Module 06: Windows Forensics

Lab Scenario

A computer forensics examiner, Steve, was called to investigate the laptop of a 26-year-old man who was arrested. Steve started searching the contents of the laptop. He began his investigation on Windows® event logs and processes using various Windows forensic tools. He checked all the registries, event logs, and processes for evidence of any crimes. During the investigation, Steve found the paths for several images and videos of child pornography. He checked all the pictures and confirmed the existence of child pornography on the laptop. Other evidence on the laptop proved that the man in custody was its primary user.

Lab Objectives

The goal of this lab is to explain the process of finding pieces of evidence from Windows OSes. Evidence in Windows OSes includes Windows memory analysis, volatile and non-volatile information, Windows event logs, Windows processes, search key values, and other data. Accomplishing this task will entail the following:

- Acquiring and investigating volatile memory contents of a Windows system
- Analyzing the Windows registry
- Examining forensic artifacts from web browsers
- Investigating loaded processes on a live computer

Overview of Windows Forensics

Windows forensics refers to investigation of cyber-crimes involving Windows machines. It involves gathering of evidence from a Windows machine so that the perpetrator(s) of a cyber-crime can be identified and prosecuted. Investigators performing forensics on Windows machines must have a thorough understanding of the various components of a Windows OS such as the file system, registries, system files, and event logs where they can find data of evidentiary value.

Lab Tasks

Recommended labs to assist you in Windows forensics:

- Acquiring volatile information from a live Windows system
- Investigating forensic image of Windows RAM
- Examining web browser artifacts

- Extracting information about loaded processes on a computer

Lab 1: Acquiring Volatile Information from a Live Windows System

Lab Scenario

For forensics investigation, investigators often need to gather data from a live Windows system to analyze details such as network information and process information by using different tools (command-line tools as well as GUI-based tools). Performing a thorough analysis will enable investigators to obtain vital evidence, which helps them solve various cases related to digital forensics.

As a forensics investigator, you should know how to collect volatile information from a live system.

Lab Objectives

Acquiring volatile information from a live system involves obtaining information such as network information and process information about an OS.

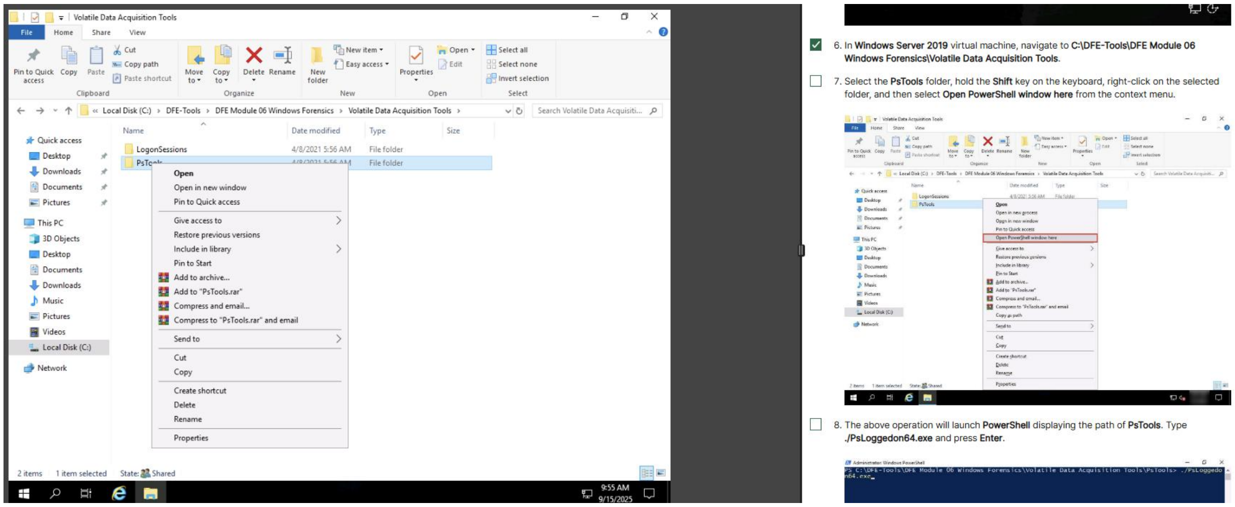
The objective of this lab is to help you collect volatile information from a live Windows system.

Overview of the Lab

This lab familiarizes you with the procedures to collect volatile information from a host computer running on a Windows OS by using tools such as **PsTools** and **LogonSessions**.

In **Windows Server 2019** virtual machine, navigate to **C:\DFE-Tools\DFE Module 06 Windows Forensics\Volatile Data Acquisition Tools**.

Select the **PsTools** folder, hold the **Shift** key on the keyboard, right-click on the selected folder, and then select **Open PowerShell window here** from the context menu.



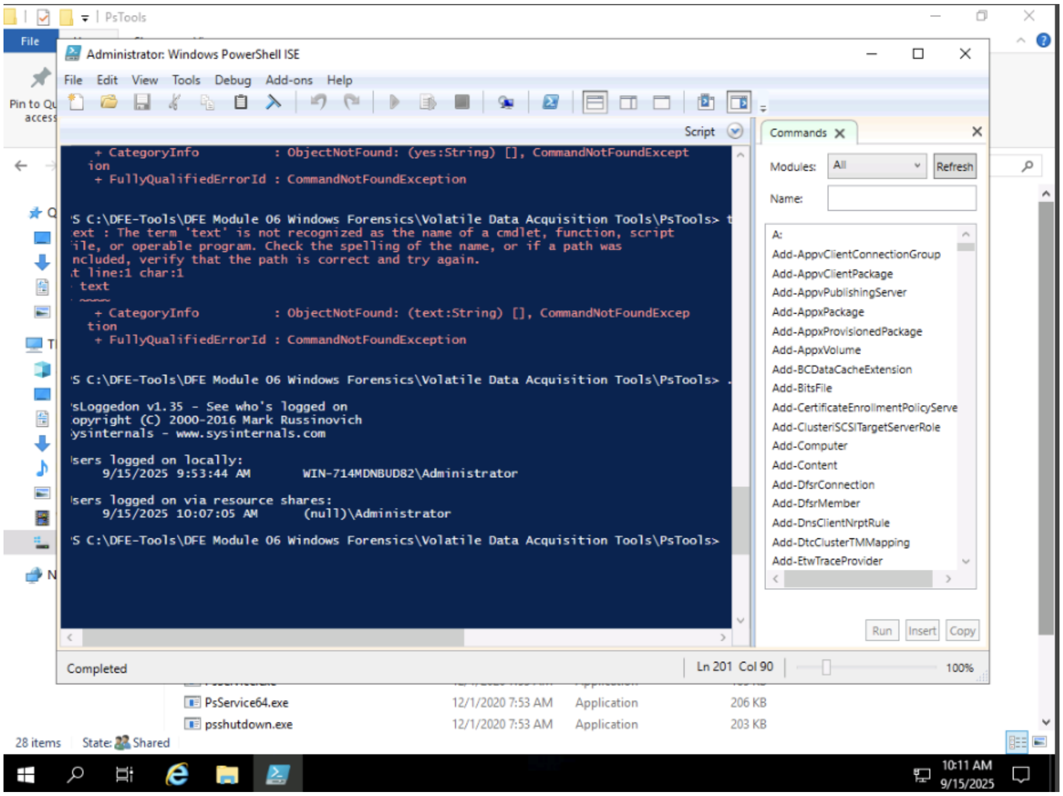
☑ 6. In **Windows Server 2019** virtual machine, navigate to **C:\DFE-Tools\DFE Module 06 Windows Forensics\Volatile Data Acquisition Tools**.

□ 7. Select the **PsTools** folder, hold the **Shift** key on the keyboard, right-click on the selected folder, and then select **Open PowerShell window here** from the context menu.

□ 8. The above operation will launch **PowerShell** displaying the path of **PsTools**. Type **./PsLoggedon64.exe** and press **Enter**.

```
PS C:\DFE-Tools\DFE Module 06 Windows Forensics\Volatile Data Acquisition Tools\PsTools> ./PsLoggedo
n64.exe_
```

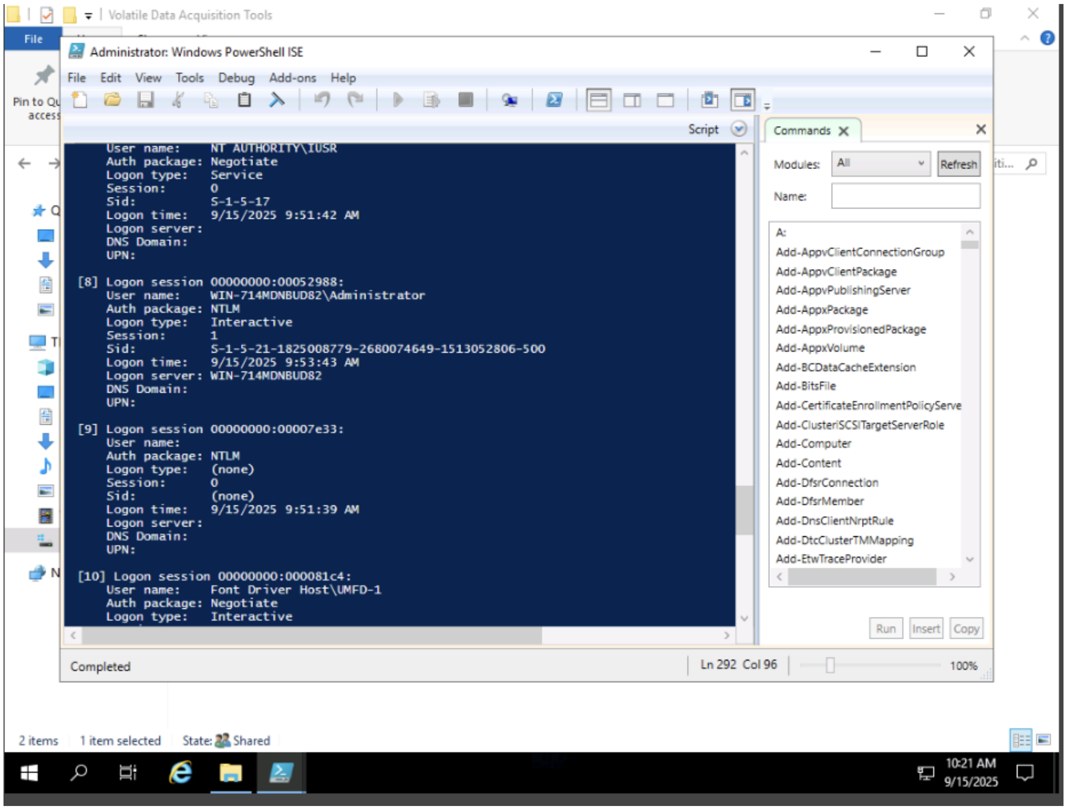
Attempted to run PsLoggedon64.exe from the PsTools folder. The tool may not have executed as expected due to environment or file differences. This demonstrates the process of launching volatile data acquisition tools in Windows.



