Module 10: Dark Web Forensics

Lab Scenario

When forensic investigators come across cases of dark web crimes, they generally do not locate any traces of criminal activity on normal browsers meant for daily use such as Google Chrome Mozilla Firefox, Microsoft Edge/Internet Explorer, etc. For perpetrating dark web crimes, criminals prefer the Tor Browser as it provides them with a high level of anonymity. In such instances, investigators need to examine the suspect machine for Tor Browser artifacts to help them solve such cases.

Tor Browser artifacts can be retrieved by examining the RAM dump of the suspect machine. In case Tor Browser has been removed/uninstalled from a system after committing the crime,investigators can discover its related artifacts by analyzing its prefetch file on a Windows machine.

Lab Objectives

The objective of this lab is to help you understand dark web forensics techniques. The tasks include:

- Discovering Tor Browser activity on a Windows machine
- Examining RAM dumps to discover Tor Browser artifacts

Overview of Dark Web Forensics

Use of dark web forensics is necessary because of an increase in illegal activities such as drugs and weapons trafficking, selling credit card details and other private information related to individuals, child pornography, etc. that are facilitated through the internet. Dark web forensics helps investigators gather evidence against the perpetrators of such dark web crimes so that they can be prosecuted in a court of law.

Lab Tasks

Recommended labs to assist you in dark web forensics:

- Detecting TOR browser on a machine
- Analyzing RAM dumps to retrieve TOR browser artifacts

Lab 1: Detecting TOR Browser on a Machine

Lab Scenario

During a search and seize operation connected with a case of an internet-based fraud in which credit card information and bank details of several individuals were stolen and sold, law enforcement authorities got hold of a few computers belonging to the suspects. During the forensic investigation of the seized computers, the investigators discovered that the suspects had tried to cover their tracks by removing all the tools/applications they had used on the systems. The investigators decided to examine the prefetch files on the system to determine the application/program that might have been used by the suspects to commit crimes. While searching through the prefetch files, the investigators located a prefetch file for Tor Browser, which indicate that this might be a case of dark web crime. How should the investigators proceed to be able to analyze the Tor Browser artifacts in this case?

As a forensic investigator, you must know how to analyze prefetch files pertaining to Tor Browser using the right tool(s).

Lab Objectives

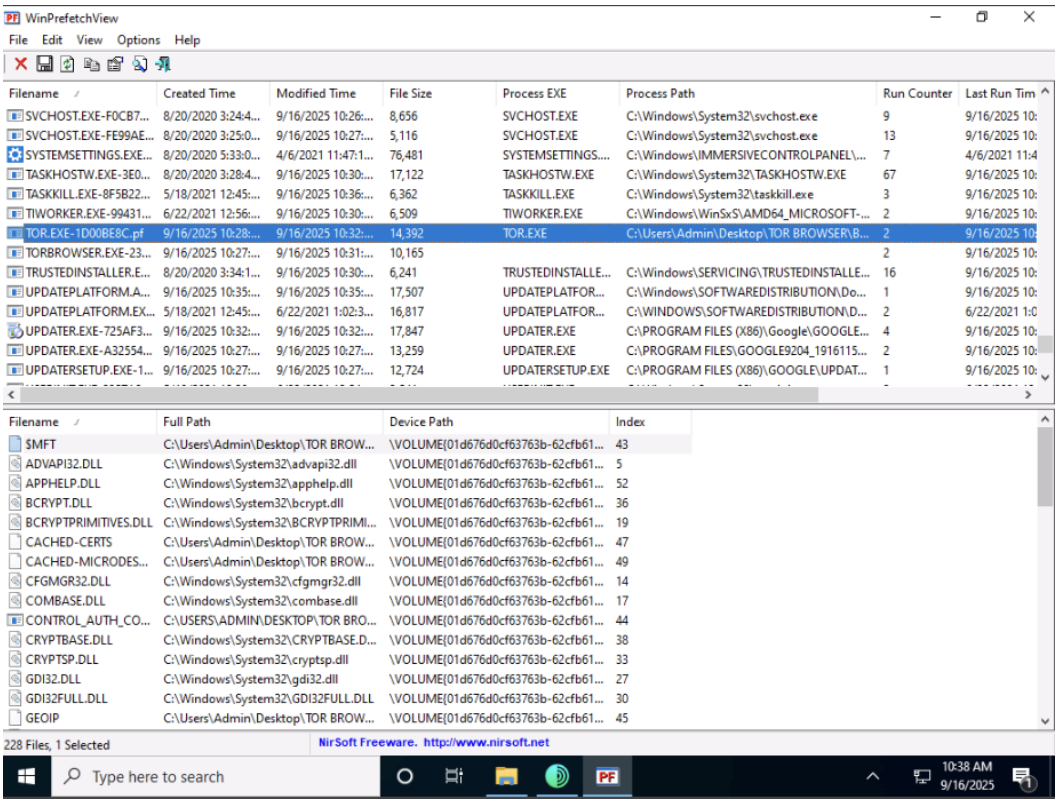
Tor Browser is based on a Mozilla Firefox browsing application that works on the concept of Onion Routing. It allows users to access the dark web and carry out criminal/illegal activities anonymously.

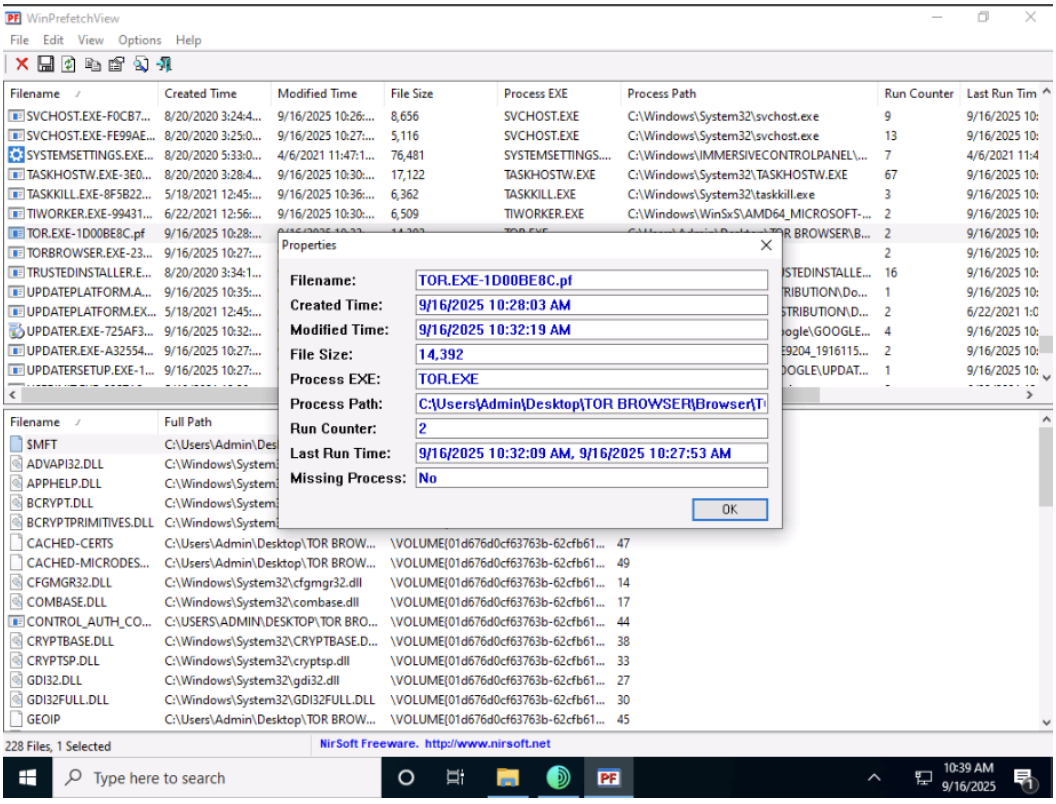
In this lab, you will learn how to retrieve Tor Browser activity from a Windows machine by:

