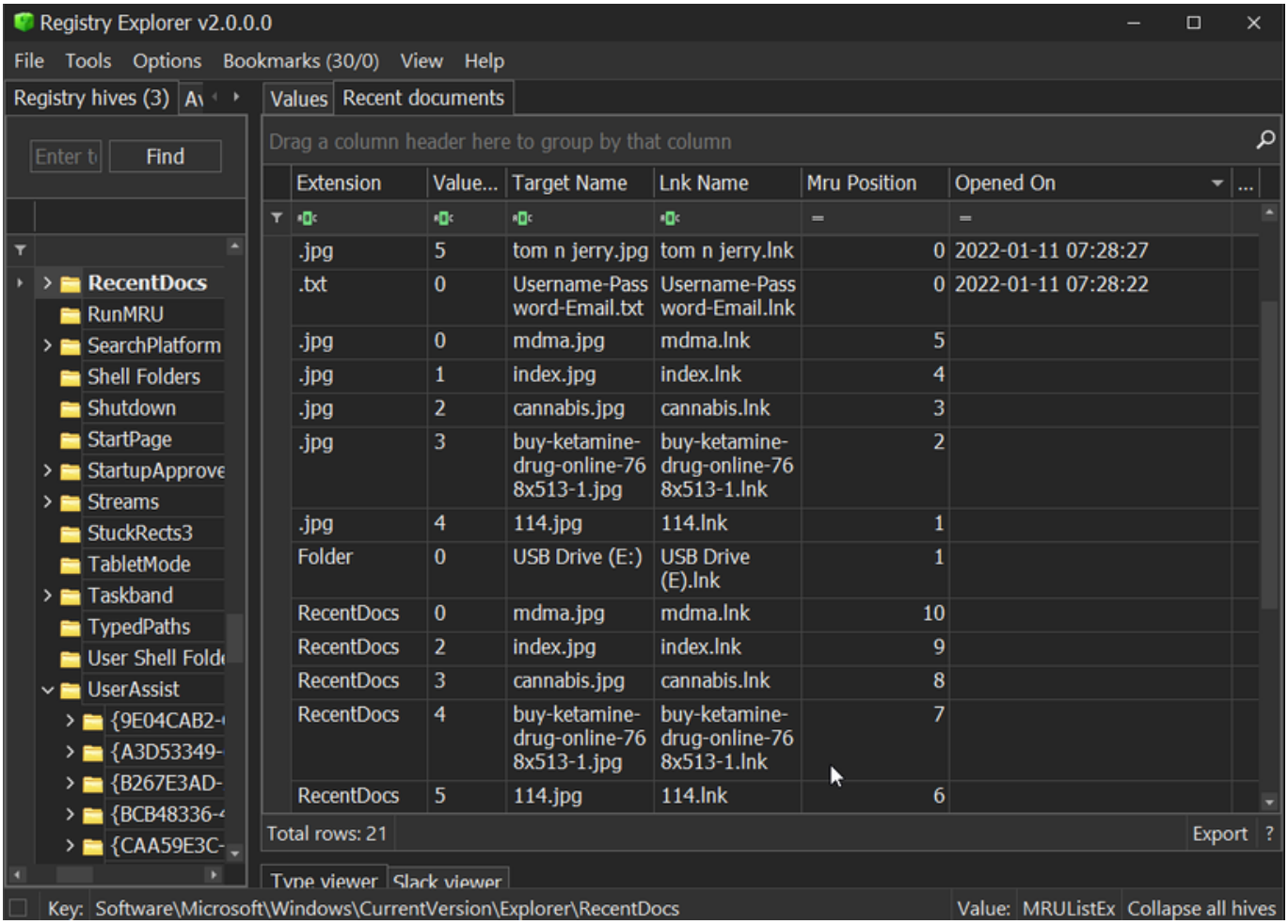


Figure 51: RecentDocs Output

As shown in the figure, we can conclude that many images were downloaded/opened and files were opened via USB.

USB USAGE

USB Key Identification: Track USB devices plugged into a machine and key tracks entries vendor, product, and version of a USB device when plugged into a machine

Location:
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumUSBSTOR

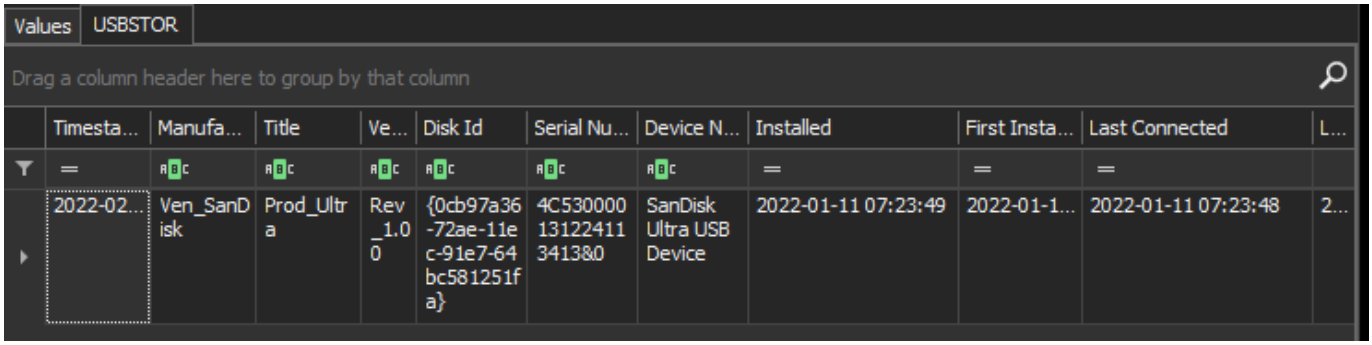


Figure 52: USBSTOR Output

USB Last Connected Time: 2022-01-11 07:23:48 timestamp matches with other artifacts timestamp to co-relate the evidence.

USB Serial Number: 4C530000131224113413 (Sandisk Ultra)

Mounted Devices: Identify the USB device that was last mapped to a specific drive letter.