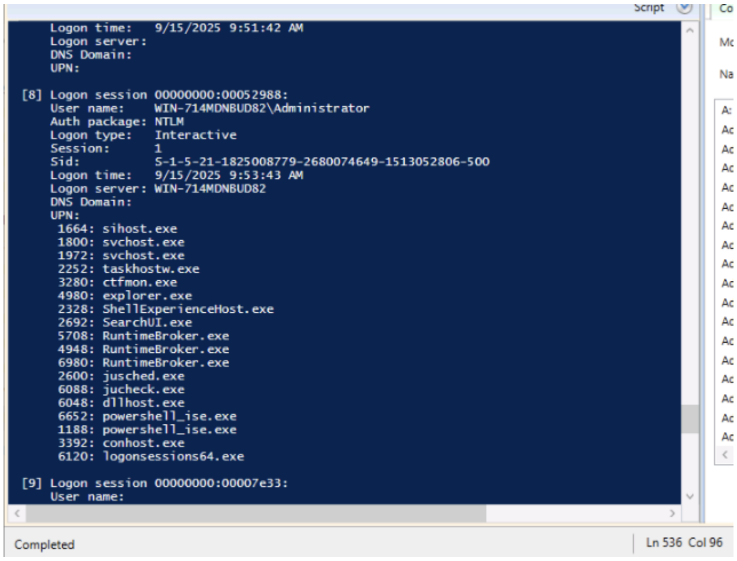
```
   + CategoryInfo          : ObjectNotFound: (yes:String) [], CommandNotFoundExcept
  ion
   + FullyQualifiedErrorId : CommandNotFoundException


'S C:\DFE-Tools\DFE Module 06 Windows Forensics\Volatile Data Acquisition Tools\PsTools> t
ext : The term 'text' is not recognized as the name of a cmdlet, function, script
ile, or operable program. Check the spelling of the name, or if a path was
ncluded, verify that the path is correct and try again.
t line:1 char:1
 text
 ~~~~
   + CategoryInfo          : ObjectNotFound: (text:String) [], CommandNotFoundExcep
  tion
   + FullyQualifiedErrorId : CommandNotFoundException


'S C:\DFE-Tools\DFE Module 06 Windows Forensics\Volatile Data Acquisition Tools\PsTools> .

'sLoggedon v1.35 - See who's logged on
opyright (C) 2000-2016 Mark Russinovich
ysinternals - www.sysinternals.com

'sers logged on locally:
     9/15/2025 9:53:44 AM       WIN-714MDNBUD82\Administrator

'sers logged on via resource shares:
     9/15/2025 10:07:05 AM      (null)\Administrator

'S C:\DFE-Tools\DFE Module 06 Windows Forensics\Volatile Data Acquisition Tools\PsTools>
```

A:
Add-AppvClientConnectionGroup
Add-AppvClientPackage
Add-AppvPublishingServer
Add-AppxPackage
Add-AppxProvisionedPackage
Add-AppxVolume
Add-BCDataCacheExtension
Add-BitsFile
Add-CertificateEnrollmentPolicyServe
Add-ClusteriSCSITargetServerRole
Add-Computer
Add-Content
Add-DfsrConnection
Add-DfsrMember
Add-DnsClientNrptRule
Add-DtcClusterTMMapping
Add-EtwTraceProvider

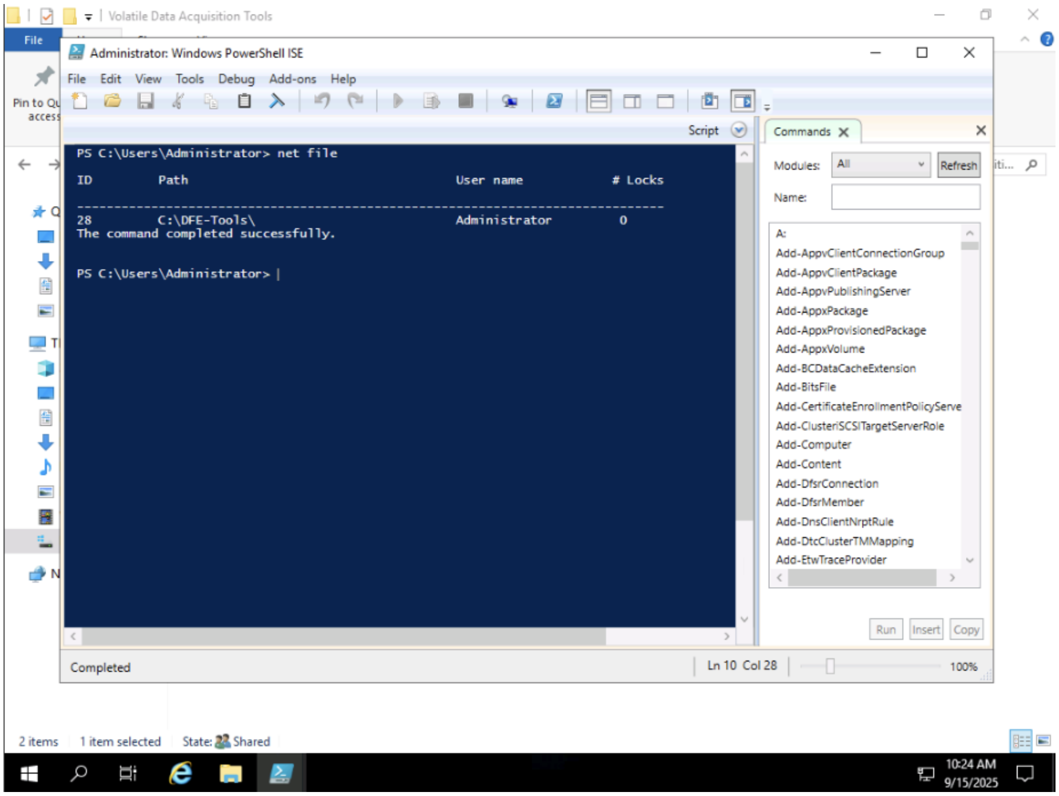
PsService64.exe	12/1/2020 7:53 AM	Application	206 KB
psshutdown.exe	12/1/2020 7:53 AM	Application	203 KB



```
    User name:    NT AUTHORITY\IUSR
    Auth package: Negotiate
    Logon type:   Service
    Session:      0
    Sid:          S-1-5-17
    Logon time:   9/15/2025 9:51:42 AM
    Logon server:
    DNS Domain:
    UPN:

[8] Logon session 00000000:00052988:
    User name:    WIN-714MDNBUD82\Administrator
    Auth package: NTLM
    Logon type:   Interactive
    Session:      1
    Sid:          S-1-5-21-1825008779-2680074649-1513052806-500
    Logon time:   9/15/2025 9:53:43 AM
    Logon server: WIN-714MDNBUD82
    DNS Domain:
    UPN:

[9] Logon session 00000000:00007e33:
    User name:
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          (none)
    Logon time:   9/15/2025 9:51:39 AM
    Logon server:
    DNS Domain:
    UPN:

[10] Logon session 00000000:000081c4:
    User name:    Font Driver Host\UMFD-1
    Auth package: Negotiate
    Logon type:   Interactive
```



```
    Logon time:   9/15/2025 9:51:42 AM
    Logon server:
    DNS Domain:
    UPN:

[8] Logon session 00000000:00052988:
    User name:    WIN-714MDNBUD82\Administrator
    Auth package: NTLM
    Logon type:   Interactive
    Session:      1
    Sid:          S-1-5-21-1825008779-2680074649-1513052806-500
    Logon time:   9/15/2025 9:53:43 AM
    Logon server: WIN-714MDNBUD82
    DNS Domain:
    UPN:
     1664: sihost.exe
     1800: svchost.exe
     1972: svchost.exe
     2252: taskhostw.exe
     3280: ctfmon.exe
     4980: explorer.exe
     2328: ShellExperienceHost.exe
     2692: SearchUI.exe
     5708: RuntimeBroker.exe
     4948: RuntimeBroker.exe
     6980: RuntimeBroker.exe
     2600: jusched.exe
     6088: jucheck.exe
     6048: dllhost.exe
     6652: powershell_ise.exe
     1188: powershell_ise.exe
     3392: conhost.exe
     6120: logonsessions64.exe

[9] Logon session 00000000:00007e33:
    User name:
```



```
PS C:\Users\Administrator> net file
ID         Path                                     User name          # Locks

-------------------------------------------------------------------------------
28         C:\DFE-Tools\                            Administrator          0
The command completed successfully.