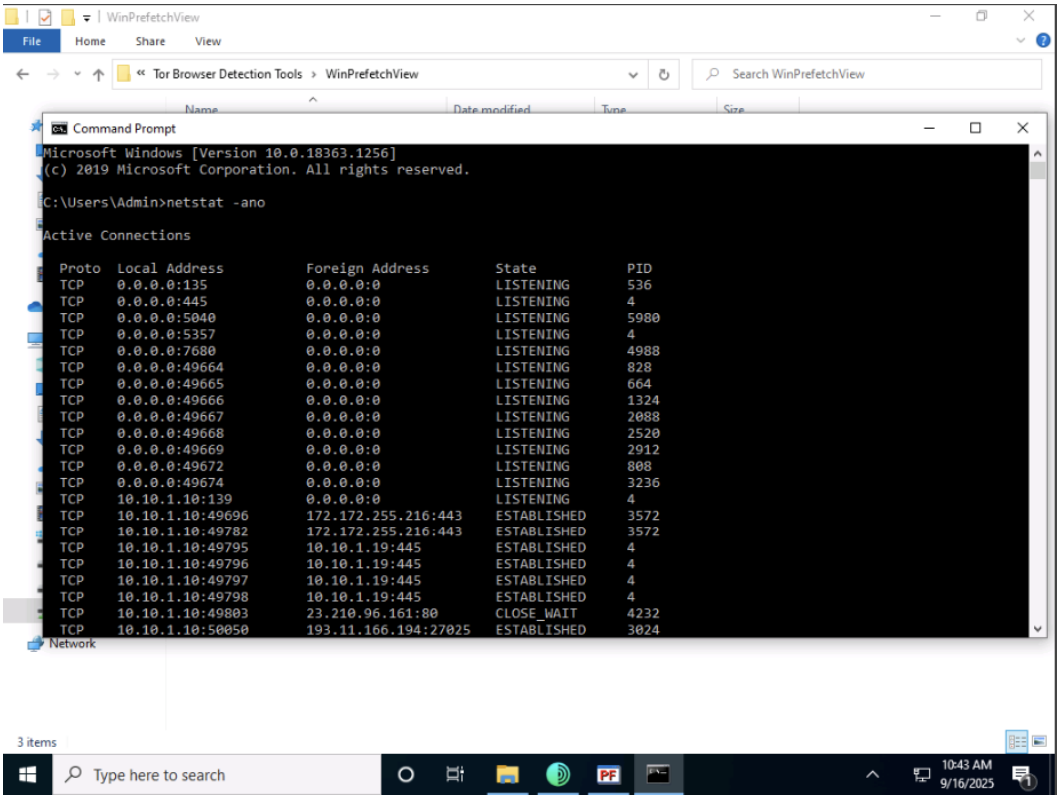
- Examining Windows prefetch files
- Monitoring network connections using netstat command

Overview of the Lab

This lab familiarizes you with the process of determining whether **Tor Browser** has been used on a suspect system with the help of **WinPrefetchView**, an application that helps you find the prefetch files pertaining to various programs that have been installed on a system. Even if a program is deleted/uninstalled from a system, the prefetch file related to it is still likely to remain on the system, which provides the evidence for that program's execution on the system.