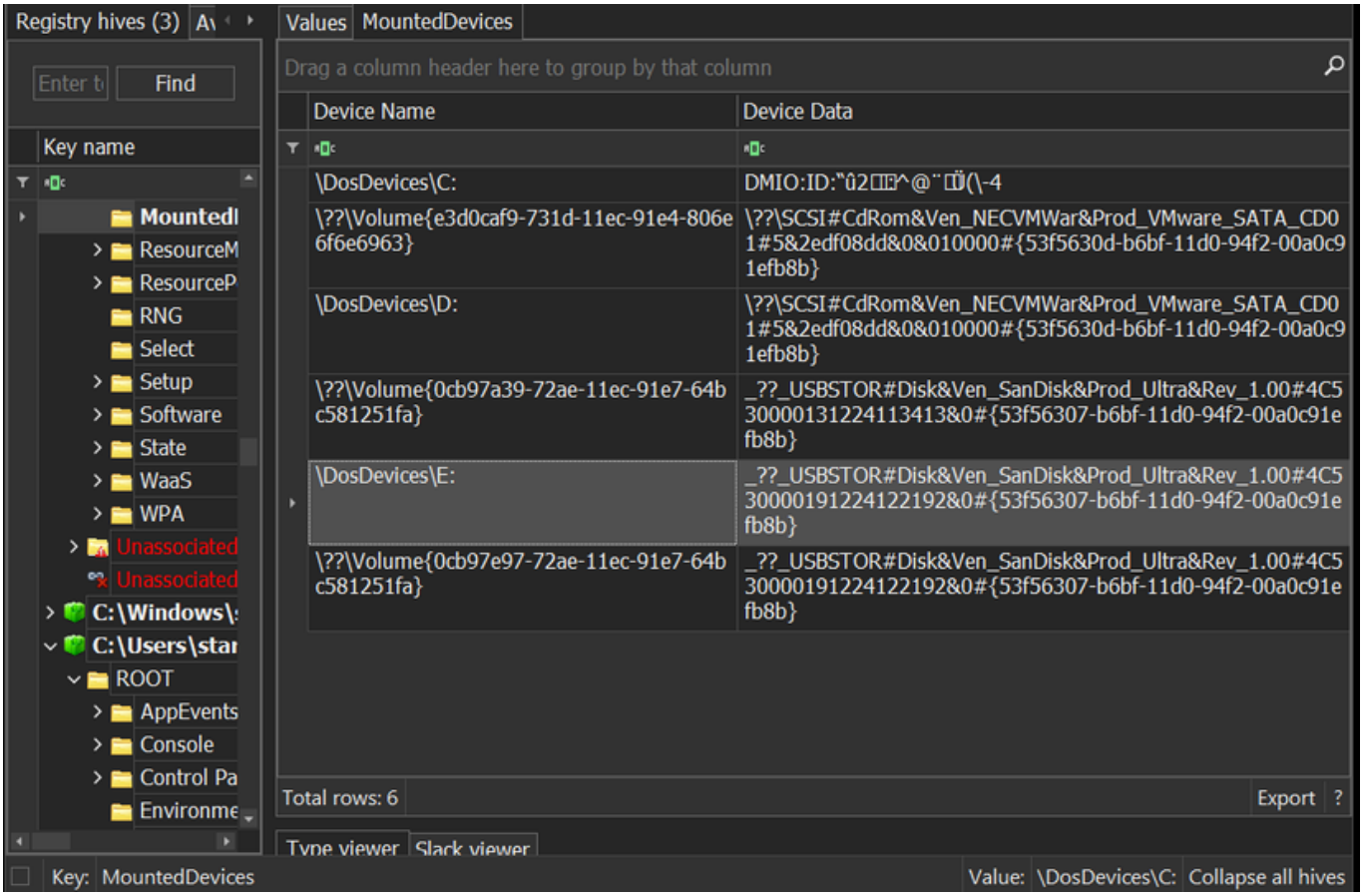


Figure 53: MountedDevices Output

9.2 Memory Forensics

To perform memory forensics, we have used the latest version of SIFT Workstation installed with Volatility Framework 2.6.1 on Windows 11 64-bit Memory Image which was acquired by FTK Imager. As the acquired image has build Number 22000 which is currently supported by the volatility framework with the profile ID "Win10x64_19041".

In our experiment, we might come across two processor namely Tor.exe and Firefox.exe. Here, "Tor.exe" is a socks proxy and firefox.exe talks to that proxy.

Tool Used: Volatility Framework 2.6.1
Device: Dell XPS 15 9500
OS: Windows 11 Home Single Language
Version: 21H2 | 22000.434
System Name: DESKTOP-GT6AAE4
Local Account Administrator Name: Dell
RAM: 32 GB
Hard Disk: 1 TB SSD

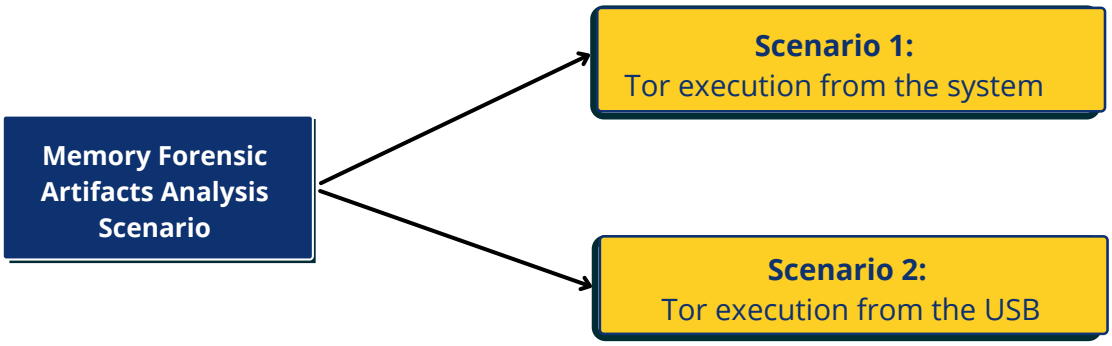


Figure 54: Memory Forensics Analysis Scenario

a) **Kdbgscan**: This is the very first command used as it helps to decrypt KDBG Structure and help to identify the system profile as it determines Operating System and Build Number and is considered a better option than imageinfo plugin for Windows 10/11 OS.

```
**************************************************
Instantiating KDBG using: /cases/memdump.mem WinXPSP2x86 (5.1.0 32bit)
Offset (P)                    : 0x352a0d080
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win10x64_19041
PsActiveProcessHead           : 0x4181bee0
PsLoadedModuleList            : 0x41829750
KernelBase                    : 0xfffff80040c00000
```

Figure 55: KDBG info plugin result

b) PSSCAN: This plugin is used to scan memory for EPROCESS blocks.

We have performed filter option using grep command for psscan command to identify the presence of the tor browser execution in this OS.

Scenario 1: Tor Execution from the Disk.

```
root@siftworkstation:/home/sansforensics/Documents# vol.py -f memdump.mem --profile=Win10x64_19041 psscan | egrep 'firefox.exe | tor.exe | Nam
e'
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                PID   PPID PDB               Time created                   Time exited
0x0000a38471e170c0 tor.exe           21308  19804 0x000000027c656000 2022-01-05 12:14:11 UTC+0000   2022-01-05 12:18:42 UTC+0000
0x0000a38471e1e080 firefox.exe       14432  19804 0x000000015db50000 2022-01-05 12:15:17 UTC+0000   2022-01-05 12:18:42 UTC+0000
0x0000a38477f780c0 firefox.exe       22316  19804 0x0000000263aea000 2022-01-05 12:14:11 UTC+0000   2022-01-05 12:18:42 UTC+0000
0x0000a384785080c0 firefox.exe        9676  19804 0x00000001978eb000 2022-01-05 12:14:11 UTC+0000   2022-01-05 12:18:42 UTC+0000
0x0000a3847861f0c0 firefox.exe       19804  16236 0x0000000422507000 2022-01-05 12:14:10 UTC+0000   2022-01-05 12:18:42 UTC+0000
0x0000a3847863a0c0 firefox.exe       16236  19380 0x0000000432754000 2022-01-05 12:14:10 UTC+0000   2022-01-05 12:14:11 UTC+0000
0x0000a38483ddf0c0 firefox.exe        8436  19804 0x0000000861e4b000 2022-01-05 12:15:32 UTC+0000   2022-01-05 12:18:42 UTC+0000
0x0000a38484cc0140 firefox.exe        7428  19804 0x000000032cd83000 2022-01-05 12:14:12 UTC+0000   2022-01-05 12:18:42 UTC+0000
0x0000a3848b414080 firefox.exe       10032  19804 0x00000002e9f0a000 2022-01-05 12:15:37 UTC+0000   2022-01-05 12:18:42 UTC+0000
0x0000a3848c4a20c0 firefox.exe       14256  19804 0x00000002e8073000 2022-01-05 12:15:33 UTC+0000   2022-01-05 12:18:42 UTC+0000
0x0000a3848e1d9080 firefox.exe       12076  19804 0x000000023cc4e000 2022-01-05 12:15:35 UTC+0000   2022-01-05 12:18:42 UTC+0000
0x0000a3848f66d080 firefox.exe       14564  19804 0x00000002d6ee2000 2022-01-05 12:15:38 UTC+0000   2022-01-05 12:18:42 UTC+0000
0x0000a3848f9af140 firefox.exe       17104  19804 0x000000041a7c3000 2022-01-05 12:14:12 UTC+0000   2022-01-05 12:18:42 UTC+0000
root@siftworkstation:/home/sansforensics/Documents#
```