PS C:\Users\Administrator> |
```

Lab 2: Investigating Forensic Image of Windows RAM

Lab Scenario

An investment-banking firm discovered that confidential information pertaining to its trade secrets has been compromised. The firm consulted its expert forensic investigator to determine the source and cause of this data breach. The firm uses Windows systems to store all its data. The investigator needs to find out if there are any malicious processes running on the firm's restricted systems that store confidential data. To do so, the investigator must examine the RAM contents of the Windows machines to identify any malicious behavior.

To be an expert forensic investigator, you must know how to detect malicious processes running on a system by using the appropriate tools.

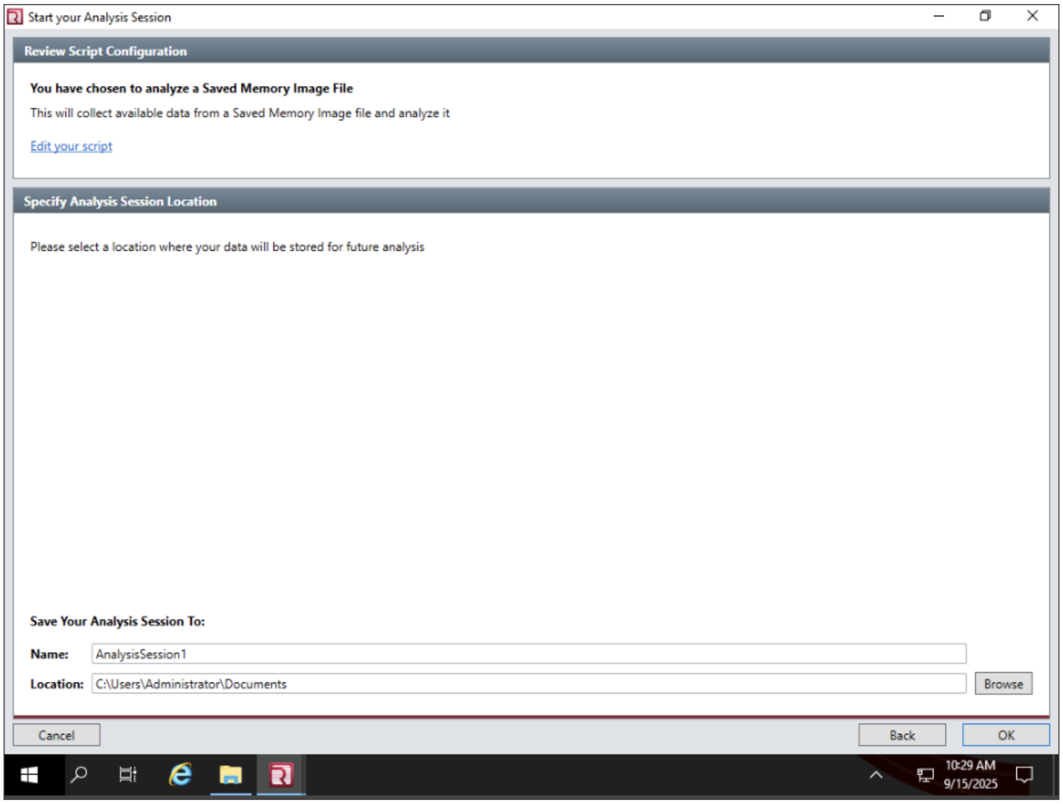
Lab Objectives

Analyzing the RAM dump of a system helps investigators retrieve valuable evidence pertaining to a case of cyber-crime.

The objective of this lab is to analyze the RAM dump of a Windows machine by using the Redline utility and Volatility framework.

Overview of the Lab

This lab familiarizes you with the examination of Windows memory dumps using the Redline utility and Volatility framework. The examination involves investigating and identifying attacks or malicious behavior that occurred on the target machine.



Start your Analysis Session

Review Script Configuration

You have chosen to analyze a Saved Memory Image File

This will collect available data from a Saved Memory Image file and analyze it

Edit your script

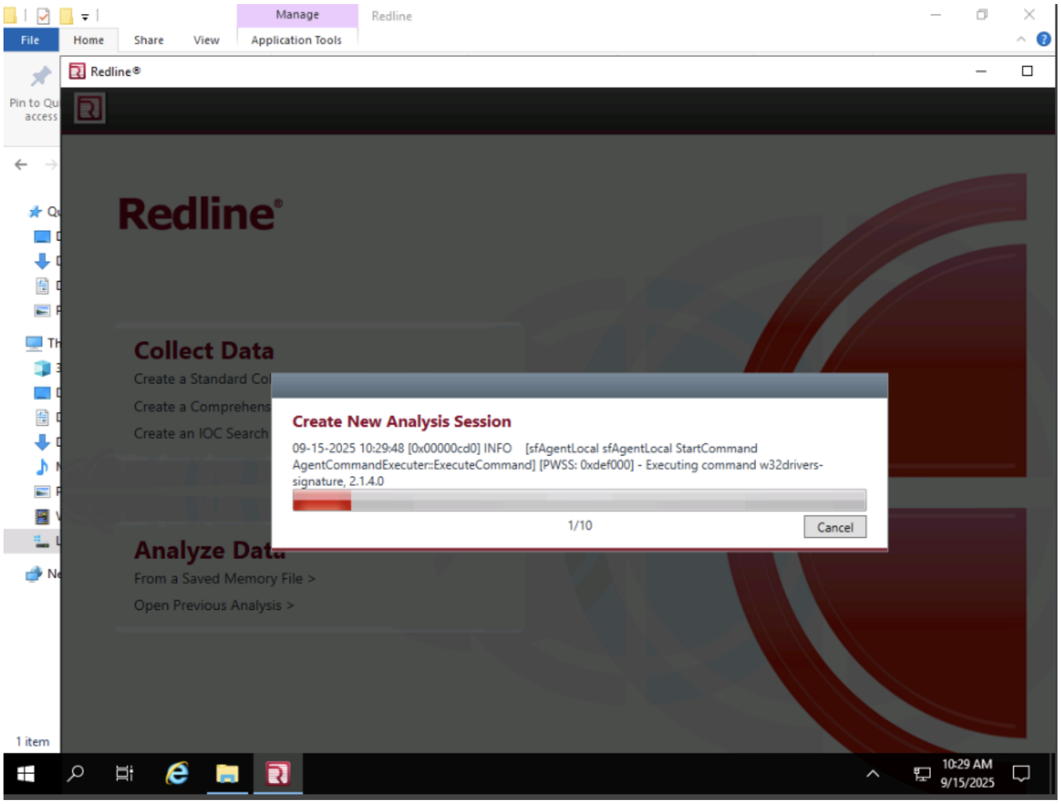
Specify Analysis Session Location

Please select a location where your data will be stored for future analysis

Save Your Analysis Session To:

Name: AnalysisSession1

Location: C:\Users\Administrator\Documents

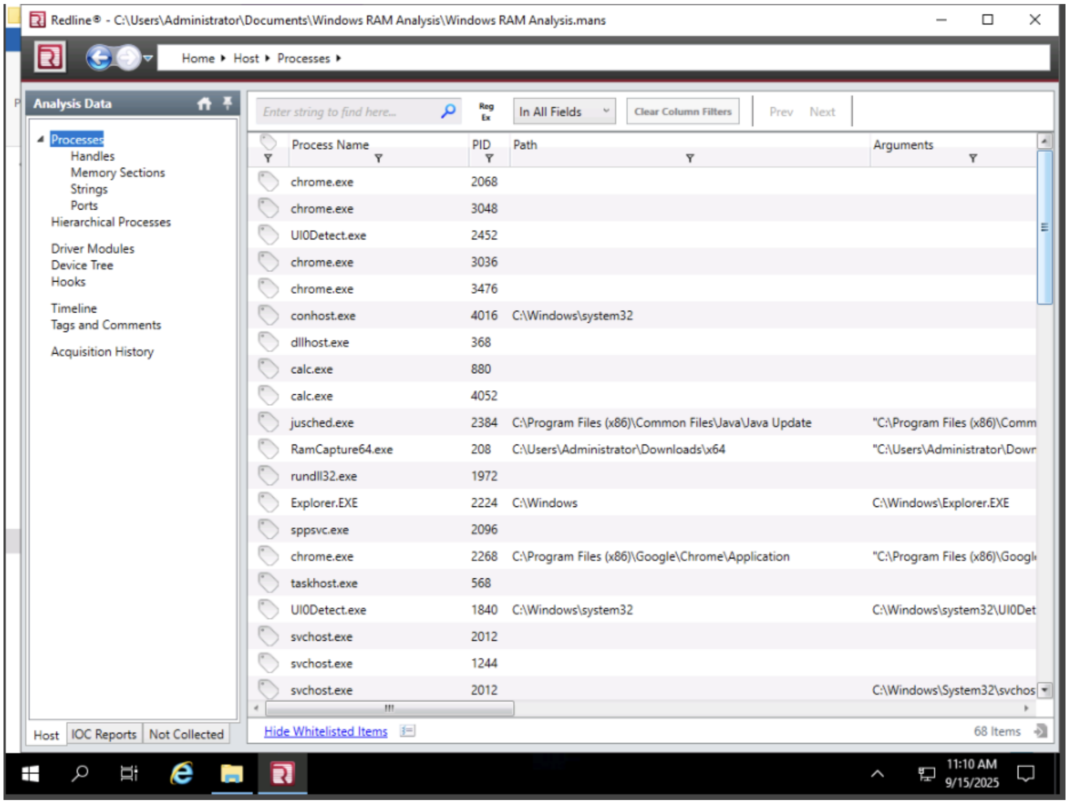


Create New Analysis Session

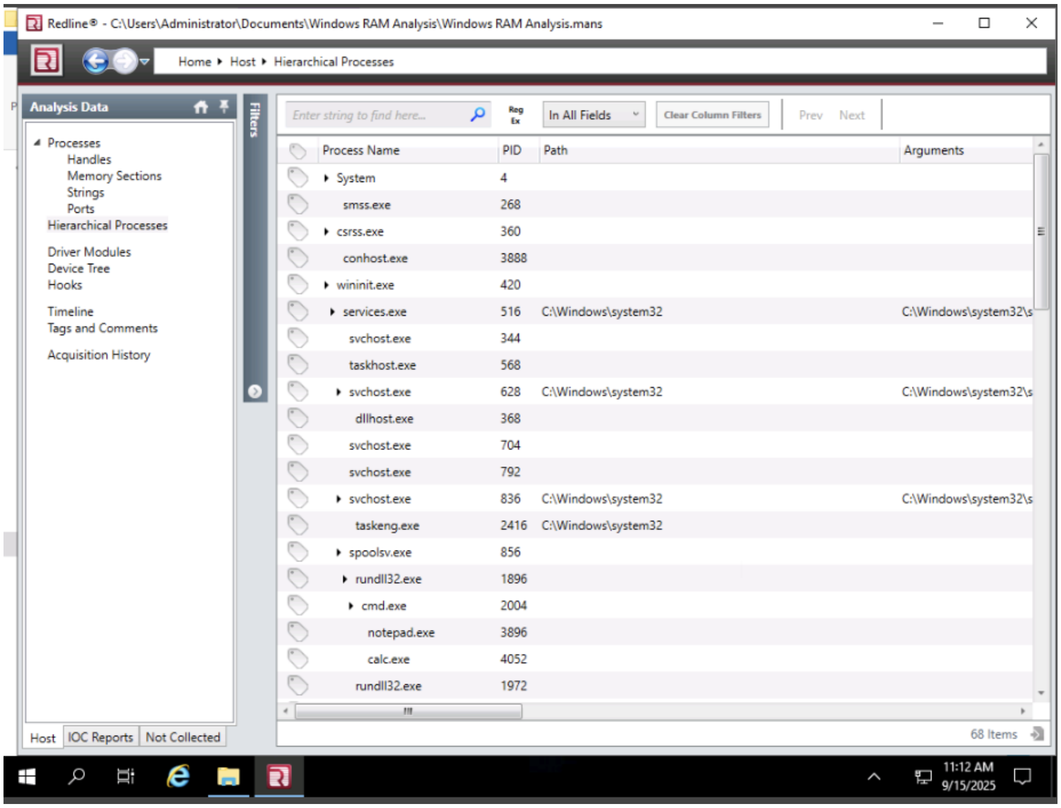
```
09-15-2025 10:29:48 [0x00000cd0] INFO    [sfAgentLocal sfAgentLocal StartCommand
AgentCommandExecuter::ExecuteCommand] [PWSS: 0xdef000] - Executing command w32drivers-
signature, 2.1.4.0
```

1/10

Cancel



Process Name	PID	Path	Arguments
chrome.exe	2068		
chrome.exe	3048		
UI0Detect.exe	2452		
chrome.exe	3036		
chrome.exe	3476		
conhost.exe	4016	C:\Windows\system32	
dllhost.exe	368		
calc.exe	880		
calc.exe	4052		
jusched.exe	2384	C:\Program Files (x86)\Common Files\Java\Java Update	"C:\Program Files (x86)\Comm
RamCapture64.exe	208	C:\Users\Administrator\Downloads\x64	"C:\Users\Administrator\Dowr
rundll32.exe	1972		
Explorer.EXE	2224	C:\Windows	C:\Windows\Explorer.EXE
sppsvc.exe	2096		
chrome.exe	2268	C:\Program Files (x86)\Google\Chrome\Application	"C:\Program Files (x86)\Googl
taskhost.exe	568		
UI0Detect.exe	1840	C:\Windows\system32	C:\Windows\system32\UI0Det
svchost.exe	2012		
svchost.exe	1244		
svchost.exe	2012		C:\Windows\System32\svchos



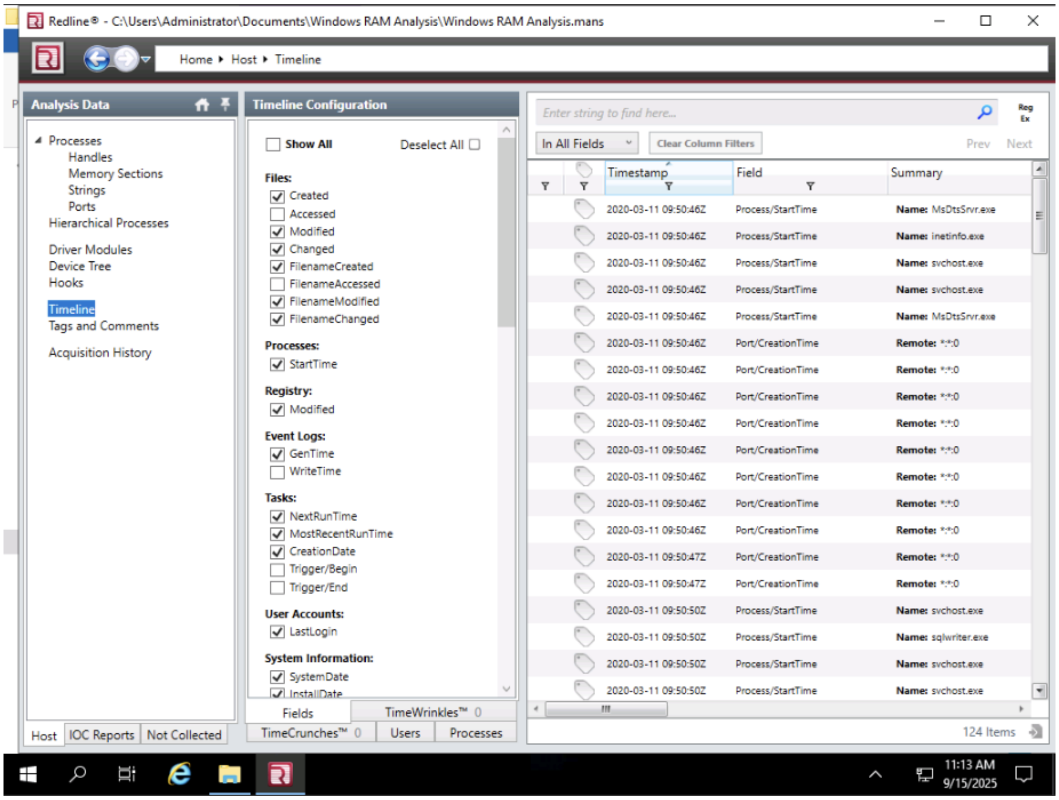
Redline® - C:\Users\Administrator\Documents\Windows RAM Analysis\Windows RAM Analysis.mans

Home ▸ Host ▸ Hierarchical Processes

Process Name	PID	Path	Arguments
▸ System	4		
smss.exe	268		
▸ csrss.exe	360		
conhost.exe	3888		
▸ wininit.exe	420		
▸ services.exe	516	C:\Windows\system32	C:\Windows\system32\s
svchost.exe	344		
taskhost.exe	568		
▸ svchost.exe	628	C:\Windows\system32	C:\Windows\system32\s
dllhost.exe	368		
svchost.exe	704		
svchost.exe	792		
▸ svchost.exe	836	C:\Windows\system32	C:\Windows\system32\s
taskeng.exe	2416	C:\Windows\system32	
▸ spoolsv.exe	856		
▸ rundll32.exe	1896		
▸ cmd.exe	2004		
notepad.exe	3896		
calc.exe	4052		
rundll32.exe	1972		

68 Items

11:12 AM
9/15/2025



Redline® - C:\Users\Administrator\Documents\Windows RAM Analysis\Windows RAM Analysis.mans

Home ▸ Host ▸ Timeline

Timeline Configuration

□ Show All Deselect All □

Files:
☑ Created
□ Accessed
☑ Modified
☑ Changed
☑ FilenameCreated
□ FilenameAccessed
☑ FilenameModified
☑ FilenameChanged

Processes:
☑ StartTime

Registry:
☑ Modified

Event Logs:
☑ GenTime
□ WriteTime

Tasks:
☑ NextRunTime
☑ MostRecentRunTime
☑ CreationDate
□ Trigger/Begin
□ Trigger/End

User Accounts:
☑ LastLogin

System Information:
☑ SystemDate
☑ InstallDate

Timestamp	Field	Summary
2020-03-11 09:50:46Z	Process/StartTime	**Name:** MsDtsSrvr.exe
2020-03-11 09:50:46Z	Process/StartTime	**Name:** inetinfo.exe
2020-03-11 09:50:46Z	Process/StartTime	**Name:** svchost.exe
2020-03-11 09:50:46Z	Process/StartTime	**Name:** svchost.exe
2020-03-11 09:50:46Z	Process/StartTime	**Name:** MsDtsSrvr.exe
2020-03-11 09:50:46Z	Port/CreationTime	**Remote:** *:*:0
2020-03-11 09:50:46Z	Port/CreationTime	**Remote:** *:*:0
2020-03-11 09:50:46Z	Port/CreationTime	**Remote:** *:*:0
2020-03-11 09:50:46Z	Port/CreationTime	**Remote:** *:*:0
2020-03-11 09:50:46Z	Port/CreationTime	**Remote:** *:*:0
2020-03-11 09:50:46Z	Port/CreationTime	**Remote:** *:*:0
2020-03-11 09:50:46Z	Port/CreationTime	**Remote:** *:*:0
2020-03-11 09:50:46Z	Port/CreationTime	**Remote:** *:*:0
2020-03-11 09:50:47Z	Port/CreationTime	**Remote:** *:*:0
2020-03-11 09:50:47Z	Port/CreationTime	**Remote:** *:*:0
2020-03-11 09:50:50Z	Process/StartTime	**Name:** svchost.exe
2020-03-11 09:50:50Z	Process/StartTime	**Name:** sqlwriter.exe
2020-03-11 09:50:50Z	Process/StartTime	**Name:** svchost.exe
2020-03-11 09:50:50Z	Process/StartTime	**Name:** svchost.exe

124 Items

11:13 AM
9/15/2025

Module 06: Windows Memory Forensics (Lab Attempted)

Objective:
The purpose of this lab was to analyze a Windows RAM image to identify active and historical processes, network connections, and other volatile data using the Volatility Framework and associated tools.

Tools Attempted:

- Volatility 2.6 (standalone Windows executable)
- PowerShell ISE
- PsLoggedon (Sysinternals)
- Windows_RAM.mem forensic image

Summary of Work:

- Navigated to the Volatility folder in the lab environment.
- Attempted to run the imageinfo plugin in Volatility to gather RAM image metadata.
- Attempted to use kdbgscan for suggested profiles.
- Attempted to identify active processes and network connections using netscan and pslist plugins.