WinPrefetchView
File Edit View Options Help
Filename | Created Time | Modified Time | File Size | Process EXE | Process Path | Run Counter | Last Run Tim
SVCHOST.EXE-F0CB7... | 8/20/2020 3:24:4... | 9/16/2025 10:26:... | 8,656 | SVCHOST.EXE | C:\Windows\System32\svchost.exe | 9 | 9/16/2025 10:
SVCHOST.EXE-FE99AE... | 8/20/2020 3:25:0... | 9/16/2025 10:27:... | 5,116 | SVCHOST.EXE | C:\Windows\System32\svchost.exe | 13 | 9/16/2025 10:
SYSTEMSETTINGS.EXE... | 8/20/2020 5:33:0... | 4/6/2021 11:47:1... | 76,481 | SYSTEMSETTINGS.... | C:\Windows\IMMERSIVECONTROLPANEL\... | 7 | 4/6/2021 11:4
TASKHOSTW.EXE-3E0... | 8/20/2020 3:28:4... | 9/16/2025 10:30:... | 17,122 | TASKHOSTW.EXE | C:\Windows\System32\TASKHOSTW.EXE | 67 | 9/16/2025 10:
TASKKILL.EXE-8F5B22... | 5/18/2021 12:45:... | 9/16/2025 10:36:... | 6,362 | TASKKILL.EXE | C:\Windows\System32\taskkill.exe | 3 | 9/16/2025 10:
TIWORKER.EXE-99431... | 6/22/2021 12:56:... | 9/16/2025 10:30:... | 6,509 | TIWORKER.EXE | C:\Windows\WinSxS\AMD64_MICROSOFT-... | 2 | 9/16/2025 10:
TOR.EXE-1D00BE8C.pf | 9/16/2025 10:28:... | 9/16/2025 10:32:... | 14,392 | TOR.EXE | C:\Users\Admin\Desktop\TOR BROWSER\B... | 2 | 9/16/2025 10:
TORBROWSER.EXE-23... | 9/16/2025 10:27:... | 9/16/2025 10:31:... | 10,165 | | | 2 | 9/16/2025 10:
TRUSTEDINSTALLER.E... | 8/20/2020 3:34:1... | 9/16/2025 10:30:... | 6,241 | TRUSTEDINSTALLE... | C:\Windows\SERVICING\TRUSTEDINSTALLE... | 16 | 9/16/2025 10:
UPDATEPLATFORM.A... | 9/16/2025 10:35:... | 9/16/2025 10:35:... | 17,507 | UPDATEPLATFOR... | C:\Windows\SOFTWAREDISTRIBUTION\Do... | 1 | 9/16/2025 10:
UPDATEPLATFORM.EX... | 5/18/2021 12:45:... | 6/22/2021 1:02:3... | 16,817 | UPDATEPLATFOR... | C:\WINDOWS\SOFTWAREDISTRIBUTION\D... | 2 | 6/22/2021 1:0
UPDATER.EXE-725AF3... | 9/16/2025 10:32:... | 9/16/2025 10:32:... | 17,847 | UPDATER.EXE | C:\PROGRAM FILES (X86)\Google\GOOGLE... | 4 | 9/16/2025 10:
UPDATER.EXE-A32554... | 9/16/2025 10:27:... | 9/16/2025 10:27:... | 13,259 | UPDATER.EXE | C:\PROGRAM FILES\GOOGLE9204_1916115... | 2 | 9/16/2025 10:
UPDATERSETUP.EXE-1... | 9/16/2025 10:27:... | 9/16/2025 10:27:... | 12,724 | UPDATERSETUP.EXE | C:\PROGRAM FILES (X86)\GOOGLE\UPDAT... | 1 | 9/16/2025 10:
Filename | Full Path | Device Path | Index
$MFT | C:\Users\Admin\Desktop\TOR BROW... | \VOLUME{01d676d0cf63763b-62cfb61... | 43
ADVAPI32.DLL | C:\Windows\System32\advapi32.dll | \VOLUME{01d676d0cf63763b-62cfb61... | 5
APPHELP.DLL | C:\Windows\System32\apphelp.dll | \VOLUME{01d676d0cf63763b-62cfb61... | 52
BCRYPT.DLL | C:\Windows\System32\bcrypt.dll | \VOLUME{01d676d0cf63763b-62cfb61... | 36
BCRYPTPRIMITIVES.DLL | C:\Windows\System32\BCRYPTPRIMI... | \VOLUME{01d676d0cf63763b-62cfb61... | 19
CACHED-CERTS | C:\Users\Admin\Desktop\TOR BROW... | \VOLUME{01d676d0cf63763b-62cfb61... | 47
CACHED-MICRODES... | C:\Users\Admin\Desktop\TOR BROW... | \VOLUME{01d676d0cf63763b-62cfb61... | 49
CFGMGR32.DLL | C:\Windows\System32\cfgmgr32.dll | \VOLUME{01d676d0cf63763b-62cfb61... | 14
COMBASE.DLL | C:\Windows\System32\combase.dll | \VOLUME{01d676d0cf63763b-62cfb61... | 17
CONTROL_AUTH_CO... | C:\USERS\ADMIN\DESKTOP\TOR BRO... | \VOLUME{01d676d0cf63763b-62cfb61... | 44
CRYPTBASE.DLL | C:\Windows\System32\CRYPTBASE.D... | \VOLUME{01d676d0cf63763b-62cfb61... | 38
CRYPTSP.DLL | C:\Windows\System32\cryptsp.dll | \VOLUME{01d676d0cf63763b-62cfb61... | 33
GDI32.DLL | C:\Windows\System32\gdi32.dll | \VOLUME{01d676d0cf63763b-62cfb61... | 27
GDI32FULL.DLL | C:\Windows\System32\GDI32FULL.DLL | \VOLUME{01d676d0cf63763b-62cfb61... | 30
GEOIP | C:\Users\Admin\Desktop\TOR BROW... | \VOLUME{01d676d0cf63763b-62cfb61... | 45
228 Files, 1 Selected
NirSoft Freeware. http://www.nirsoft.net
Type here to search
10:38 AM
9/16/2025


WinPrefetchView
File Edit View Options Help
Properties
Filename: TOR.EXE-1D00BE8C.pf
Created Time: 9/16/2025 10:28:03 AM
Modified Time: 9/16/2025 10:32:19 AM
File Size: 14,392
Process EXE: TOR.EXE
Process Path: C:\Users\Admin\Desktop\TOR BROWSER\Browser\T
Run Counter: 2
Last Run Time: 9/16/2025 10:32:09 AM, 9/16/2025 10:27:53 AM
Missing Process: No
OK
228 Files, 1 Selected
NirSoft Freeware. http://www.nirsoft.net
Type here to search
10:39 AM
9/16/2025



Lab 2: Analyzing RAM Dumps to Retrieve TOR Browser Artifacts

Lab Scenario

Forensic investigators have seized a computer belonging to a drug trafficker who is suspected of expanding his drug smuggling network through the dark web. During investigation, it was found that the suspect had been using Tor Browser on his system to engage in drug trafficking and its expansion. To extract more information on the suspect's activities related to drug trafficking, investigators need to analyze the RAM dump of his system so that it reveals all his activities on Tor Browser. The artifacts obtained from the RAM dump can help the investigators extract evidence that can be used to prosecute the suspect.

As a forensic investigator, you must know how to analyze the RAM dump of a suspect machine and retrieve Tor Browser artifacts.