Figure 56: PSSCAN output (Scenario 1)

Scenario 2: Tor Execution from the USB.

```
root@siftworkstation:/home/sansforensics/Desktop/cases# vol.py -f memdump.mem --profile=Win10x64_19041 psscan | egrep 'firefox.exe | t
or.exe | Name'
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                PID   PPID PDB               Time created                   Time exited
0x0000ca88c5f26140 firefox.exe       10252  18772 0x000000026338f000 2022-01-05 07:29:14 UTC+0000   2022-01-05 07:34:45 UTC+0000
0x0000ca88d7ee70c0 firefox.exe       15800  18772 0x0000000347fbd000 2022-01-05 07:31:31 UTC+0000   2022-01-05 07:34:45 UTC+0000
0x0000ca88d944e080 firefox.exe       18772  18744 0x000000043297c000 2022-01-05 07:29:09 UTC+0000   2022-01-05 07:34:45 UTC+0000
0x0000ca88da02e080 firefox.exe       18308  18772 0x000000042ec87000 2022-01-05 07:29:11 UTC+0000   2022-01-05 07:34:45 UTC+0000
0x0000ca88da3e70c0 firefox.exe        3112  18772 0x0000000401ce9000 2022-01-05 07:30:42 UTC+0000   2022-01-05 07:34:45 UTC+0000
0x0000ca88da883080 tor.exe           22720  18772 0x000000032e3a0000 2022-01-05 07:29:12 UTC+0000   2022-01-05 07:34:45 UTC+0000
0x0000ca88dbc6f0c0 firefox.exe       19356  18772 0x000000080fa25000 2022-01-05 07:33:57 UTC+0000   2022-01-05 07:34:45 UTC+0000
0x0000ca88dc887200 firefox.exe       19964  18772 0x000000029606e000 2022-01-05 07:29:13 UTC+0000   2022-01-05 07:34:45 UTC+0000
0x0000ca88dd9f2080 firefox.exe       18744  10476 0x00000007fcbd6000 2022-01-05 07:29:09 UTC+0000   2022-01-05 07:29:12 UTC+0000
0x0000ca88dda600c0 firefox.exe       15860  18772 0x00000007d7ea2000 2022-01-05 07:33:19 UTC+0000   2022-01-05 07:34:45 UTC+0000
0x0000ca88ddab9140 firefox.exe       21080  18772 0x000000026ab02000 2022-01-05 07:29:15 UTC+0000   2022-01-05 07:34:45 UTC+0000
0x0000ca88de1670c0 firefox.exe        1836  18772 0x000000034ebbb000 2022-01-05 07:33:54 UTC+0000   2022-01-05 07:34:45 UTC+0000
0x0000ca88de4ad140 firefox.exe       10152  18772 0x000000032df79000 2022-01-05 07:30:08 UTC+0000   2022-01-05 07:34:45 UTC+0000
root@siftworkstation:/home/sansforensics/Desktop/cases#
```

Figure 57: PSSCAN output (Scenario 2)

In both scenarios, the PSSCAN plugin has displayed the Tor.exe/Firefox.exe Program including Process ID, Parent Process ID, Offset and Timestamp.

c): DLLList: This plugin prints dll list associated with the program.

Scenario 1: Tor Execution from the Disk

```
root@siftworkstation:/home/sansforensics/Documents# vol.py -f memdump.mem --profile=Win10
x64_19041 dlllist -p 21308
Volatility Foundation Volatility Framework 2.6.1
**************************************************************************
tor.exe pid:  21308
Unable to read PEB for task.
root@siftworkstation:/home/sansforensics/Documents#
```

Figure 58: DLLList Output (Scenario 1)

Scenario 2: Tor Execution from the USB

```
root@siftworkstation:/home/sansforensics/Desktop/cases# vol.py -f memdump.mem --profile=W
in10x64_19041 dlllist -p 18772
Volatility Foundation Volatility Framework 2.6.1
**************************************************************************
firefox.exe pid:  18772
Unable to read PEB for task.
root@siftworkstation:/home/sansforensics/Desktop/cases#
```

Figure 59: DLLList Output (Scenario 2)

In both scenarios, the Dlllist plugin was unable to read Process Environment Block (PEB) of Tor.exe PID and failed to fetch the results.

d): Getsids: Print process security identifiers, the below figure, shows SIDs associated with Tor Browser.

Scenario 1: Tor Execution from the Disk

```
root@siftworkstation:/home/sansforensics/Documents# vol.py -f memdump.mem --profile=Win10x64_19041 getsids | egr
ep 'firefox.exe | tor.exe'
Volatility Foundation Volatility Framework 2.6.1
firefox.exe (16236): S-1-5-21-1294655557-2711347711-1488551409-1001
firefox.exe (16236): S-1-5-21-1294655557-2711347711-1488551409-513 (Domain Users)
firefox.exe (16236): S-1-1-0 (Everyone)
firefox.exe (16236): S-1-5-114 (Local Account (Member of Administrators))
firefox.exe (16236): S-1-5-32-544 (Administrators)
firefox.exe (16236): S-1-5-32-545 (Users)
firefox.exe (16236): S-1-5-4 (Interactive)
firefox.exe (16236): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
firefox.exe (16236): S-1-5-11 (Authenticated Users)
firefox.exe (16236): S-1-5-15 (This Organization)
firefox.exe (16236): S-1-5-113 (Local Account)
firefox.exe (16236): S-1-5-5-0-5592014 (Logon Session)
firefox.exe (16236): S-1-2-0 (Local (Users with the ability to log in locally))
firefox.exe (16236): S-1-5-64-10 (NTLM Authentication)
firefox.exe (16236): S-1-16-8192 (Medium Mandatory Level)
firefox.exe (19804): S-1-5-21-1294655557-2711347711-1488551409-1001
firefox.exe (19804): S-1-5-21-1294655557-2711347711-1488551409-513 (Domain Users)
firefox.exe (19804): S-1-1-0 (Everyone)
firefox.exe (19804): S-1-5-114 (Local Account (Member of Administrators))
firefox.exe (19804): S-1-5-32-544 (Administrators)
firefox.exe (19804): S-1-5-32-545 (Users)
```

Figure 60: Getsids Output (Scenario 1)

Scenario 2: Tor Execution from the USB

```
root@siftworkstation:/home/sansforensics/Desktop/cases# vol.py -f memdump.mem --profile=Win10x64_19041 getsids |
 egrep 'firefox.exe | tor.exe'
Volatility Foundation Volatility Framework 2.6.1
firefox.exe (18744): S-1-5-21-1294655557-2711347711-1488551409-1001
firefox.exe (18744): S-1-5-21-1294655557-2711347711-1488551409-513 (Domain Users)
firefox.exe (18744): S-1-1-0 (Everyone)
firefox.exe (18744): S-1-5-114 (Local Account (Member of Administrators))
firefox.exe (18744): S-1-5-32-544 (Administrators)
firefox.exe (18744): S-1-5-32-545 (Users)
firefox.exe (18744): S-1-5-4 (Interactive)
firefox.exe (18744): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
firefox.exe (18744): S-1-5-11 (Authenticated Users)
firefox.exe (18744): S-1-5-15 (This Organization)
firefox.exe (18744): S-1-5-113 (Local Account)
firefox.exe (18744): S-1-5-5-0-317601 (Logon Session)
firefox.exe (18744): S-1-2-0 (Local (Users with the ability to log in locally))
firefox.exe (18744): S-1-5-64-10 (NTLM Authentication)
firefox.exe (18744): S-1-16-8192 (Medium Mandatory Level)
firefox.exe (18772): S-1-5-21-1294655557-2711347711-1488551409-1001
firefox.exe (18772): S-1-5-21-1294655557-2711347711-1488551409-513 (Domain Users)
firefox.exe (18772): S-1-1-0 (Everyone)
firefox.exe (18772): S-1-5-114 (Local Account (Member of Administrators))
firefox.exe (18772): S-1-5-32-544 (Administrators)
firefox.exe (18772): S-1-5-32-545 (Users)
firefox.exe (18772): S-1-5-4 (Interactive)
```

Figure 61: Getsids Output (Scenario 2)

In the above figure, we can observe, the Tor.exe processor ID is assigned with user permission and user groups.

f) Memory Dump: This plugin performs a memory dump and we perform a string search based on the process ID to find the login credentials, browser history & user keystrokes.