- Encountered multiple runtime issues: path errors, command recognition issues in PowerShell, and inability to execute certain commands due to environment constraints.
- Successfully ran PsLoggedon, which returned the local administrator user and no active resource share connections.

Learning Outcomes:

- Practiced navigating PowerShell and lab directory structures for memory forensics.
- Learned how to locate and attempt to analyze RAM images using Volatility.
- Gained familiarity with expected output from imageinfo, kdbgscan, netscan, and pslist.
- Documented troubleshooting steps and errors encountered for future reference.

Notes:

- Lab was not completed due to environmental limitations and tool execution errors.

- Screenshots of attempted commands and results are included to document the investigative process.
- If this lab were fully operational, subsequent steps would include process tree analysis, file and registry handles retrieval, and identification of suspicious processes such as rundll32.exe.

Lab 3: Examining Web Browser Artifacts

Lab Scenario

Stuart is an employee at a technology firm. His company witnessed a dip in his performance over a period and found his conduct at the workplace to be extremely suspicious. They consulted an expert forensic investigator to examine Stuart's workstation. As part of the investigation, the investigator must examine the caches, cookies, and browsing history stored in the browser(s) used on the suspect's workstation. Examining and analyzing caches, cookies, and browsing history can help an investigator gather valuable evidence to solve a case of cyber-crime.

To be an expert forensic investigator, you must know how to examine and analyze the browsing history, cookies, and caches stored in browsers.

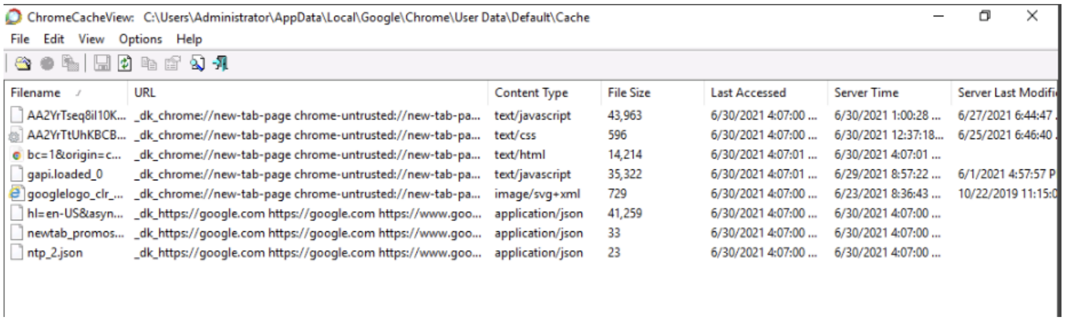
Lab Objectives

The history, cookies, and cache of a browser store important data pertaining to users' browsing activities. In the event of a cyber-crime, investigating the history, cookies, and cache of web browser(s) helps investigators retrieve valuable artifacts to solve the case.

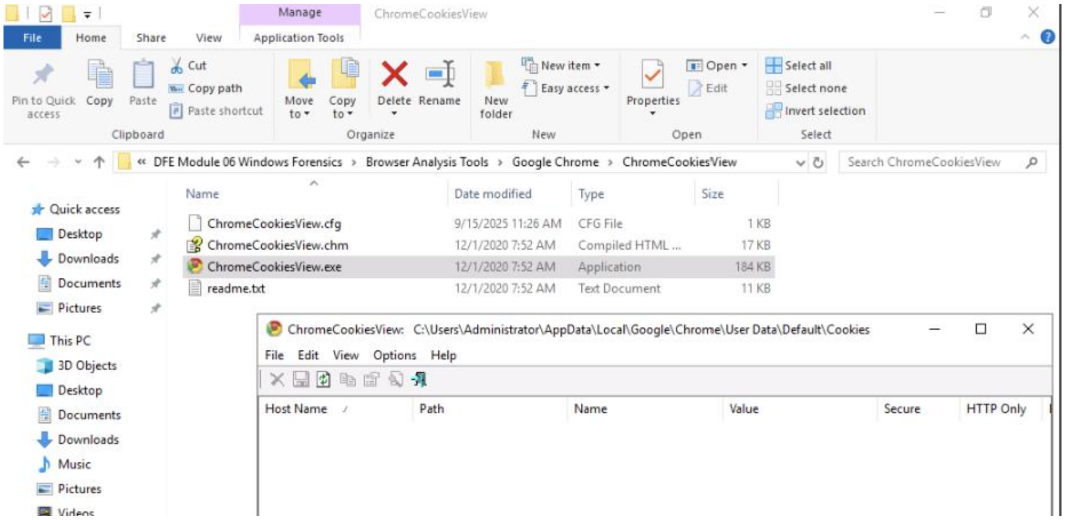
The objective of this lab is to investigate and extract web-browser artifacts such as browsing history, cookies, and cache.

Overview of the Lab

This lab familiarizes you with the tools **ChromeCacheView**, **ChromeHistoryView** and **ChromeCookiesView** and helps you understand how to retrieve artifacts pertaining to cache files, browsing history, and cookies from **Google Chrome** browser.


ChromeCacheView: C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modifi
AA2YrTseq8il10K...	_dk_chrome://new-tab-page chrome-untrusted://new-tab-pa...	text/javascript	43,963	6/30/2021 4:07:00 ...	6/30/2021 1:00:28 ...	6/27/2021 6:44:47
AA2YrTtUhKBCB...	_dk_chrome://new-tab-page chrome-untrusted://new-tab-pa...	text/css	596	6/30/2021 4:07:00 ...	6/30/2021 12:37:18...	6/25/2021 6:46:40
bc=1&origin=c...	_dk_chrome://new-tab-page chrome-untrusted://new-tab-pa...	text/html	14,214	6/30/2021 4:07:01 ...	6/30/2021 4:07:01 ...	
gapi.loaded_0	_dk_chrome://new-tab-page chrome-untrusted://new-tab-pa...	text/javascript	35,322	6/30/2021 4:07:01 ...	6/29/2021 8:57:22 ...	6/1/2021 4:57:57 P
googlelogo_clr_...	_dk_chrome://new-tab-page chrome-untrusted://new-tab-pa...	image/svg+xml	729	6/30/2021 4:07:00 ...	6/23/2021 8:36:43 ...	10/22/2019 11:15:0
hl=en-US&asyn...	_dk_https://google.com https://google.com https://www.goo...	application/json	41,259	6/30/2021 4:07:00 ...	6/30/2021 4:07:00 ...	
newtab_promos...	_dk_https://google.com https://google.com https://www.goo...	application/json	33	6/30/2021 4:07:00 ...	6/30/2021 4:07:00 ...	
ntp_2.json	_dk_https://google.com https://google.com https://www.goo...	application/json	23	6/30/2021 4:07:00 ...	6/30/2021 4:07:00 ...	



« DFE Module 06 Windows Forensics › Browser Analysis Tools › Google Chrome › ChromeCookiesView

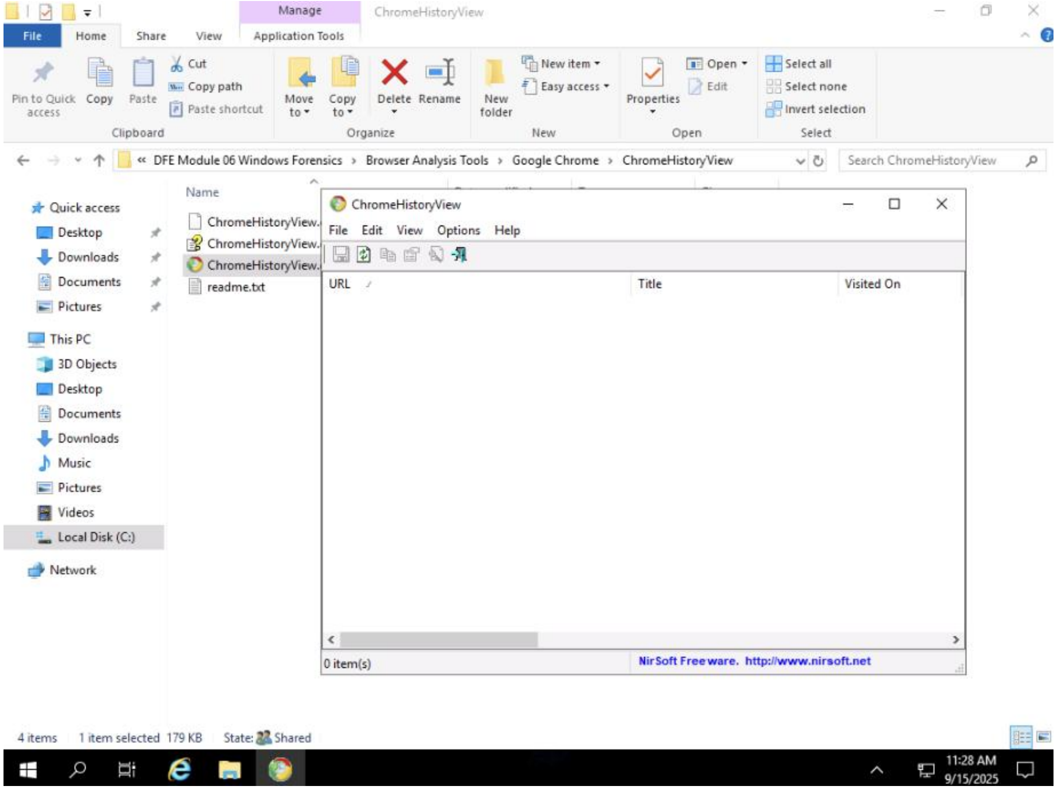
Name	Date modified	Type	Size
ChromeCookiesView.cfg	9/15/2025 11:26 AM	CFG File	1 KB
ChromeCookiesView.chm	12/1/2020 7:52 AM	Compiled HTML ...	17 KB
ChromeCookiesView.exe	12/1/2020 7:52 AM	Application	184 KB
readme.txt	12/1/2020 7:52 AM	Text Document	11 KB

ChromeCookiesView: C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cookies

Host Name	Path	Name	Value	Secure	HTTP Only

ChromeCookiesView Analysis

- Opened ChromeCookiesView and pointed it to the default Chrome cookies location for the Administrator user.
- The tool executed successfully but **no cookies were present** in the browser profile.
- The output was completely empty, indicating no stored session data or artifacts at the time of the lab.



ChromeHistoryView Analysis

- Opened ChromeHistoryView and directed it to the default Chrome history location for the Administrator user.
- The tool executed successfully but **no browsing history was present** in the browser profile.
- The output was empty, indicating no visited URLs or recorded web activity at the time of the lab.

Lab 4: Extracting Information About Loaded Processes on a Computer

Lab Scenario

Processes are instances of computer programs running on a system and contain the code required for activity. Any program or malware will have various methods that will combine to give the result. An investigator should know the default processes to separate them from suspicious ones. To be an expert computer forensics investigator, you must understand how to extract information about loaded processes on a victim computer, which can be of importance during forensic investigation.

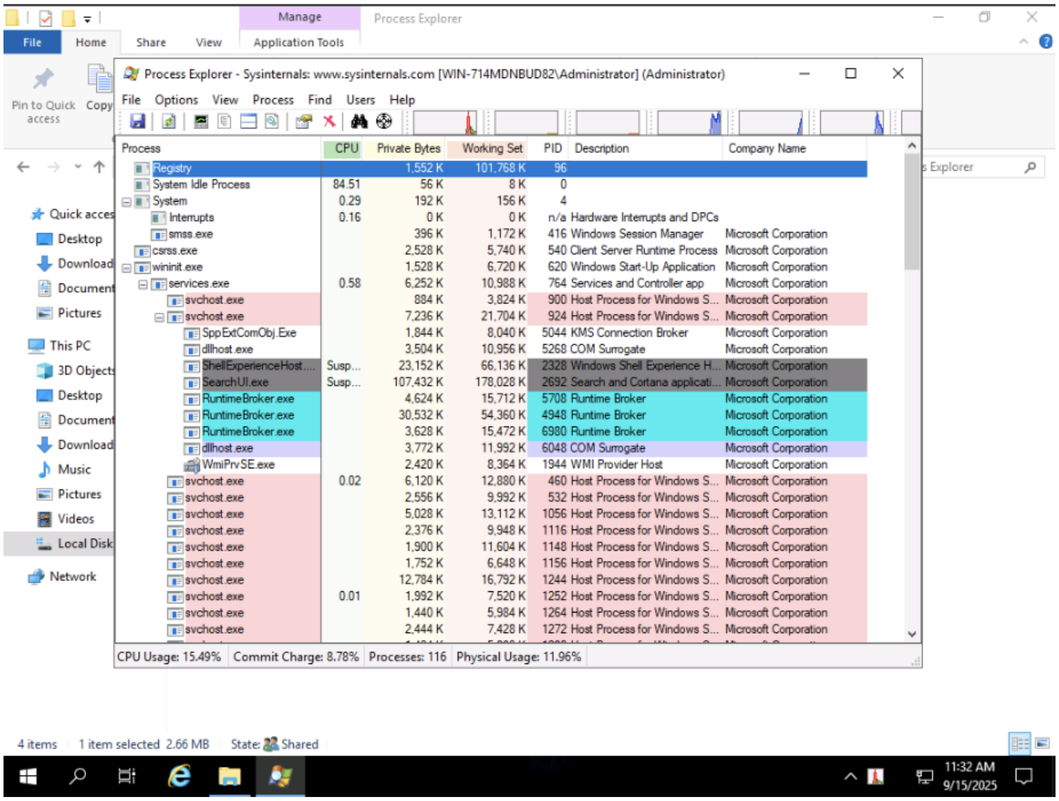
Lab Objectives

A process is an instance of a computer program that is being executed. Forensic investigators can examine these processes running on a computer for any malicious activity.

The purpose of this lab is to help you learn how to investigate loaded processes. In this lab, you will learn how to use Process Explorer.

Overview of the Lab