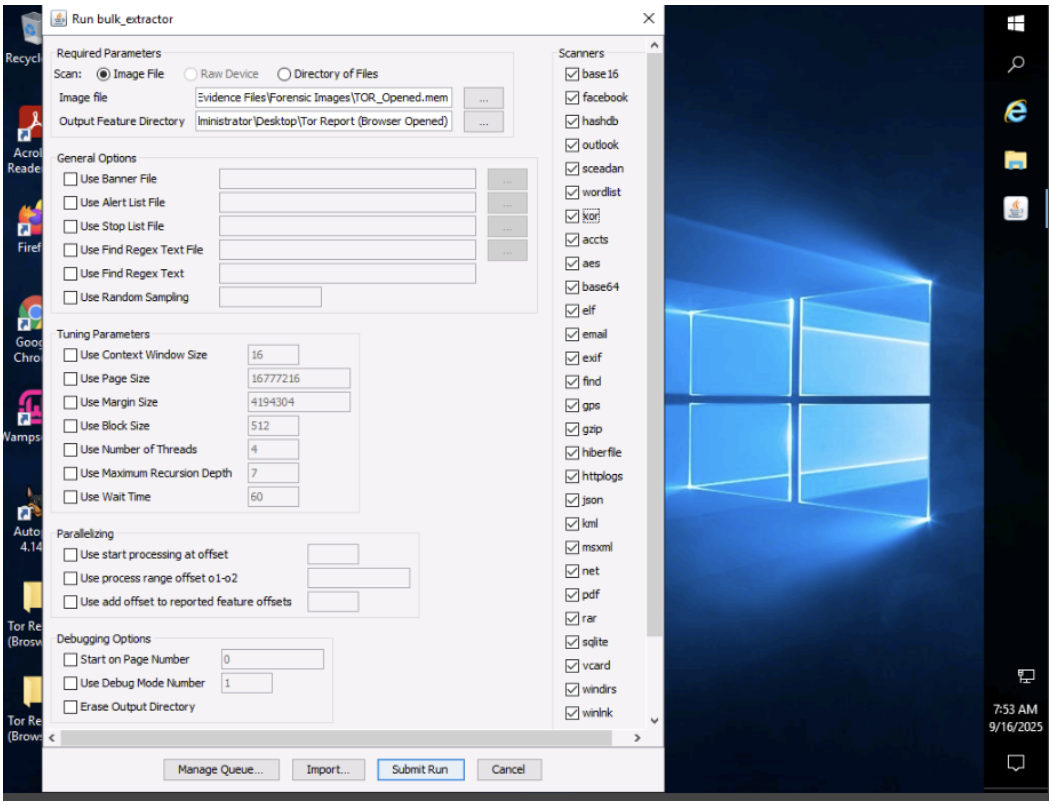
Lab Objectives

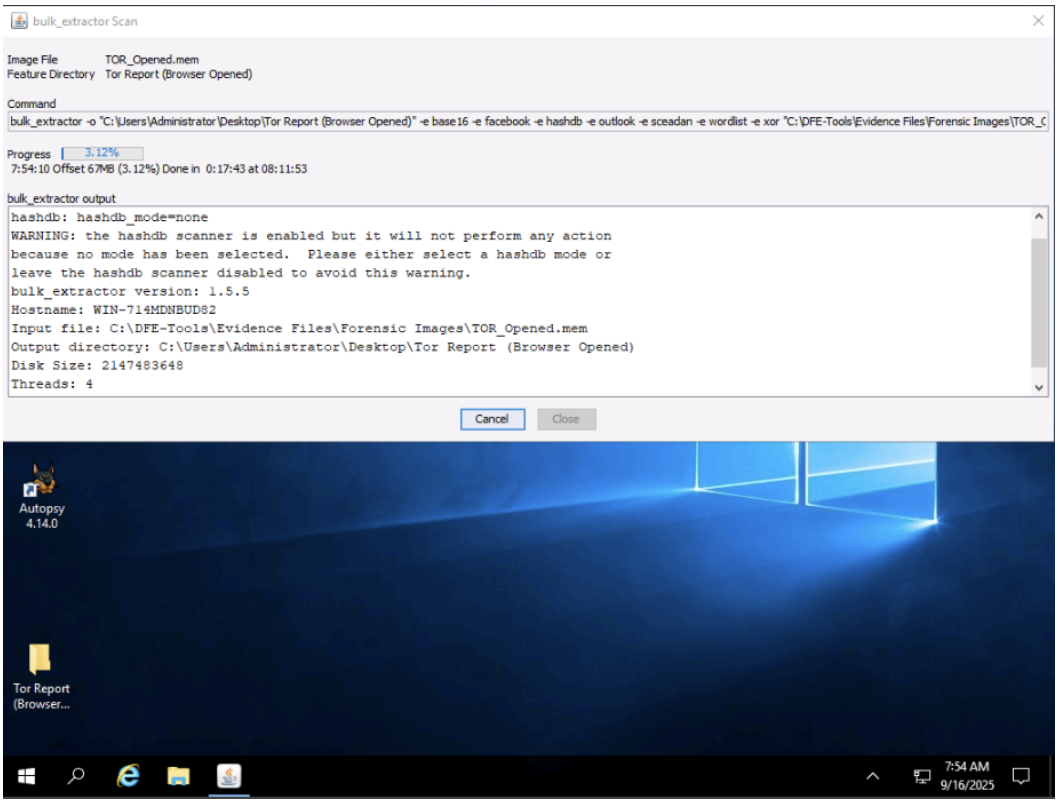
The memory dump collected from a suspect machine not only contains artifacts related to the browser, but also all the activities that occurred on it. Analyzing RAM dump can help investigators find all details pertaining to the activities that an attacker has performed on the system using Tor Browser.

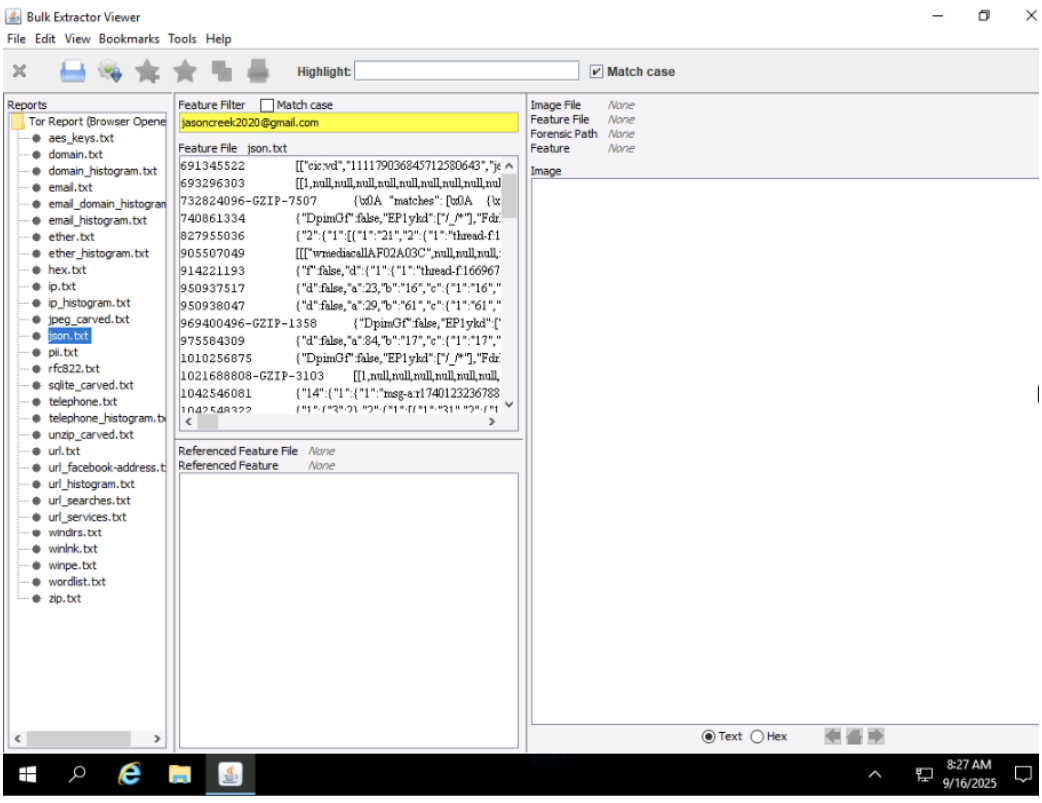
The objective of this lab is to help you learn how to examine a RAM dump and recover potential artifacts pertaining to Tor Browser using the Bulk Extractor tool.