Scenario 1: Tor Execution from the Disk

```
root@siftworkstation:/home/sansforensics/Documents# strings -e l ./21308.dmp | grep 'tor.exe'
DDVDataCollector.exe
\Device\HarddiskVolume3\Users\dell\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe
\Device\HarddiskVolume3\Users\dell\Desktop\desk2\Tor Browser\Browser\TorBrowser\Tor\tor.exe
\Device\HarddiskVolume3\Users\dell\Desktop\desk2\Tor Browser\Browser\TorBrowser\Tor\tor.exe
\Device\HarddiskVolume3\Users\dell\Desktop\desk2\Tor Browser\Browser\TorBrowser\Tor\tor.exe
\Device\HarddiskVolume3\Users\dell\Desktop\desk2\Tor Browser\Browser\TorBrowser\Tor\tor.exe
\Device\HarddiskVolume8\TOR BROWSER\Browser\TorBrowser\Tor\tor.exe
\Device\HarddiskVolume3\Users\dell\Desktop\desk2\Tor Browser\Browser\TorBrowser\Tor\tor.exe
\Device\HarddiskVolume3\Users\dell\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe.lock
\Device\HarddiskVolume8\TOR BROWSER\Browser\TorBrowser\Tor\tor.exe
\Device\HarddiskVolume3\Users\dell\Desktop\desk2\Tor Browser\Browser\TorBrowser\Tor\tor.exe
C:\Users\dell\Desktop\desk2\Tor Browser\Browser\TorBrowser\Tor\tor.exe
\Device\HarddiskVolume3\Users\dell\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exeb}
\Device\HarddiskVolume3\Users\dell\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe
```

```
"C:\Users\dell\Desktop\Tor Browser\Browser\TorBrowser\Tor\tor.exe" --defaults-torrc "C:\Users\dell\Desktop\Tor B
rowser\Browser\TorBrowser\Data\Tor\torrc-defaults" -f "C:\Users\dell\Desktop\Tor Browser\Browser\TorBrowser\Data
\Tor\torrc" DataDirectory "C:\Users\dell\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor" ClientOnionAuthDir "C:
\Users\dell\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\onion-auth" GeoIPFile "C:\Users\dell\Desktop\Tor Bro
wser\Browser\TorBrowser\Data\Tor\geoip" GeoIPv6File "C:\Users\dell\Desktop\Tor Browser\Browser\TorBrowser\Data\T
or\geoip6" HashedControlPassword 16:5c5298da83bc31df60672b9fe13cfe9b2ff8bdccac7d04cadfd47e99fe +__ControlPort 91
51 +__SocksPort "127.0.0.1:9150 ExtendedErrors IPv6Traffic PreferIPv6 KeepAliveIsolateSOCKSAuth" __OwningControl
lerProcess 19804 DisableNetwork 1
```

```
script@http://losf3msiygfmizgshddciot35lxxlf3huhme3ab3eme27e5kcicty4ad.onion<http://losf3msiygfmizgshddciot35lxx
lf3huhme3ab3eme27e5kcicty4ad.onion
http://losf3msiygfmizgshddciot35lxxlf3huhme3ab3eme27e5kcicty4ad.onion/stats.wp.com/s-202118.js
http://losf3msiygfmizgshddciot35lxxlf3huhme3ab3eme27e5kcicty4ad.onion/stats.wp.com/s-202118.js
http://losf3msiygfmizgshddciot35lxxlf3huhme3ab3eme27e5kcicty4ad.onion/
xorw7fyvcyd.onion/login
7oc76tcna45fme47oqjrei4d4aa7xorw7fyvcyd.onion/login
main_frame@http://freshonifyfe4rmuh6qwpsexfhdrww7wnt5qmkoertwxmcuvm4woo4ad.onion<
http://freshonifyfe4rmuh6qwpsexfhdrww7wnt5qmkoertwxmcuvm4woo4ad.onion/?query=drug
http://freshonifyfe4rmuh6qwpsexfhdrww7wnt5qmkoertwxmcuvm4woo4ad.onion/?query=drug
http://hitman3u7q5wq33h5k3p2zrz4lv3jzfofezj7epeucewg5v4dxsypqqd.onion/i/bitcoinmonero.jpg
xmlhttprequest@https://va.tawk.to<http://losf3msiygfmizgshddciot35lxxlf3huhme3ab3eme27e5kcicty4ad.onion
default-src 'none'; connect-src https://duckduckgo.com https://*.duckduckgo.com https://3g2upl4pq6kufc4m.onion/
https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/; manifest-src https://duckduckgo.com htt
ps://*.duckduckgo.com https://3g2upl4pq6kufc4m.onion/ https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twags
wzczad.onion/; media-src https://duckduckgo.com https://*.duckduckgo.com https://3g2upl4pq6kufc4m.onion/ https:/
/duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/; script-src blob: https://duckduckgo.com https:
//*.duckduckgo.com https://3g2upl4pq6kufc4m.onion/ https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzc
zad.onion/ 'unsafe-inline' 'unsafe-eval'; font-src data: https://duckduckgo.com https://*.duckduckgo.com https:/
/3g2upl4pq6kufc4m.onion/ https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/; img-src data:
https://duckduckgo.com https://*.duckduckgo.com https://3g2upl4pq6kufc4m.onion/ https://duckduckgogg42xjoc72x3sj
asowoarfbgcmvfimaftt6twagswzczad.onion/; style-src https://duckduckgo.com https://*.duckduckgo.com https://3g2up
l4pq6kufc4m.onion/ htt
```

Figure 62: Memory Dump Output (Scenario 1)

In the above figure, all the .onion websites visited by the user and full path of Tor Browser was captured in plain text in the memory and it is an excellent wealth of information for the forensic investigator.