This lab familiarizes you with the Process Explorer tool and helps you understand how to examine information pertaining to loaded processes on a victim's system.

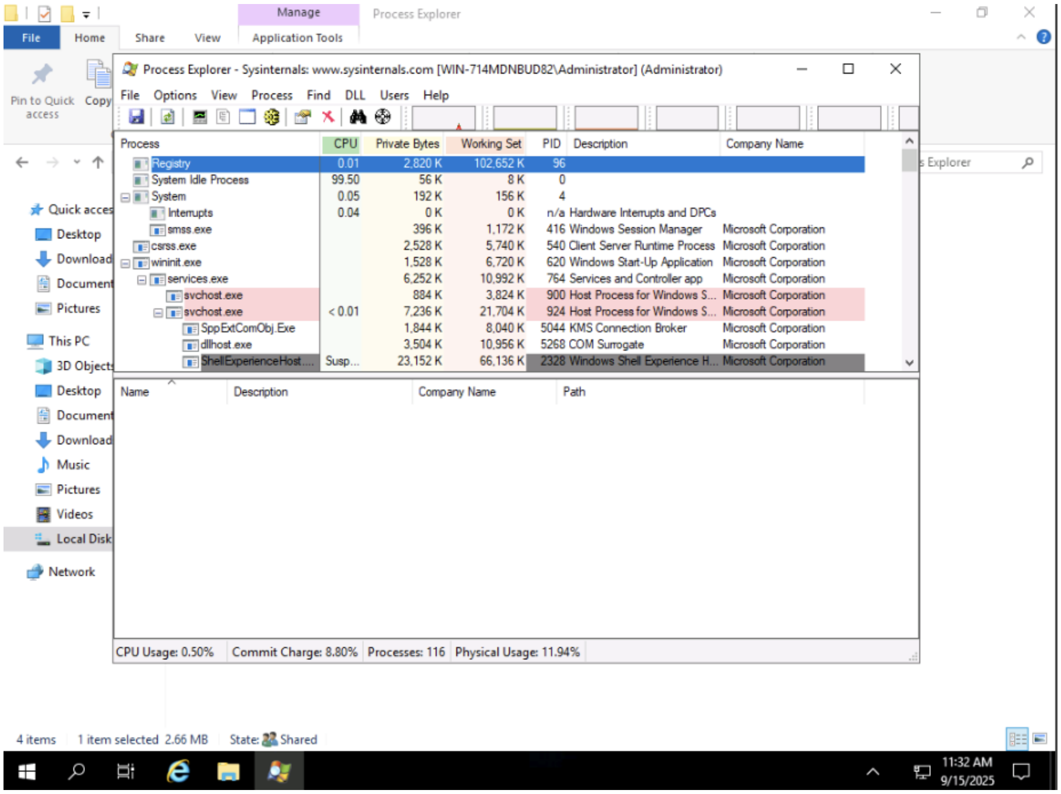


Process Explorer - Sysinternals: www.sysinternals.com [WIN-714MDNBUD82\Administrator] (Administrator)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		1,552 K	101,768 K	96		
System Idle Process	84.51	56 K	8 K	0		
System	0.29	192 K	156 K	4		
Interrupts	0.16	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		396 K	1,172 K	416	Windows Session Manager	Microsoft Corporation
csrss.exe		2,528 K	5,740 K	540	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,528 K	6,720 K	620	Windows Start-Up Application	Microsoft Corporation
services.exe	0.58	6,252 K	10,988 K	764	Services and Controller app	Microsoft Corporation
svchost.exe		884 K	3,824 K	900	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,236 K	21,704 K	924	Host Process for Windows S...	Microsoft Corporation
SppExtComObj.Exe		1,844 K	8,040 K	5044	KMS Connection Broker	Microsoft Corporation
dllhost.exe		3,504 K	10,956 K	5268	COM Surrogate	Microsoft Corporation
ShellExperienceHost....	Susp...	23,152 K	66,136 K	2328	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	107,432 K	178,028 K	2692	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe		4,624 K	15,712 K	5708	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		30,532 K	54,360 K	4948	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		3,628 K	15,472 K	6980	Runtime Broker	Microsoft Corporation
dllhost.exe		3,772 K	11,992 K	6048	COM Surrogate	Microsoft Corporation
WmiPrvSE.exe		2,420 K	8,364 K	1944	WMI Provider Host	Microsoft Corporation
svchost.exe	0.02	6,120 K	12,880 K	460	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,556 K	9,992 K	532	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,028 K	13,112 K	1056	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,376 K	9,948 K	1116	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,900 K	11,604 K	1148	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,752 K	6,648 K	1156	Host Process for Windows S...	Microsoft Corporation
svchost.exe		12,784 K	16,792 K	1244	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	1,992 K	7,520 K	1252	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,440 K	5,984 K	1264	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,444 K	7,428 K	1272	Host Process for Windows S...	Microsoft Corporation

CPU Usage: 15.49% | Commit Charge: 8.78% | Processes: 116 | Physical Usage: 11.96%

4 items 1 item selected 2.66 MB State: Shared



Process Explorer - Sysinternals: www.sysinternals.com [WIN-714MDNBUD82\Administrator] (Administrator)

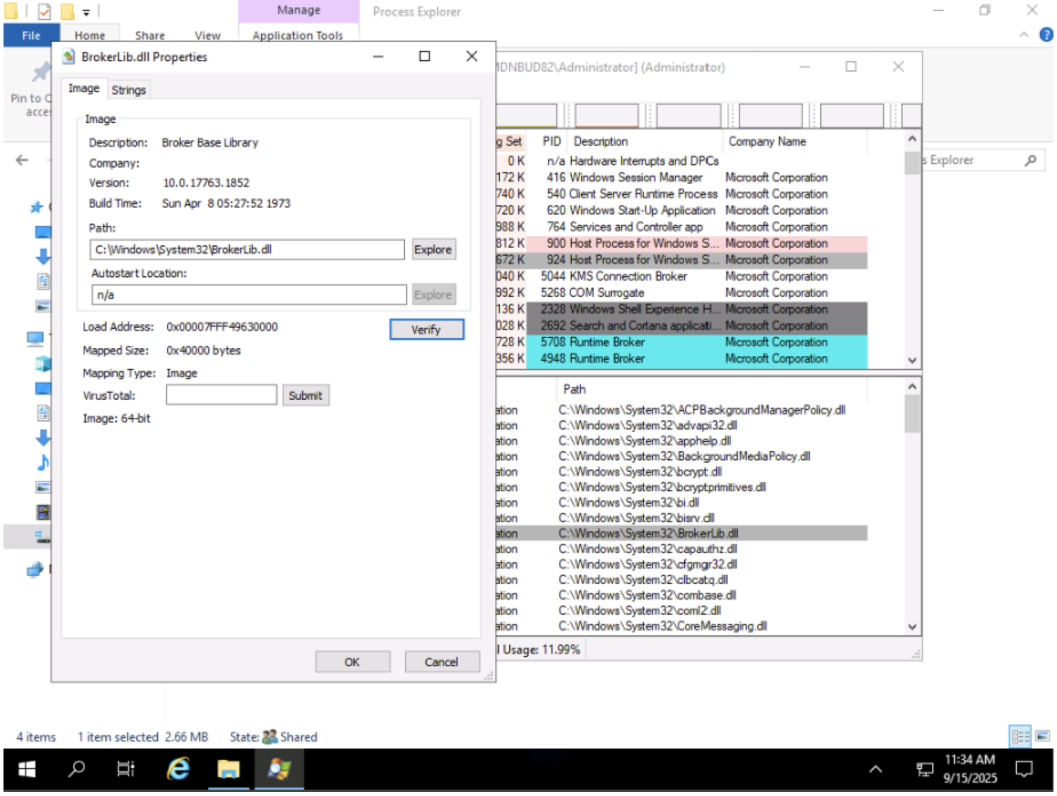
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry	0.01	2,820 K	102,652 K	96		
System Idle Process	99.50	56 K	8 K	0		
System	0.05	192 K	156 K	4		
Interrupts	0.04	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		396 K	1,172 K	416	Windows Session Manager	Microsoft Corporation
csrss.exe		2,528 K	5,740 K	540	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,528 K	6,720 K	620	Windows Start-Up Application	Microsoft Corporation
services.exe		6,252 K	10,992 K	764	Services and Controller app	Microsoft Corporation
svchost.exe		884 K	3,824 K	900	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	7,236 K	21,704 K	924	Host Process for Windows S...	Microsoft Corporation
SppExtComObj.Exe		1,844 K	8,040 K	5044	KMS Connection Broker	Microsoft Corporation
dllhost.exe		3,504 K	10,956 K	5268	COM Surrogate	Microsoft Corporation
ShellExperienceHost....	Susp...	23,152 K	66,136 K	2328	Windows Shell Experience H...	Microsoft Corporation

Name	Description	Company Name	Path

CPU Usage: 0.50% | Commit Charge: 8.80% | Processes: 116 | Physical Usage: 11.94%

4 items 1 item selected 2.66 MB State: Shared

11:32 AM
9/15/2025



BrokerLib.dll Properties

Image

Description: Broker Base Library

Company:

Version: 10.0.17763.1852

Build Time: Sun Apr 8 05:27:52 1973

Path:

C:\Windows\System32\BrokerLib.dll

Autostart Location:

n/a

Load Address: 0x00007FFF49630000

Mapped Size: 0x40000 bytes

Mapping Type: Image

VirusTotal:

Image: 64-bit

DNBUD82\Administrator] (Administrator)

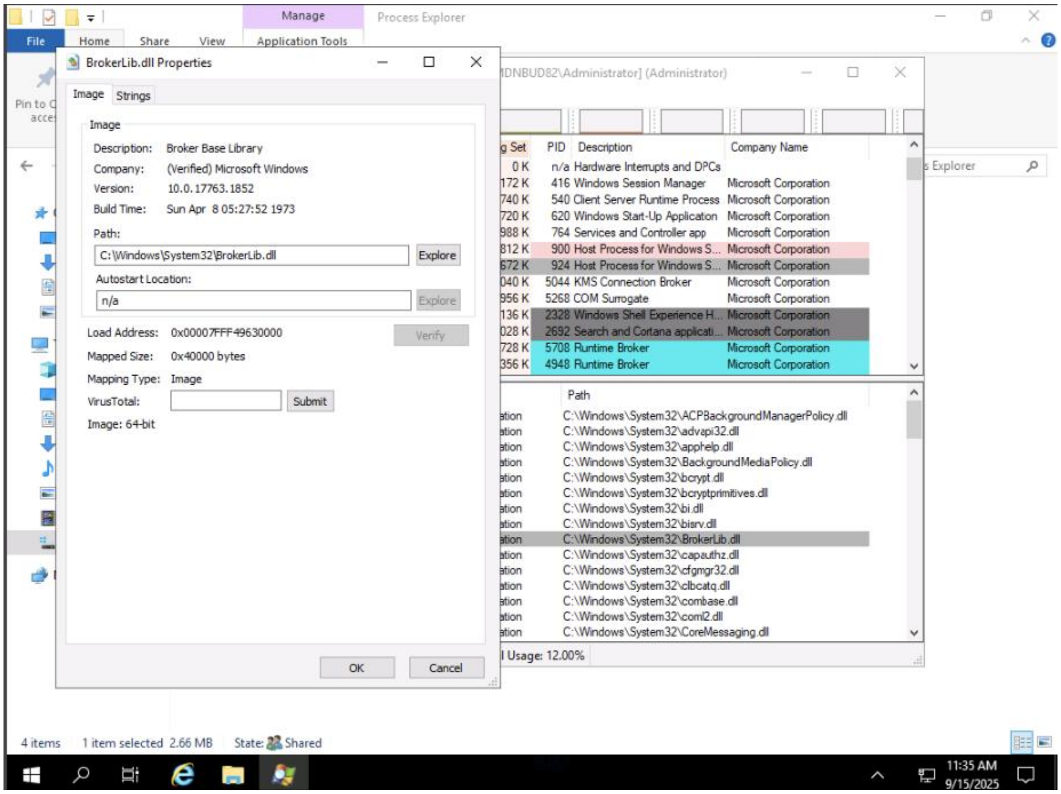
g Set	PID	Description	Company Name
0 K	n/a	Hardware Interrupts and DPCs	
172 K	416	Windows Session Manager	Microsoft Corporation
740 K	540	Client Server Runtime Process	Microsoft Corporation
720 K	620	Windows Start-Up Application	Microsoft Corporation
988 K	764	Services and Controller app	Microsoft Corporation
812 K	900	Host Process for Windows S...	Microsoft Corporation
672 K	924	Host Process for Windows S...	Microsoft Corporation
040 K	5044	KMS Connection Broker	Microsoft Corporation
992 K	5268	COM Surrogate	Microsoft Corporation
136 K	2328	Windows Shell Experience H...	Microsoft Corporation
028 K	2692	Search and Cortana applicati...	Microsoft Corporation
728 K	5708	Runtime Broker	Microsoft Corporation
356 K	4948	Runtime Broker	Microsoft Corporation

	Path
ation	C:\Windows\System32\ACPBackgroundManagerPolicy.dll
ation	C:\Windows\System32\advapi32.dll
ation	C:\Windows\System32\apphelp.dll
ation	C:\Windows\System32\BackgroundMediaPolicy.dll
ation	C:\Windows\System32\bcrypt.dll
ation	C:\Windows\System32\bcryptprimitives.dll
ation	C:\Windows\System32\bi.dll
ation	C:\Windows\System32\bisrv.dll
ation	C:\Windows\System32\BrokerLib.dll
ation	C:\Windows\System32\capauthz.dll
ation	C:\Windows\System32\cfgmgr32.dll
ation	C:\Windows\System32\clbcatq.dll
ation	C:\Windows\System32\combase.dll
ation	C:\Windows\System32\coml2.dll
ation	C:\Windows\System32\CoreMessaging.dll

l Usage: 11.99%

4 items 1 item selected 2.66 MB State: Shared

11:34 AM
9/15/2025



Image

Description: Broker Base Library
Company: (Verified) Microsoft Windows
Version: 10.0.17763.1852
Build Time: Sun Apr 8 05:27:52 1973

Path:
C:\Windows\System32\BrokerLib.dll

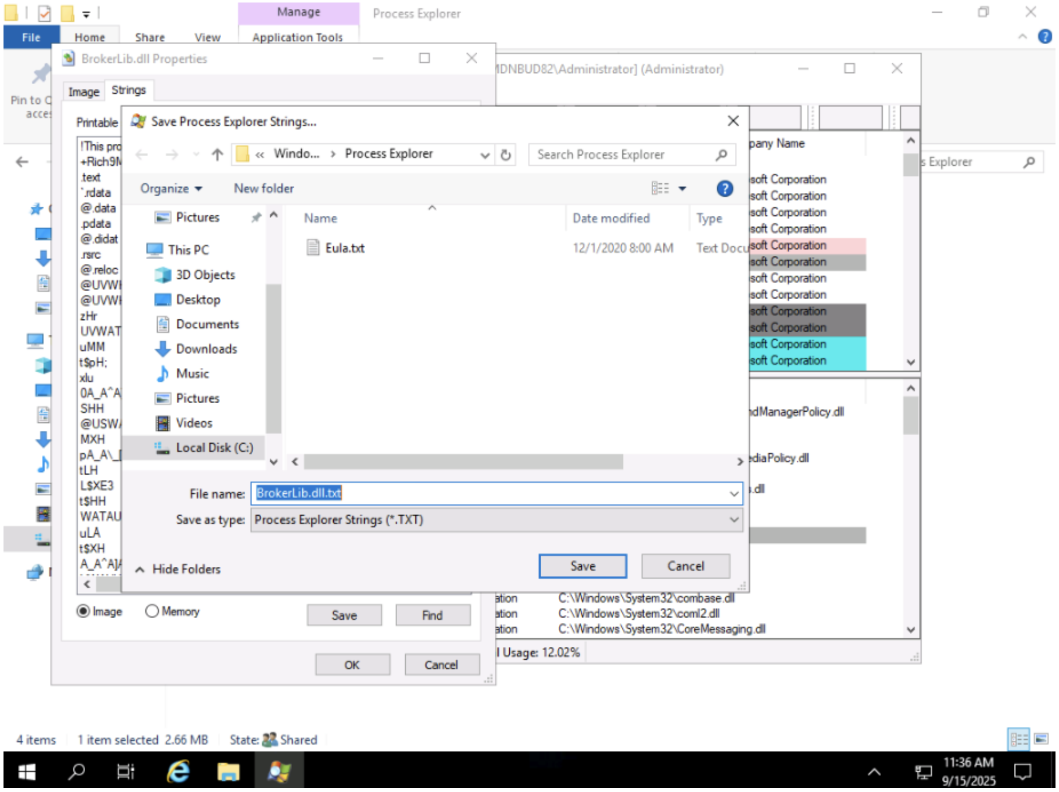
Autostart Location:
n/a

Load Address: 0x00007FFF49630000
Mapped Size: 0x40000 bytes
Mapping Type: Image
VirusTotal:
Image: 64-bit

DNBUD82\Administrator] (Administrator)