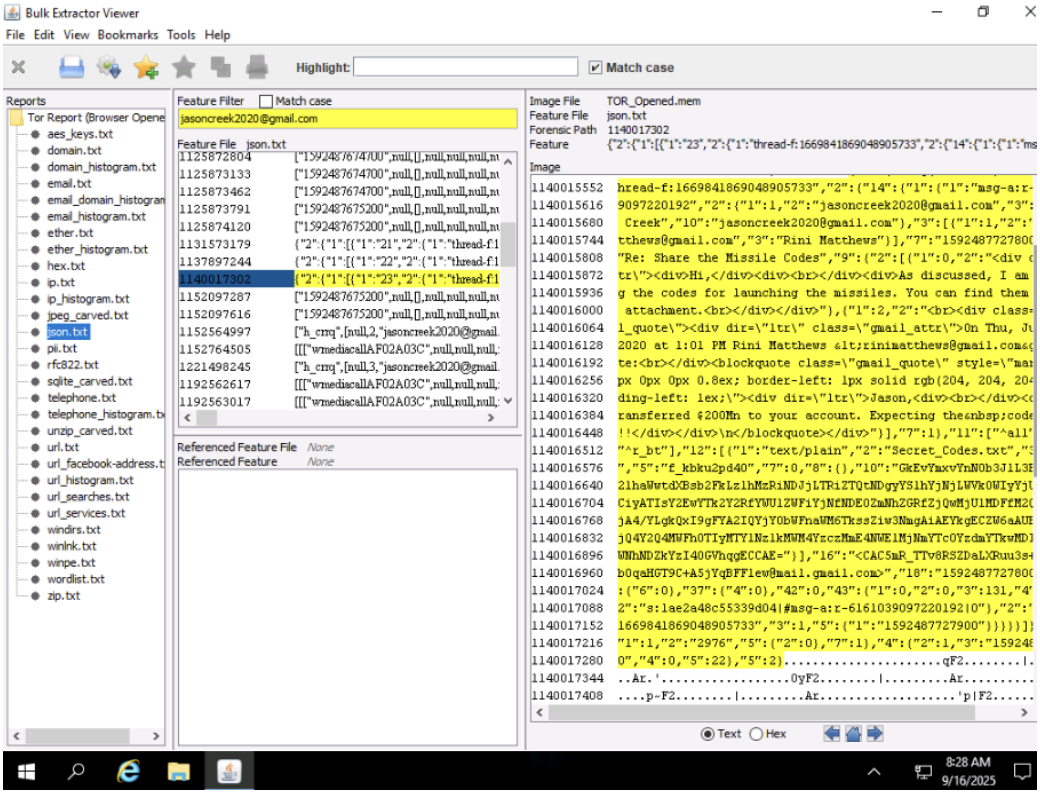
Overview of the Lab

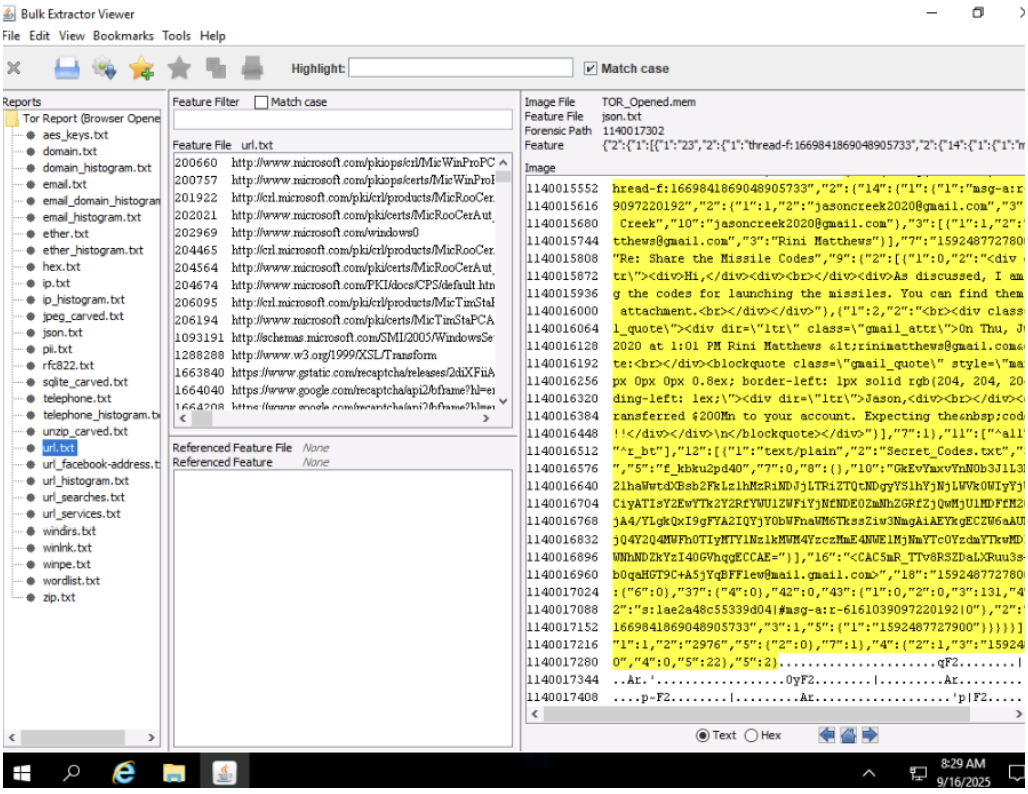
This lab familiarizes you with the process of analyzing a RAM dump containing **Tor Browser** artifacts with the help of **Bulk Extractor**.