Scenario 2: Tor Execution from the USB

```
root@siftworkstation:/home/sansforensics/Desktop/cases# strings -e l ./22720.dmp | grep "tor.exe"
MpCopyAccelerator.exe
Integrator.exeC:\Program Files\Microsoft Office\root\IntegrationMicrosoft Office Click-to-Run Integrator
ByteCodeGenerator.exeC:\Windows\System32AppX Deployment Bytecode Generator EXE
MpCopyAccelerator.exeC:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2108.7-0Microsoft Malware Protectio
n Copy Accelerator Utility
DDVDataCollector.exeC:\Program Files\Dell\DellDataVaultDell Data Vault Data Collector Service
OSProfileCollector.exeC:\Program Files\Dell\SARemediation\agentOSProfileCollector
EmEditor.exeC:\Users\dell\AppData\Local\Programs\EmEditorEmEditor
tor.exeE:\TOR BROWSER\Browser\TorBrowser\Tortor.exe
Narrator.exerol
Locator.exe
Locator.exe
ByteCodeGenerator.exe
ByteCodeGenerator.exe
AcroTextExtractor.exe
Narrator.exe.mui
Narrator.exe.mui
Narrator.exe.mui
Locator.exe.mui2
Narrator.exe.mui
tor.exeE:\TOR BROWSER\Browser\TorBrowser\Tortor.exe
```

```
\Device\HarddiskVolume8\TOR BROWSER\Browser\TorBrowser\Tor\tor.exe
"E:\TOR BROWSER\Browser\TorBrowser\Tor\tor.exe" --defaults-torrc "E:\TOR BROWSER\Browser\TorBrowser\Data\Tor\tor
rc-defaults" -f "E:\TOR BROWSER\Browser\TorBrowser\Data\Tor\torrc" DataDirectory "E:\TOR BROWSER\Browser\TorBrow
ser\Data\Tor" ClientOnionAuthDir "E:\TOR BROWSER\Browser\TorBrowser\Data\Tor\onion-auth" GeoIPFile "E:\TOR BROWS
ER\Browser\TorBrowser\Data\Tor\geoip" GeoIPv6File "E:\TOR BROWSER\Browser\TorBrowser\Data\Tor\geoip6" HashedCont
rolPassword 16:68657b620a8b688d60f95e3e14d8b427a1f0c3972a9fbf96fd023bec53 +__ControlPort 9151 +__SocksPort "127.
0.0.1:9150 ExtendedErrors IPv6Traffic PreferIPv6 KeepAliveIsolateSOCKSAuth" __OwningControllerProcess 18772 Disa
bleNetwork 1
```

```
l4pq6kufc4m.onion/ https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/ 'unsafe-inline'; obje
ct-src 'none'; worker-src blob:; child-src blob: https://duckduckgo.com https://*.duckduckgo.com https://3g2upl4
pq6kufc4m.onion/ https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/; frame-src blob: https:
//duckduckgo.com https://*.duckduckgo.com https://3g2upl4pq6kufc4m.onion/ https://duckduckgogg42xjoc72x3sjasowoa
rfbgcmvfimaftt6twagswzczad.onion/; form-action https://duckduckgo.com https://*.duckduckgo.com https://3g2upl4pq
6kufc4m.onion/ https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/; frame-ancestors 'self';
base-uri 'self'; block-all-mixed-content
(http,khsnou3d7qfftrzcagmpzsbaippr5sjpiyb4itofkhoelvkzcics7oid.onion)
://hackingcovdntbsyvfqbs6dswnfdrvoygqbi4coiknh4ubuv643frpad.onion/ from extracting canvas data because no user i
nput was detected.
http://hackingcovdntbsyvfqbs6dswnfdrvoygqbi4coiknh4ubuv643frpad.onion/
TorShops | Create your own .onion store - buy and sell drugs, guns, counterfeits, fake ids, fake passports for b
itcoin
TorShops | Create your own .onion store - buy and sell drugs, guns, counterfeits, fake ids, fake passports for b
itcoin
(http,khsnou3d7qfftrzcagmpzsbaippr5sjpiyb4itofkhoelvkzcics7oid.onion)
4coiknh4ubuv643frpad.onion/
http://hyf37my27mgaqzc7suszc3nstlmss2xf76vjsl2zygpu7v5qxjigbqqd.onion/
(http,hyf37my27mgaqzc7suszc3nstlmss2xf76vjsl2zygpu7v5qxjigbqqd.onion)
(http,khsnou3d7qfftrzcagmpzsbaippr5sjpiyb4itofkhoelvkzcics7oid.onion)
nnbizqx7cvxe4njde3l4cz75gxhdg73lpqlcflql7vad.onion
mvadrbcmsuaqcxl3iorhna5lf6lwwq2xtcat2ij7fjid.onion
kzk6aulen2amvoapjyl2wp5eb3c4ytpwvnjsxywg3gqd.onion
mqzada7q55zik7ft3dbpd5cxxwqciqn7yvbkz3bdnvad.onion
http://freshonifyfe4rmuh6qwpsexfhdrww7wnt5qmkoertwxmcuvm4woo4ad.onion/
```

Figure 63: Memory Dump Output (Scenario 2)

Even in scenario 2, all the .onion websites visited by the user and full path of Tor Browser (USB Device Path) was captured in plain text in the memory dump.

9.3 Network Forensics

The packets are captured from the live system while browsing the websites in the Tor browser using network capturing tools.

Tool Used: NetworkMiner

As unencrypted network traffic is sent between localhost TCP sockets on the computer, in our experiment we use network miner to capture the traffic from the localhost of the tor browser. Tor browser use a SOCKS proxy which is listening on TCP port 9150 rather than an HTTP proxy and Tor listens for SOCKS connections on port 9050 and there will be unencrypted network traffic from the SOCKS protocol which connect to our local Tor client, so we can sniff traffic on localhost to capture packets of the tor browser.

We can also use the RawCap tool to sniff the localhost traffic and export it in pcap format so that it can support Wireshark or NetworkMiner to analyse the traffic.

We can observe in figure 64, network miner has captured all the drug images which was loaded by the tor browser while browsing the drug marketplace.