```
g Set   PID  Description                     Company Name
  0 K   n/a  Hardware Interrupts and DPCs
172 K   416  Windows Session Manager         Microsoft Corporation
740 K   540  Client Server Runtime Process   Microsoft Corporation
720 K   620  Windows Start-Up Application    Microsoft Corporation
988 K   764  Services and Controller app     Microsoft Corporation
812 K   900  Host Process for Windows S...   Microsoft Corporation
672 K   924  Host Process for Windows S...   Microsoft Corporation
040 K  5044  KMS Connection Broker           Microsoft Corporation
956 K  5268  COM Surrogate                   Microsoft Corporation
136 K  2328  Windows Shell Experience H...   Microsoft Corporation
028 K  2692  Search and Cortana applicati... Microsoft Corporation
728 K  5708  Runtime Broker                  Microsoft Corporation
356 K  4948  Runtime Broker                  Microsoft Corporation
```

```
         Path
ation    C:\Windows\System32\ACPBackgroundManagerPolicy.dll
ation    C:\Windows\System32\advapi32.dll
ation    C:\Windows\System32\apphelp.dll
ation    C:\Windows\System32\BackgroundMediaPolicy.dll
ation    C:\Windows\System32\bcrypt.dll
ation    C:\Windows\System32\bcryptprimitives.dll
ation    C:\Windows\System32\bi.dll
ation    C:\Windows\System32\bisrv.dll
ation    C:\Windows\System32\BrokerLib.dll
ation    C:\Windows\System32\capauthz.dll
ation    C:\Windows\System32\cfgmgr32.dll
ation    C:\Windows\System32\clbcatq.dll
ation    C:\Windows\System32\combase.dll
ation    C:\Windows\System32\coml2.dll
ation    C:\Windows\System32\CoreMessaging.dll
l Usage: 12.00%
```



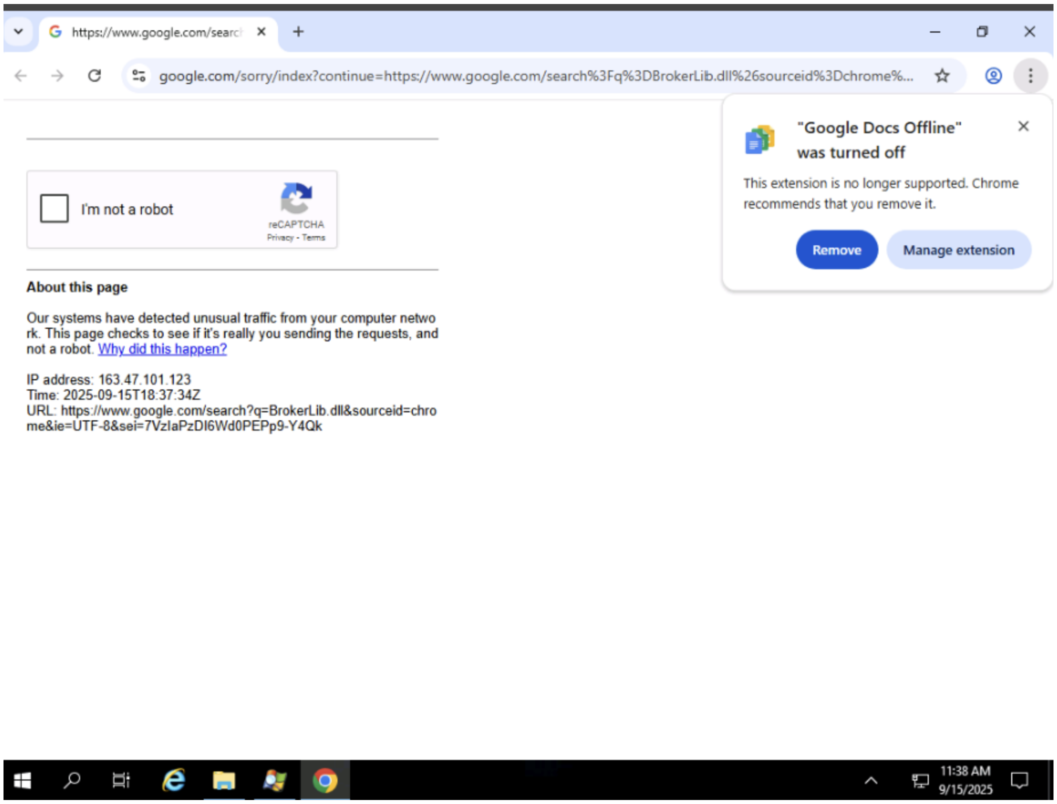
```
!This pro
+Rich9M
.text
`.rdata
@.data
.pdata
@.didat
.rsrc
@.reloc
@UVWI
@UVWI
zHr
UVWAT
uMM
t$pH;
xlu
0A_A^A
SHH
@USWA
MXH
pA_A\_
tLH
L$XE3
t$HH
WATAU
uLA
t$XH
A_A^AJ
```

Name	Date modified	Type
Eula.txt	12/1/2020 8:00 AM	Text Docu

File name: BrokerLib.dll.txt
Save as type: Process Explorer Strings (*.TXT)