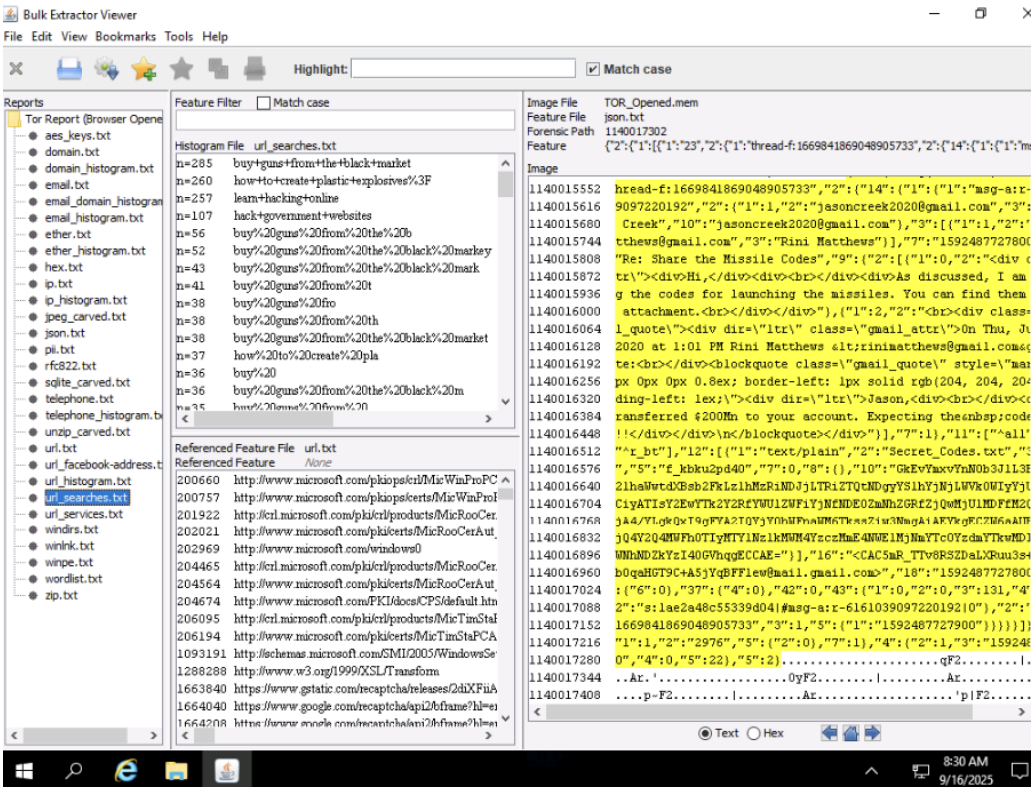


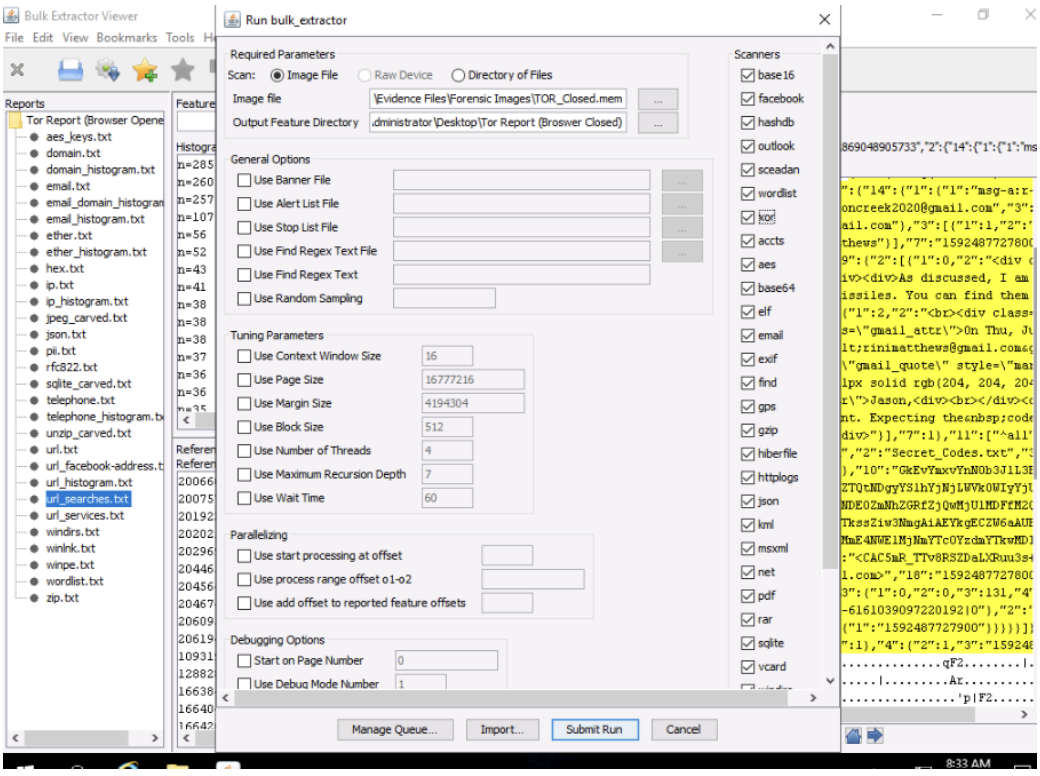

bulk_extractor Scan
Image File TOR_Opened.mem
Feature Directory Tor Report (Browser Opened)
Command
bulk_extractor -o "C:\Users\Administrator\Desktop\Tor Report (Browser Opened)" -e base16 -e facebook -e hashdb -e outlook -e sceadan -e wordlist -e xor "C:\DFE-Tools\Evidence Files\Forensic Images\TOR_C
Progress 3.12%
7:54:10 Offset 67MB (3.12%) Done in 0:17:43 at 08:11:53
bulk_extractor output
hashdb: hashdb_mode=none
WARNING: the hashdb scanner is enabled but it will not perform any action
because no mode has been selected. Please either select a hashdb mode or
leave the hashdb scanner disabled to avoid this warning.
bulk_extractor version: 1.5.5
Hostname: WIN-714MDNBUD82
Input file: C:\DFE-Tools\Evidence Files\Forensic Images\TOR_Opened.mem
Output directory: C:\Users\Administrator\Desktop\Tor Report (Browser Opened)
Disk Size: 2147483648
Threads: 4
Cancel
Close
Autopsy 4.14.0
Tor Report (Browser...
7:54 AM 9/16/2025