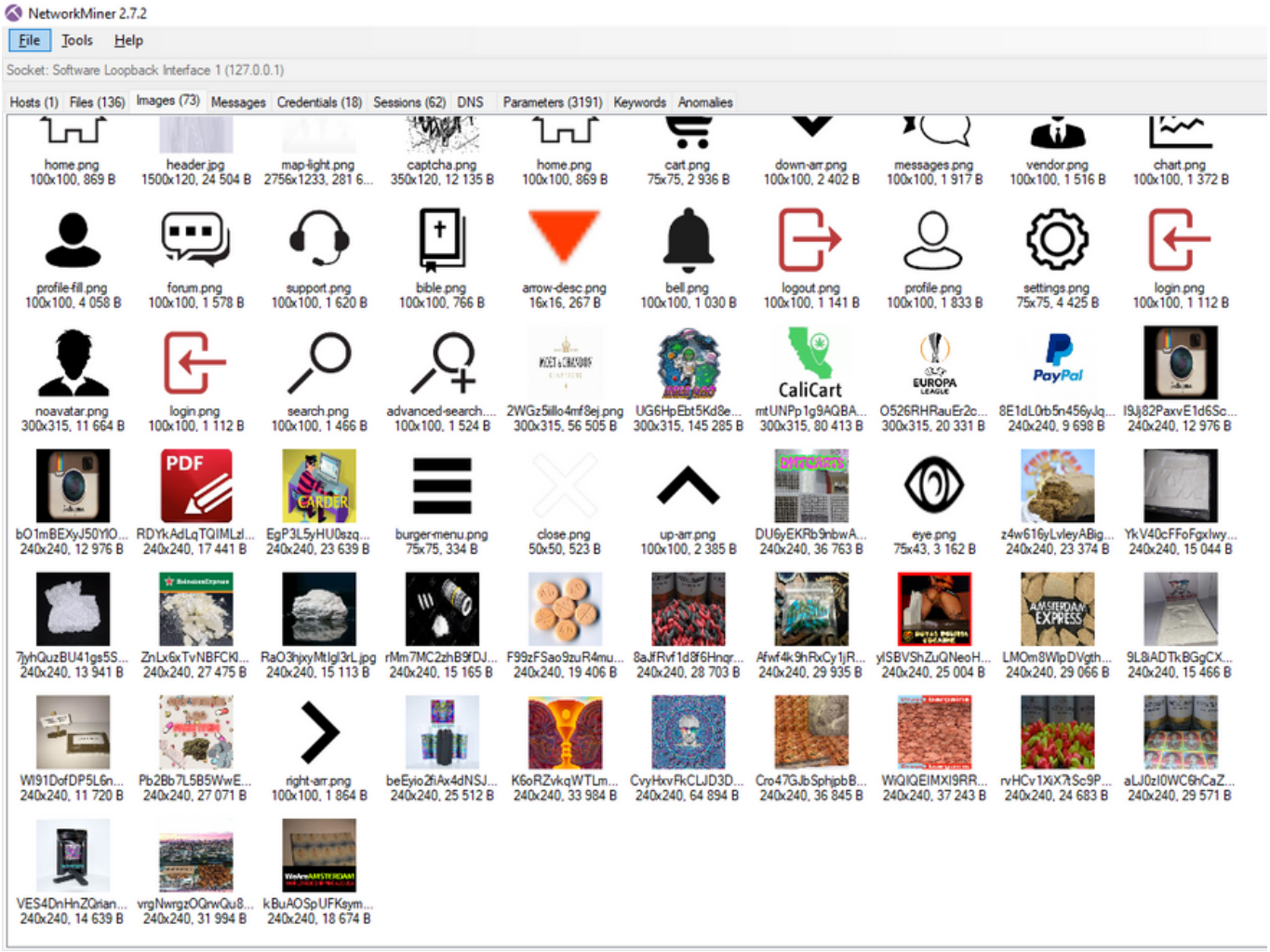


Figure 64: Image captured by Network Miner while browsing Drug websites by Tor Browser

Figure 65: Image captured by Network Miner while browsing Drug websites by Tor Browser

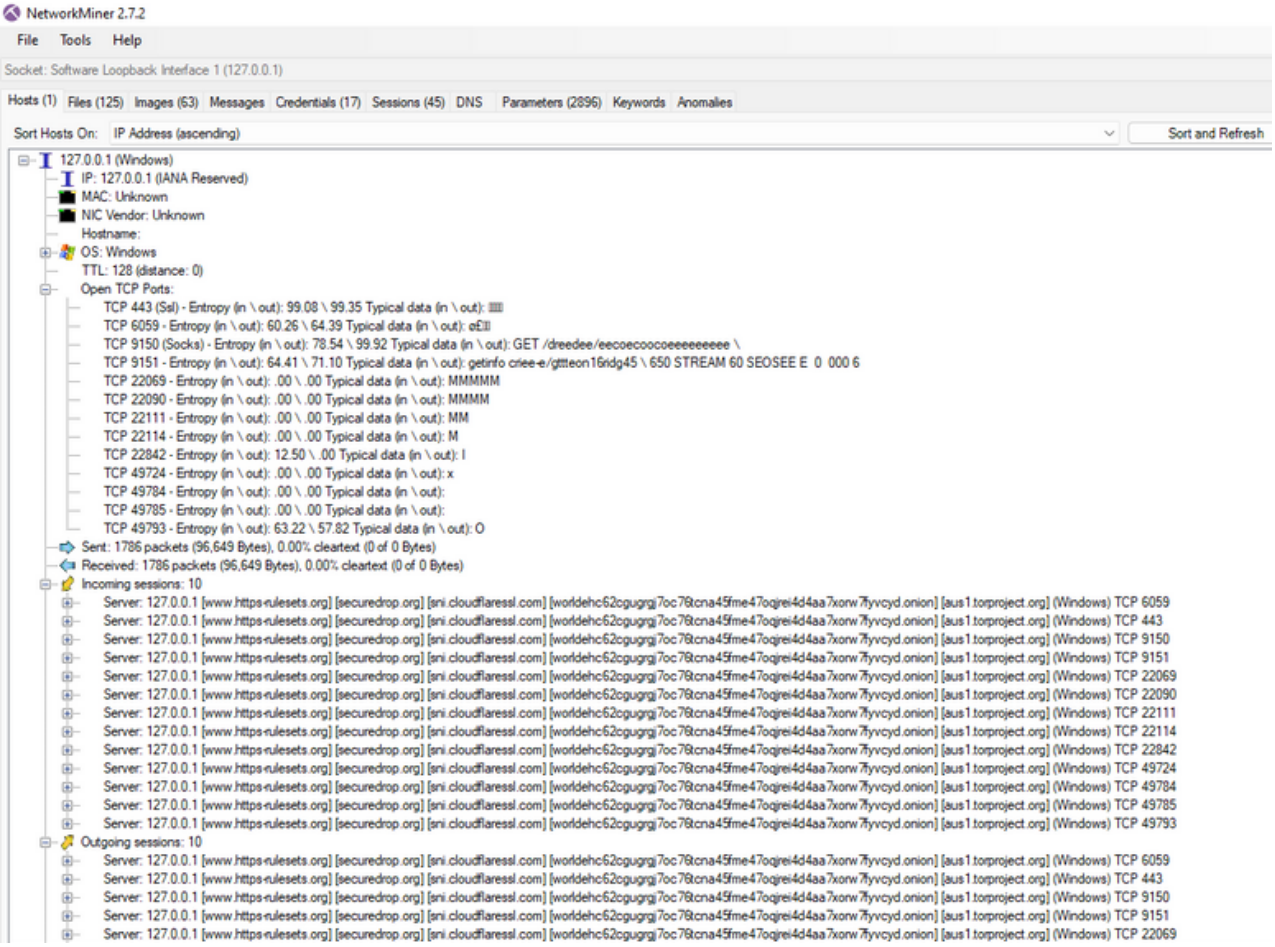


Figure 65: URL & Host Details captured by the tool while browsing the .onion websites

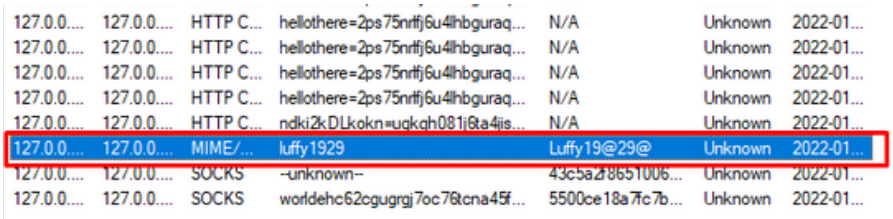


Figure 66: Username and Password captured in Plaintext which was used to login Drug Marketplace