```
pany Name
soft Corporation
soft Corporation
soft Corporation
soft Corporation
soft Corporation
soft Corporation
soft Corporation
soft Corporation
soft Corporation
soft Corporation
soft Corporation
soft Corporation
```

```
dManagerPolicy.dll
diaPolicy.dll
.dll
ation    C:\Windows\System32\combase.dll
ation    C:\Windows\System32\coml2.dll
ation    C:\Windows\System32\CoreMessaging.dll
l Usage: 12.02%
```



https://www.google.com/searc

google.com/sorry/index?continue=https://www.google.com/search%3Fq%3DBrokerLib.dll%26sourceid%3Dchrome%...

□ I'm not a robot

reCAPTCHA
Privacy - Terms

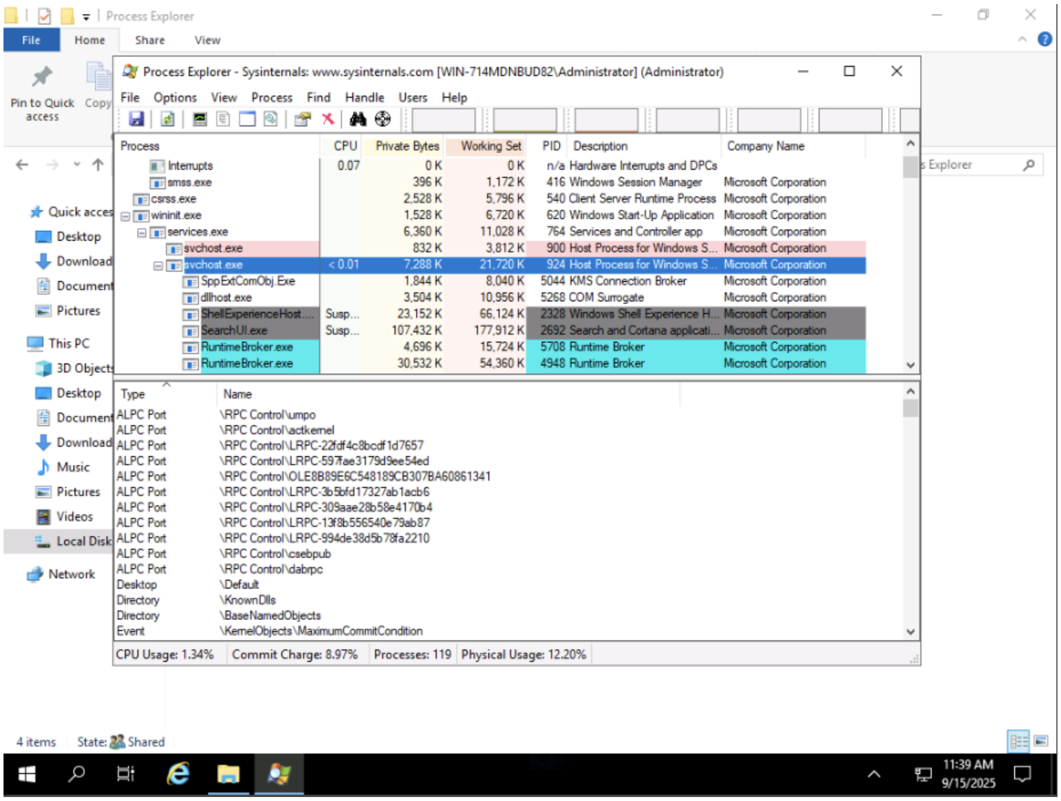
About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. Why did this happen?

IP address: 163.47.101.123
Time: 2025-09-15T18:37:34Z
URL: https://www.google.com/search?q=BrokerLib.dll&sourceid=chrome&ie=UTF-8&sei=7VzlaPzDI6Wd0PEPp9-Y4Qk

"Google Docs Offline" was turned off

This extension is no longer supported. Chrome recommends that you remove it.



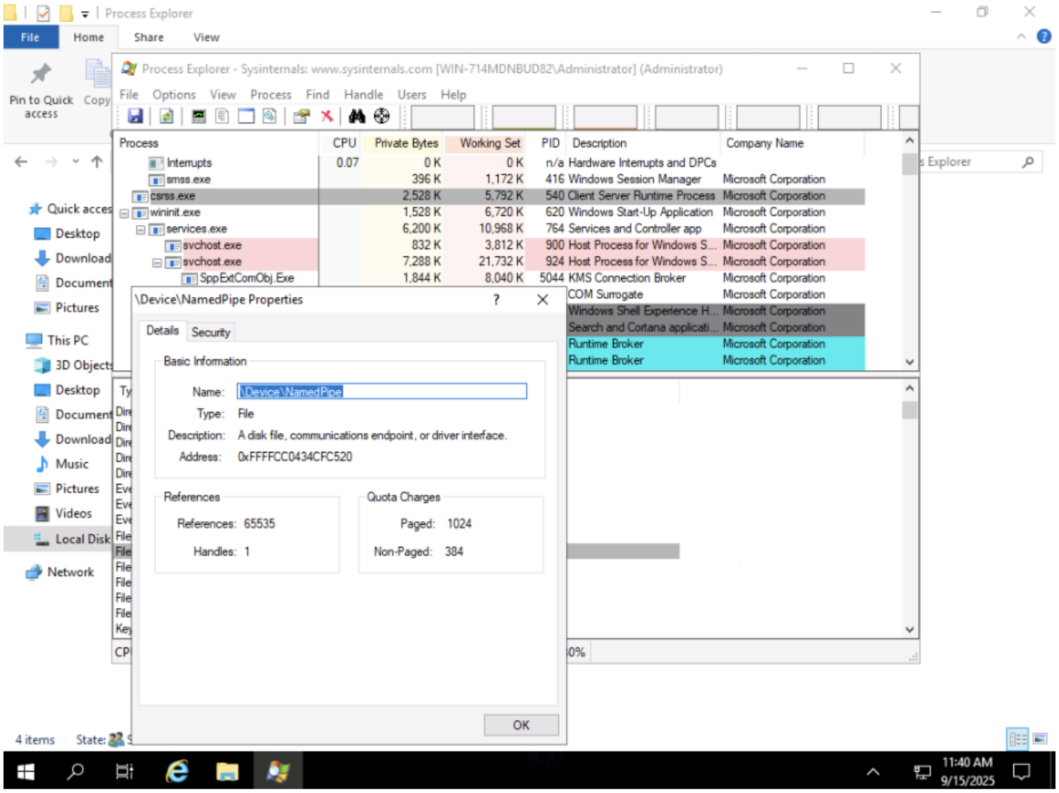
Process Explorer - Sysinternals: www.sysinternals.com [WIN-714MDNBUD82\Administrator] (Administrator)