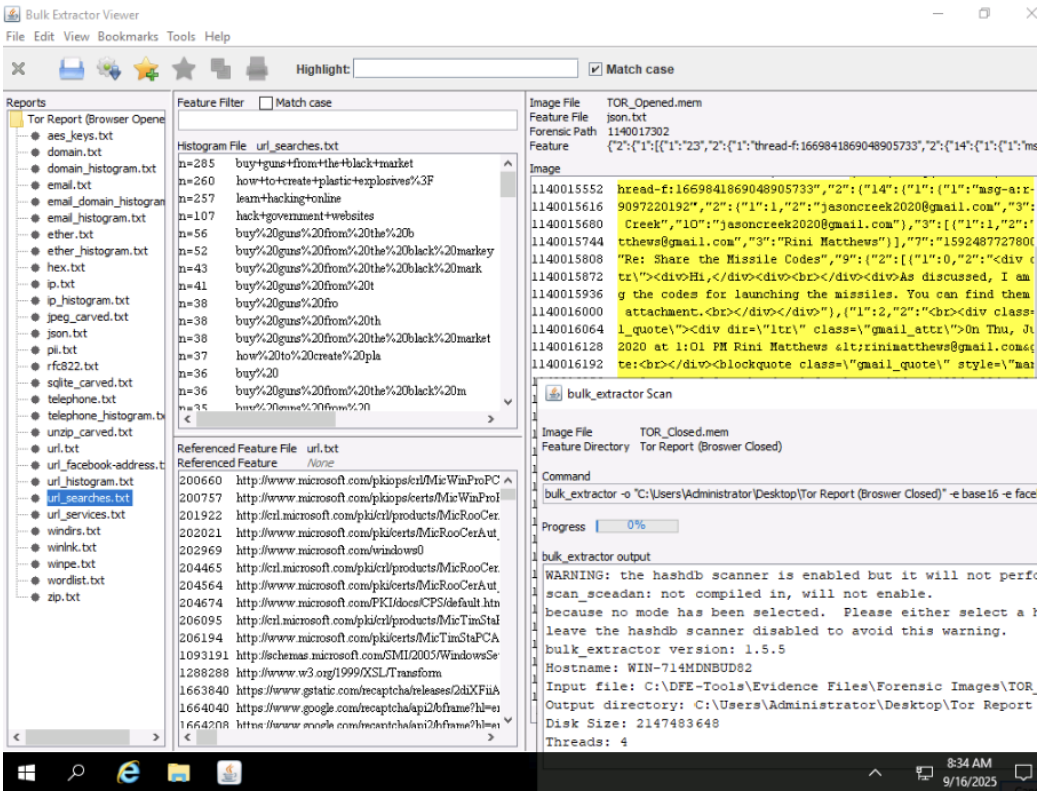

Bulk Extractor Viewer
File Edit View Bookmarks Tools Help
Highlight:
Match case
Reports
Tor Report (Browser Opene
aes_keys.txt
domain.txt
domain_histogram.txt
email.txt
email_domain_histogran
email_histogram.txt
ether.txt
ether_histogram.txt
hex.txt
ip.txt
ip_histogram.txt
jpeg_carved.txt
json.txt
pii.txt
rfc822.txt
sqlite_carved.txt
telephone.txt
telephone_histogram.tx
unzip_carved.txt
url.txt
url_facebook-address.t
url_histogram.txt
url_searches.txt
url_services.txt
windlrs.txt
winlnk.txt
winpe.txt
wordlist.txt
zip.txt
Feature Filter
Match case
jasoncreek2020@gmail.com
Feature File json.txt
691345522 [["cic:vd","111179036845712580643","je
693296303 [[1,null,null,null,null,null,null,null,nul
732824096-GZIP-7507 {\x0A "matches": [\x0A {\x
740861334 {"DpimGf":false,"EP1ykd":["/_/*"],"Fdr
827955036 {"2":{"1":[{"1":"21","2":{"1":"thread-f:1
905507049 [[["wmediscallA,F02A03C",null,null,null,
914221193 {"f":false,"d":{"1":{"1":"thread-f:166967
950937517 {"d":false,"a":23,"b":"16","c":{"1":"16","
950938047 {"d":false,"a":29,"b":"61","c":{"1":"61","
969400496-GZIP-1358 {"DpimGf":false,"EP1ykd":["
975584309 {"d":false,"a":84,"b":"17","c":{"1":"17","
1010256875 {"DpimGf":false,"EP1ykd":["/_/*"],"Fdr
1021688808-GZIP-3103 [[1,null,null,null,null,null,null,
1042546081 {"14":{"1":{"1":"msg-a:r1740123236788
Referenced Feature File None
Referenced Feature None
Image File None
Feature File None
Forensic Path None
Feature None
Image
Text
Hex
8:27 AM 9/16/2025


Bulk Extractor Viewer
File Edit View Bookmarks Tools Help
Highlight:
Match case
Reports
Tor Report (Browser Opene
aes_keys.txt
domain.txt
domain_histogram.txt
email.txt
email_domain_histogran
email_histogram.txt
ether.txt
ether_histogram.txt
hex.txt
ip.txt
ip_histogram.txt
jpeg_carved.txt
json.txt
pii.txt
rfc822.txt
sqlite_carved.txt
telephone.txt
telephone_histogram.tx
unzip_carved.txt
url.txt
url_facebook-address.t
url_histogram.txt
url_searches.txt
url_services.txt
windirs.txt
winlnk.txt
winpe.txt
wordlist.txt
zip.txt
Feature Filter
Match case
jasoncreek2020@gmail.com
Feature File json.txt
1125872804
1125873133
1125873462
1125873791
1125874120
1131573179
1137897244
1140017302
1152097287
1152097616
1152564997
1152764505
1221498245
1192562617
1192563017
Referenced Feature File None
Referenced Feature None
Image File TOR_Opened.mem
Feature File json.txt
Forensic Path 1140017302
Feature
Image
1140015552
1140015616
1140015680
1140015744
1140015808
1140015872
1140015936
1140016000
1140016064
1140016128
1140016192
1140016256
1140016320
1140016384
1140016448
1140016512
1140016576
1140016640
1140016704
1140016768
1140016832
1140016896
1140016960
1140017024
1140017088
1140017152
1140017216
1140017280
1140017344
1140017408
Text
Hex
8:28 AM
9/16/2025


Bulk Extractor Viewer
File Edit View Bookmarks Tools Help
Highlight:
Match case
Reports
Tor Report (Browser Opene
aes_keys.txt
domain.txt
domain_histogram.txt
email.txt
email_domain_histogran
email_histogram.txt
ether.txt
ether_histogram.txt
hex.txt
ip.txt
ip_histogram.txt
jpeg_carved.txt
json.txt
pii.txt
rfc822.txt
sqlite_carved.txt
telephone.txt
telephone_histogram.tx
unzip_carved.txt
url.txt
url_facebook-address.t
url_histogram.txt
url_searches.txt
url_services.txt
windirs.txt
winlnk.txt
winpe.txt
wordlist.txt
zip.txt
Feature Filter
Match case
Feature File url.txt
200660 http://www.microsoft.com/pkiops/crl/MicWinProPC
200757 http://www.microsoft.com/pkiops/certs/MicWinProI
201922 http://crl.microsoft.com/pki/crl/products/MicRooCer
202021 http://www.microsoft.com/pki/certs/MicRooCerAut
202969 http://www.microsoft.com/windows0
204465 http://crl.microsoft.com/pki/crl/products/MicRooCer
204564 http://www.microsoft.com/pki/certs/MicRooCerAut
204674 http://www.microsoft.com/PKI/docs/CPS/default.htn
206095 http://crl.microsoft.com/pki/crl/products/MicTimStaI
206194 http://www.microsoft.com/pki/certs/MicTimStaPCA
1093191 http://schemas.microsoft.com/SMI/2005/WindowsSe
1288288 http://www.w3.org/1999/XSL/Transform
1663840 https://www.gstatic.com/recaptcha/releases/2diXFiiA
1664040 https://www.google.com/recaptcha/api2/bframe?hl=e
Referenced Feature File None
Referenced Feature None
Image File TOR_Opened.mem
Feature File json.txt
Forensic Path 1140017302
Feature
Image
1140015552
1140015616
1140015680
1140015744
1140015808
1140015872
1140015936
1140016000
1140016064
1140016128
1140016192
1140016256
1140016320
1140016384
1140016448
1140016512
1140016576
1140016640
1140016704
1140016768
1140016832
1140016896
1140016960
1140017024
1140017088
1140017152
1140017216
1140017280
1140017344
1140017408
Text
Hex
8:29 AM
9/16/2025