10. Man-in-the-Middle Attack: Sniffing Traffic

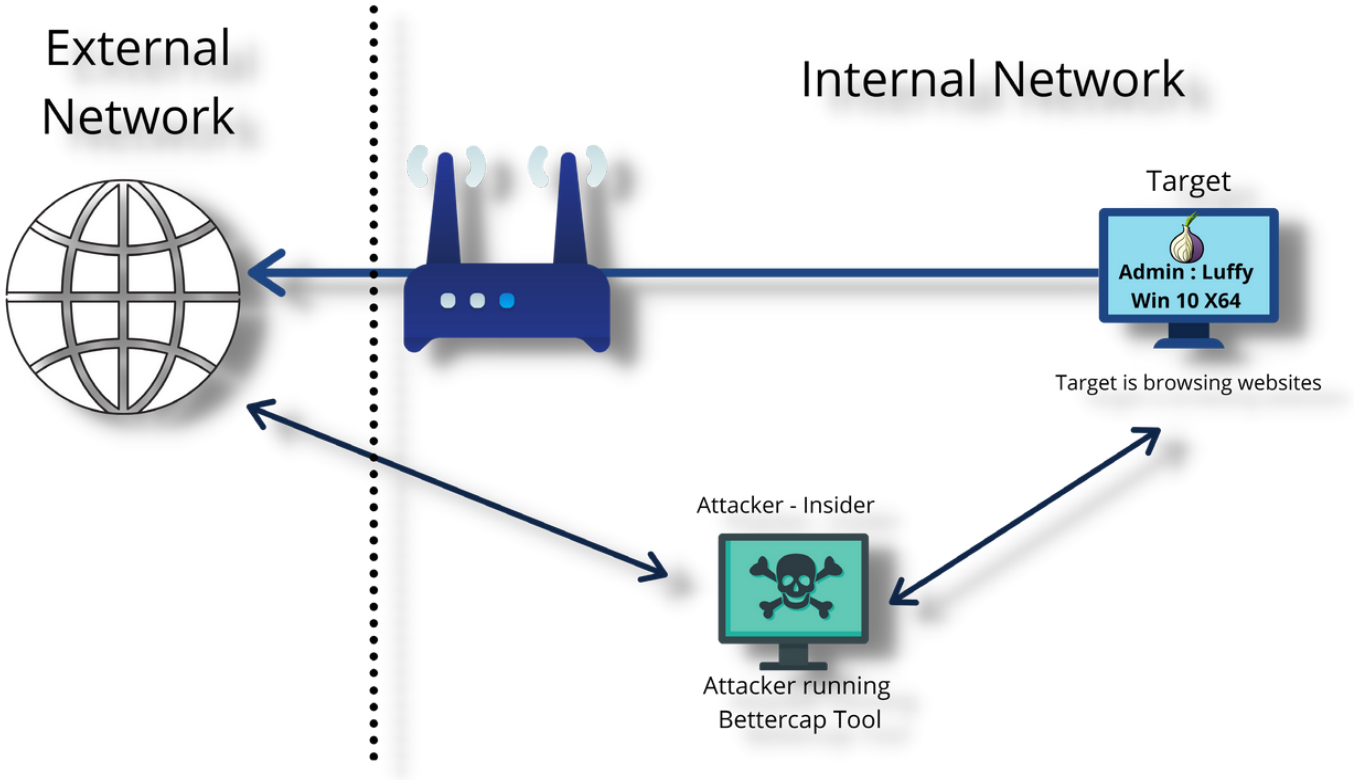


Figure 67: Man-in-the-Middle Attack

For our research work, we will be using the BetterCAP tool which is an amazing powerful MITM Attack written in Golang. It can manipulate HTTP, HTTPS and TCP traffic in real-time.

As shown in figure 67, the target will be running Windows 10 64-Bit OS installed with the latest Tor Browser and we will be using the latest Kali-Linux Version 2020.2 VM to perform MITM Attack. During a MITM attack, the tool forces the network to consider the attacker machine as the router by spoofing the router mac address using ARP cache poisoning by sending gratuitous ARP responses to the target or through some other method. After this, all legitimate traffic flows through the attacker system and is then forwarded to the router. Now BetterCAP tool can sniff the traffic and modify them on the fly.

SOURCE: 1. *https://www.kali.org/downloads/*

BetterCAP Tool Dependencies

- build-essential
- libpcap-dev
- libusb-1.0-0-dev (required by the HID module)
- libnetfilter-queue-dev (on Linux only, required by the packet.proxy module)

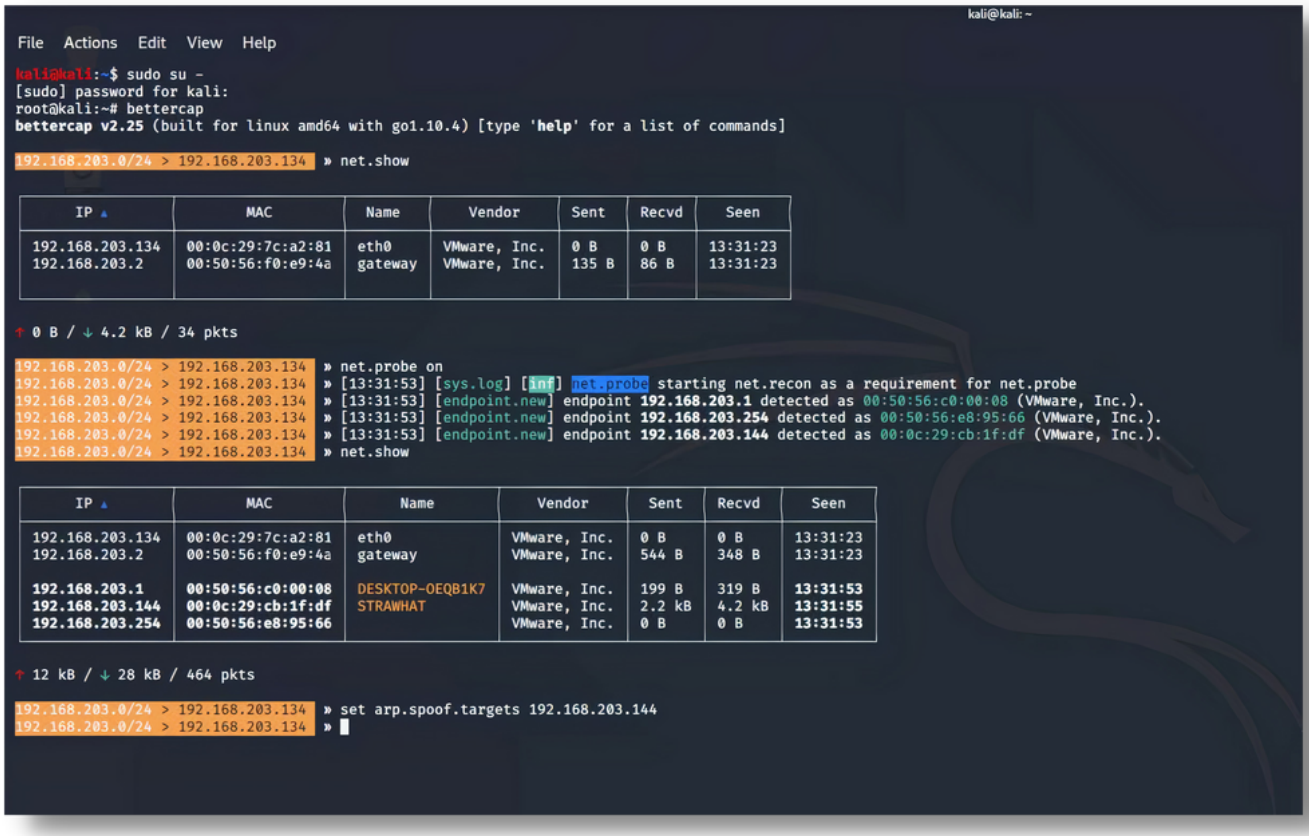


Figure 68: MITM Attack using Bettercap Tool

Figure 69: MITM Attack: All the websites requested by Target system using Microsoft Edge were captured by the Tool

We conclude from figure 69, that websites, requested by the Tor browser were not sniffed by the Bettercap Tool and the traffic are intercepted when the target system requests information from Microsoft Edge or Chrome browser.

11. Dark Web Monitoring and OSINT

Dark Web itself is research-driven and loaded with valuable information but its very hard to mine data and track the source. As darkweb is the prime place for illegal activity, usage of darkweb monitoring/OSINT tools is a valuable asset for Law Enforcement Agencies where they can gather intelligence on targets by harvesting publicly available data from the dark web.