```
Process                CPU     Private Bytes  Working Set   PID  Description                       Company Name
    Interrupts         0.07            0 K          0 K     n/a  Hardware Interrupts and DPCs
    smss.exe                         396 K      1,172 K     416  Windows Session Manager           Microsoft Corporation
  csrss.exe                        2,528 K      5,796 K     540  Client Server Runtime Process     Microsoft Corporation
⊟ wininit.exe                      1,528 K      6,720 K     620  Windows Start-Up Application      Microsoft Corporation
  ⊟ services.exe                   6,360 K     11,028 K     764  Services and Controller app       Microsoft Corporation
      svchost.exe                    832 K      3,812 K     900  Host Process for Windows S...     Microsoft Corporation
    ⊟ svchost.exe      < 0.01      7,288 K     21,720 K     924  Host Process for Windows S...     Microsoft Corporation
        SppExtComObj.Exe           1,844 K      8,040 K    5044  KMS Connection Broker             Microsoft Corporation
        dllhost.exe                3,504 K     10,956 K    5268  COM Surrogate                     Microsoft Corporation
        ShellExperienceHost.... Susp...  23,152 K   66,124 K    2328  Windows Shell Experience H...     Microsoft Corporation
        SearchUI.exe   Susp...   107,432 K    177,912 K    2692  Search and Cortana applicati...   Microsoft Corporation
        RuntimeBroker.exe          4,696 K     15,724 K    5708  Runtime Broker                    Microsoft Corporation
        RuntimeBroker.exe         30,532 K     54,360 K    4948  Runtime Broker                    Microsoft Corporation
```

```
Type        Name
ALPC Port   \RPC Control\umpo
ALPC Port   \RPC Control\actkernel
ALPC Port   \RPC Control\LRPC-22fdf4c8bcdf1d7657
ALPC Port   \RPC Control\LRPC-597fae3179d9ee54ed
ALPC Port   \RPC Control\OLE8B89E6C548189CB307BA60861341
ALPC Port   \RPC Control\LRPC-3b5bfd17327ab1acb6
ALPC Port   \RPC Control\LRPC-309aae28b58e4170b4
ALPC Port   \RPC Control\LRPC-13f8b556540e79ab87
ALPC Port   \RPC Control\LRPC-994de38d5b78fa2210
ALPC Port   \RPC Control\csebpub
ALPC Port   \RPC Control\dabrpc
Desktop     \Default
Directory   \KnownDlls
Directory   \BaseNamedObjects
Event       \KernelObjects\MaximumCommitCondition
```

CPU Usage: 1.34% | Commit Charge: 8.97% | Processes: 119 | Physical Usage: 12.20%

4 items   State: Shared



Process Explorer - Sysinternals: www.sysinternals.com [WIN-714MDNBUD82\Administrator] (Administrator)

```
Process              CPU   Private Bytes  Working Set  PID   Description                     Company Name
  Interrupts         0.07          0 K          0 K    n/a   Hardware Interrupts and DPCs
  smss.exe                       396 K      1,172 K    416   Windows Session Manager         Microsoft Corporation
csrss.exe                      2,528 K      5,792 K    540   Client Server Runtime Process   Microsoft Corporation
wininit.exe                    1,528 K      6,720 K    620   Windows Start-Up Application    Microsoft Corporation
  services.exe                 6,200 K     10,968 K    764   Services and Controller app     Microsoft Corporation
    svchost.exe                  832 K      3,812 K    900   Host Process for Windows S...   Microsoft Corporation
    svchost.exe                7,288 K     21,732 K    924   Host Process for Windows S...   Microsoft Corporation
      SppExtComObj.Exe         1,844 K      8,040 K   5044   KMS Connection Broker           Microsoft Corporation
                                                             COM Surrogate                   Microsoft Corporation
                                                             Windows Shell Experience H...   Microsoft Corporation
                                                             Search and Cortana applicati... Microsoft Corporation
                                                             Runtime Broker                  Microsoft Corporation
                                                             Runtime Broker                  Microsoft Corporation
```

\Device\NamedPipe Properties

Details | Security

Basic Information

Name: \Device\NamedPipe

Type: File

Description: A disk file, communications endpoint, or driver interface.

Address: 0xFFFFCC0434CFC520

References

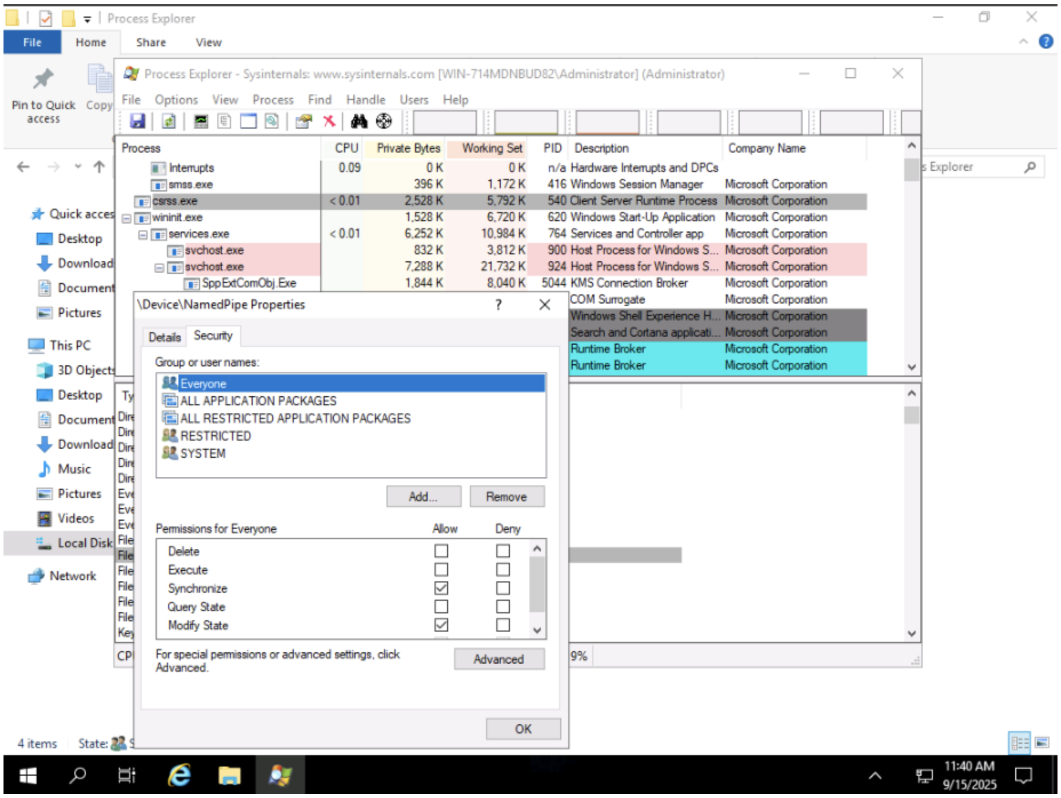
References: 65535

Handles: 1

Quota Charges

Paged: 1024

Non-Paged: 384



Process Explorer - Sysinternals: www.sysinternals.com [WIN-714MDNBUD82\Administrator] (Administrator)

```
Process              CPU   Private Bytes  Working Set  PID   Description                     Company Name
  Interrupts         0.09          0 K          0 K    n/a   Hardware Interrupts and DPCs
  smss.exe                       396 K      1,172 K    416   Windows Session Manager         Microsoft Corporation
csrss.exe            < 0.01    2,528 K      5,792 K    540   Client Server Runtime Process   Microsoft Corporation
wininit.exe                    1,528 K      6,720 K    620   Windows Start-Up Application    Microsoft Corporation
  services.exe       < 0.01    6,252 K     10,984 K    764   Services and Controller app     Microsoft Corporation
    svchost.exe                  832 K      3,812 K    900   Host Process for Windows S...   Microsoft Corporation
    svchost.exe                7,288 K     21,732 K    924   Host Process for Windows S...   Microsoft Corporation
      SppExtComObj.Exe         1,844 K      8,040 K   5044   KMS Connection Broker           Microsoft Corporation
                                                             COM Surrogate                   Microsoft Corporation
                                                             Windows Shell Experience H...   Microsoft Corporation
                                                             Search and Cortana applicati... Microsoft Corporation
                                                             Runtime Broker                  Microsoft Corporation
                                                             Runtime Broker                  Microsoft Corporation
```

\Device\NamedPipe Properties

Details | Security

Group or user names:

- Everyone
- ALL APPLICATION PACKAGES
- ALL RESTRICTED APPLICATION PACKAGES
- RESTRICTED
- SYSTEM

Permissions for Everyone	Allow	Deny
Delete	□	□
Execute	□	□
Synchronize	☑	□
Query State	□	□
Modify State	☑	□

For special permissions or advanced settings, click Advanced.

Module 06: Windows Forensics – Summary

Lab Focus:
This module demonstrates the investigation of Windows systems to collect and analyze forensic evidence. Investigators focus on volatile memory, Windows event logs, loaded processes, and browser artifacts to identify malicious behavior or evidence of crimes.

Lab 1 – Acquiring Volatile Information from a Live Windows System:

- Investigators collected live system information including network connections and running processes.
- Tools such as PsTools and LogonSessions were used to capture volatile system data.

Lab 2 – Investigating Forensic Image of Windows RAM:

- RAM dumps from Windows machines were examined to detect malicious activity or compromised processes.
- Tools used include Redline and Volatility framework, allowing analysis of memory contents and identification of suspicious processes.

Lab 3 – Examining Web Browser Artifacts:

- Investigated browser caches, cookies, and history to retrieve artifacts of user activity.
- Tools included ChromeCacheView, ChromeHistoryView, and ChromeCookiesView.
- Both ChromeCookiesView and ChromeHistoryView displayed no data in this instance, indicating no recorded activity.

Lab 4 – Extracting Information About Loaded Processes on a Computer:

- Loaded processes on a Windows system were analyzed to identify suspicious or malicious activity.
- Process Explorer was used to review process information and determine potential security threats.

Key Takeaways:

- Windows forensics requires collection of both volatile and non-volatile data.
- Memory analysis, browser artifacts, and loaded processes are critical sources of evidence.

- Tools like PsTools, LogonSessions, Redline, Volatility, and Process Explorer help investigators gather and interpret forensic data efficiently.