Bulk Extractor Viewer
File Edit View Bookmarks Tools Help
Highlight:
Match case
Reports
Tor Report (Browser Opene
aes_keys.txt
domain.txt
domain_histogram.txt
email.txt
email_domain_histogran
email_histogram.txt
ether.txt
ether_histogram.txt
hex.txt
ip.txt
ip_histogram.txt
jpeg_carved.txt
json.txt
pii.txt
rfc822.txt
sqlite_carved.txt
telephone.txt
telephone_histogram.tx
unzip_carved.txt
url.txt
url_facebook-address.t
url_histogram.txt
url_searches.txt
url_services.txt
windirs.txt
winlnk.txt
winpe.txt
wordlist.txt
zip.txt
Feature Filter
Match case
Histogram File url_searches.txt
n=285 buy+guns+from+the+black+market
n=260 how+to+create+plastic+explosives%3F
n=257 learn+hacking+online
n=107 hack+government+websites
n=56 buy%20guns%20from%20the%20b
n=52 buy%20guns%20from%20the%20black%20markey
n=43 buy%20guns%20from%20the%20black%20mark
n=41 buy%20guns%20from%20t
n=38 buy%20guns%20fro
n=38 buy%20guns%20from%20th
n=38 buy%20guns%20from%20the%20black%20market
n=37 how%20to%20create%20pla
n=36 buy%20
n=36 buy%20guns%20from%20the%20black%20m
Referenced Feature File url.txt
Referenced Feature None
200660 http://www.microsoft.com/pkiops/crl/MicWinProPC
200757 http://www.microsoft.com/pkiops/certs/MicWinProI
201922 http://crl.microsoft.com/pki/crl/products/MicRooCer
202021 http://www.microsoft.com/pki/certs/MicRooCerAut
202969 http://www.microsoft.com/windows0
204465 http://crl.microsoft.com/pki/crl/products/MicRooCer
204564 http://www.microsoft.com/pki/certs/MicRooCerAut
204674 http://www.microsoft.com/PKI/docs/CPS/default.htm
206095 http://crl.microsoft.com/pki/crl/products/MicTimStaP
206194 http://www.microsoft.com/pki/certs/MicTimStaPCA
1093191 http://schemas.microsoft.com/SMI/2005/WindowsSe
1288288 http://www.w3.org/1999/XSL/Transform
1663840 https://www.gstatic.com/recaptcha/releases/2diXFiiA
1664040 https://www.google.com/recaptcha/api2/bframe?hl=e
Image File TOR_Opened.mem
Feature File json.txt
Forensic Path 1140017302
Feature {"2":{"1":[{"1":"23","2":{"1":"thread-f:1669841869048905733","2":{"14":{"1":{"1":"ms
Image
1140015552 hread-f:1669841869048905733","2":{"14":{"1":{"1":"msg-a:r-
1140015616 9097220192","2":{"1":1,"2":"jasoncreek2020@gmail.com","3":
1140015680 Creek","10":"jasoncreek2020@gmail.com"},"3":[{"1":1,"2":"
1140015744 tthews@gmail.com","3":"Rini Matthews"}],"7":"159248772780
1140015808 "Re: Share the Missile Codes","9":{"2":[{"1":0,"2":"<div
1140015872 tr\"> Hi,
 As discussed, I am
1140015936 g the codes for launching the missiles. You can find them
1140016000 attachment.
 "),{"1":2,"2":"
<div class=
1140016064 l_quote\"><div dir=\"ltr\" class=\"gmail_attr\">On Thu, Ju
1140016128 2020 at 1:01 PM Rini Matthews <rinimatthews@gmail.com&
1140016192 te:
 <blockquote class=\"gmail_quote\" style=\"ma
1140016256 px 0px 0px 0.8ex; border-left: 1px solid rgb(204, 204, 204
1140016320 ding-left: 1ex;\"><div dir=\"ltr\">Jason,
 <
1140016384 ransferred $200Mn to your account. Expecting the code
1140016448 !! \n</blockquote> "}],"7":1},"11":["^all"
1140016512 "^r_bt"],"12":[{"1":"text/plain","2":"Secret_Codes.txt","3
1140016576 ","5":"f_kbku2pd40","7":0,"8":{},"10":"GkEvYmxvYnN0b3J1L3E
1140016640 2lhaWwtdXBsb2FkLzlhMzRiNDJjLTRiZTQtNDgyYS1hYjNjLWVk0WIyYjl
1140016704 CiyATIsY2EwYTk2Y2RfYWU1ZWFiYjNtNDE0ZmNhZGRfZjQwMjUlMDFfM2(
1140016768 jA4/YLgkQxT9gFYA2TQYjY0hWFmaWM6TkssZiw3NmgAiAEYkgECZW6aUE
1140016832 jQ4Y2Q4MWFh0TIyMTY1NzlkMWM4YzczMmE4NWE1MjNmYTc0YzdmYTkwMDJ
1140016896 WNhNDZkYzI40GVhqgECCAE="}],"16":"<CAC5mR_TTv8RSZDaLXRuu3s+
1140016960 b0qaHGT9C+A5jYqBFFlew@mail.gmail.com>","18":"1592487727800
1140017024 :{"6":0},"37":{"4":0},"42":0,"43":{"1":0,"2":0,"3":131,"4"
1140017088 2":"s:lae2a48c55339d04|#msg-a:r-6161039097220192|0"},"2":"
1140017152 16698418690489057 33","3":1,"5":{"1":"1592487727900"}}}}}]}
1140017216 "1":1,"2":"2976","5":{"2":0},"7":1},"4":{"2":1,"3":"159248
1140017280 0","4":0,"5":22},"5":2}.....qF2.....|.
1140017344 ..Ar.'.....0yF2.....|.....Ar.....
1140017408 ....p-F2.....|.....Ar.....'p|F2.....
Text Hex
8:30 AM
9/16/2025


Bulk Extractor Viewer
Run bulk_extractor
Required Parameters
Scan: Image File Raw Device Directory of Files
Image file \Evidence Files\Forensic Images\TOR_Closed.mem
Output Feature Directory dministrator\Desktop\Tor Report (Broswer Closed)
General Options
Use Banner File
Use Alert List File
Use Stop List File
Use Find Regex Text File
Use Find Regex Text
Use Random Sampling
Tuning Parameters
Use Context Window Size 16
Use Page Size 16777216
Use Margin Size 4194304
Use Block Size 512
Use Number of Threads 4
Use Maximum Recursion Depth 7
Use Wait Time 60
Parallelizing
Use start processing at offset
Use process range offset o1-o2
Use add offset to reported feature offsets
Debugging Options
Start on Page Number 0
Use Debug Mode Number 1
Scanners
base16
facebook
hashdb
outlook
sceadan
wordlist
kor
accts
aes
base64
elf
email
exif
find
gps
gzip
hiberfile
httplogs
json
kml
msxml
net
pdf
rar
sqlite
vcard
Manage Queue...
Import...
Submit Run
Cancel



Analyzing RAM Dumps to Retrieve TOR Browser Artifacts

Lab Scenario:

During an investigation of internet-based fraud and dark web criminal activity, law enforcement seized computers from suspects involved in illegal activities, including drug trafficking. Tor Browser usage was suspected, and forensic investigators needed to extract evidence from the suspect machines. RAM dumps of the systems were acquired to retrieve artifacts related to Tor Browser, even in cases where the browser had been uninstalled or removed.

Lab Objectives:

- Discover Tor Browser activity on a Windows machine using prefetch files and the netstat command.
- Analyze RAM dumps to retrieve Tor Browser artifacts, including websites visited, email access, and other user activity.
- Understand dark web forensics techniques for investigating criminal activity facilitated through Tor Browser.

Overview of the Lab:
This lab focused on using **Bulk Extractor** to analyze RAM dumps and extract Tor Browser artifacts. The process included:

- Locating Tor Browser prefetch files using **WinPrefetchView** to confirm prior usage.
- Running **Bulk Extractor** to scan memory dumps and generate reports for "Browser Opened" and "Browser Closed" states.
- Examining specific output files such as domain.txt to identify visited domains, including multiple Gmail accesses.
- Interpreting artifacts to construct a timeline of user activity on Tor Browser.

Lab Challenges:
Due to lab time restrictions and limits on extended session allowances, the RAM dump extraction could not be fully completed. Download times for the tools and the progress time for bulk extraction exceeded the maximum allowed lab time. As a result, the lab could not be fully finalized, but key steps were executed to demonstrate the methodology for recovering Tor Browser activity from RAM dumps.