OnionScan is one of the best open-source tools to monitor the darkweb .onion services. The OnionScan is written in Go Language that checks for operational security leaks or software misconfiguration. Most of the security breaches happen due to human error and this tool takes advantage of such misconfiguration and scans .onion websites for Apache mod_status Leak, Open Directories, EXIF Tags, Server Fingerprint, 3rd party **Analytics IDs, PGP Identities, SSH, FTP & SMTP, Cryptocurrency Clients and protocols including IRC, XMPP, VNC & ricochet.**

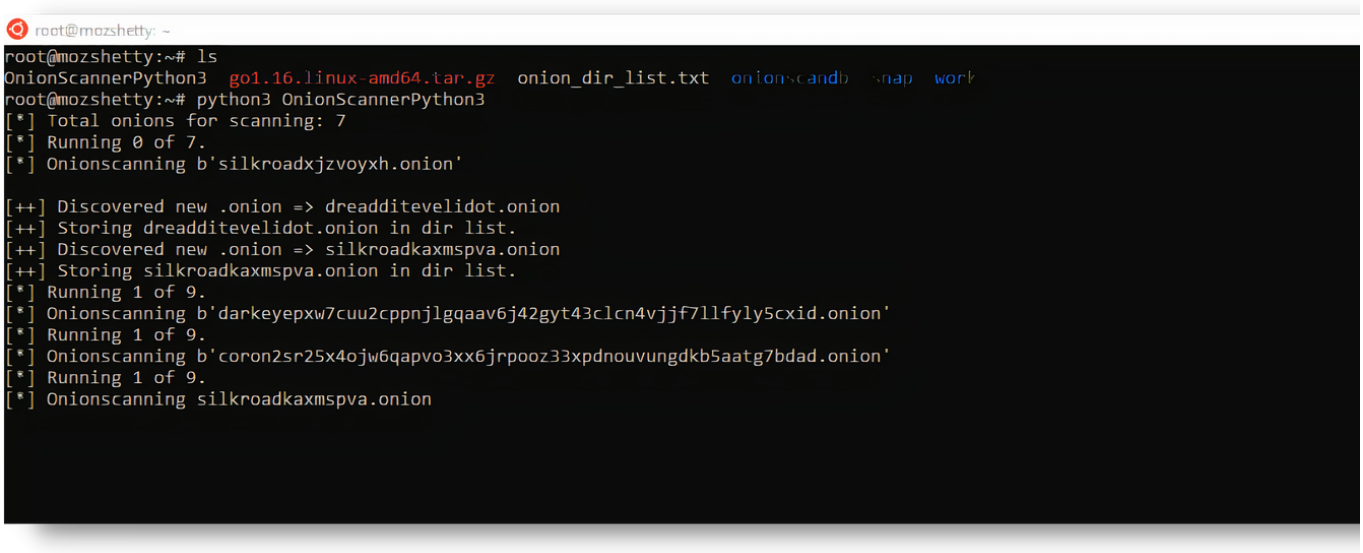


Figure 70: Onionscan Tool running in VPS

In figure 70, we have deployed OnionScan in Virtual Private Server which will be scanning the stored .onion websites for misconfigurations. It will be running 24x7 without human intervention and the final output will be stored in JSON format.

Investigators can use Torbot to crawl the .onion websites to collect open data from the dark web. Torbot is an automation toolset that helps us to scan across the Darknet connecting, gathering, refining, and analyzing the data and with the help of a sub-module called randomizer which randomizes the header information and IP address which would help in preventing IP blocking and helps in maintaining anonymity.

SOURCE:
1. https://github.com/s-rah/onionscan
2. https://4n6shetty.tech/Setting-up-Darkweb-Monitoring-using-Onionscan-deployed-in-Virtual-Private-Server
3. https://github.com/DedSecInside/TorBot

OnionScan scan can pull EXIF Data from the darknet websites which can be major evidence for the LEA. As you can see in figure 71, EXIF data was pulled by OnionScan Tool from one of the infamous sites involved in malpractices that had hit the darknet.

Figure 71: Onionscan EXIF DATA (Source: Krpt3ia)

List of Darkweb OSINT & Bitcoin Analysis Methods:

- TinyEye Reverse Image Search
- Wayback Machine
- Breached Database (Forums)
- Blockchain Explorer
- Maltego
- Hidden Codes, Embedded video Links to the clearnet
- Whois History
- Download URL - Whois Search
- WhatWeb - Web Scanner
- WGET Torrify
- GraphSense
- TorBo

12. Conclusion & Future Work:

This paper presents a forensic analysis of the latest Tor Browser and other programs on the Windows 11 system. We have analysed all the artifacts in both disk & memory; we can conclude from our results, that the Tor browser leaves more artifacts in both the memory and the hard disk. We have performed analysis on the latest OS and programs which are up to date using free and open-source tools. This helps Law Enforcement Agencies to perform analysis on seized hard disk or volatility memory without the help of any commercial tools.

By acknowledging the obtained results from this research work, a forensic investigator can prove the execution of Tor Browser and other programs even after a user has attempted to delete it permanently, including the full path of the program and its associated files along with creation and last execution time/date.

As part of future research, we are interested in executing network forensics where we can perform the packet capture at the unencrypted layer (Localhost) using different methods or run, network forensic capture tool using remote service or netcat command, and perform analysis on Tor browser which is installed on the Tails operating system.

References:

[1]. Darcie, W., Boggs, R.J., Sammons, J., Fenger, T., 2014. Online Anonymity: Forensic Analysis of the Tor Browser Bundle. Technical Report. Marshall University.
(URL: http://www.marshall.edu/forensics/files/WinklerDarcieResearchPaper 8-6-141.pdf)

[2]. Perry, M., Clark, E., Murdoch, S., Koppen, G., 2018. Design and Implementation of the Tor Browser. Technical Report. The Tor Project.
(URL: https://www.torproject.org/projects/torbrowser/design/)

[3]. Aron Warren, A., 2017. Tor Browser Artifacts in Windows 10. Technical Report: SANS.
(URL:https://www.sans.org/reading-room/whitepapers/forensics/tor-browser-artifacts-windows-10-37642)

[4]. TOR Forensics: Investigating the Tor Browser for Evidence.
(URL: https://netseedblog.com/security/tor-forensics-investingating-tor-for-evidence/)

[5]. Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web.
(URL: https://www.sciencedirect.com/science/article/pii/S0379073819301082)

[6]. Bip-0039-wordlists
(URL: https://github.com/bitcoin/bips/blob/master/bip-0039/bip-0039-wordlists.md)

[7]. Michael Doran, A Forensic Look at Bitcoin Cryptocurrency; SANS,
(URL:https://digital-forensics.sans.org/community/papers/gcfa/forensic-bitcoin-cryptocurrency_11168)

[8]. Memory Forensics & Tor.
(URL: https://bitofhex.com/2018/04/29/volatility-and-tor/)

[9]. Brett Hawkins, Under the ocean of the Internet - The Deep Web; SANS
(URL:https://www.sans.org/reading-room/whitepapers/covert/ocean-internet-deep-web-37012)

[10]. Private Key Generation in Bitcoin Wallets as defined in BIP-0039
(URL:https://privatekeys.org/2017/09/03/private-key-generation-in-bitcoin-wallets-as-defined-in-bip-0039/)

DSCI
PROMOTING DATA PROTECTION

KARNATAKA STATE POLICE
CRIMINAL INVESTIGATION DEPARTMENT
C.I.D

Infosys Foundation

CENTRE FOR CYBERCRIME INVESTIGATION TRAINING & RESEARCH

Cybercrime Division, Carlton House, 2nd Floor,
Annexe Building -2, CID HQRS,
Palace Road, Bengaluru, Karnataka - 560001

ccitr@dsci.in

080-22374726

@CybercrimeCID

@DSCI_Connect