

CY-640 - Cyber Crime and Forensics Labs

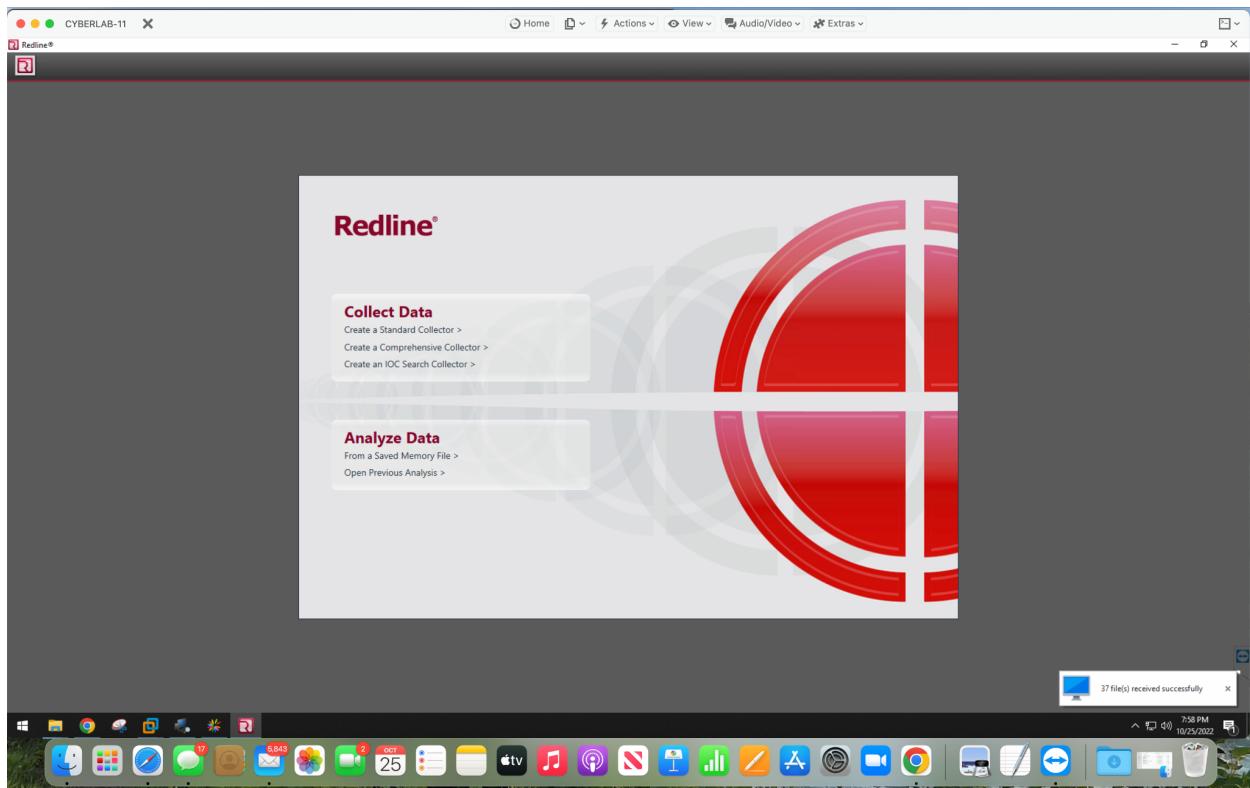
Nikhil Patel

Spring Trimester 2022

10/31/2022

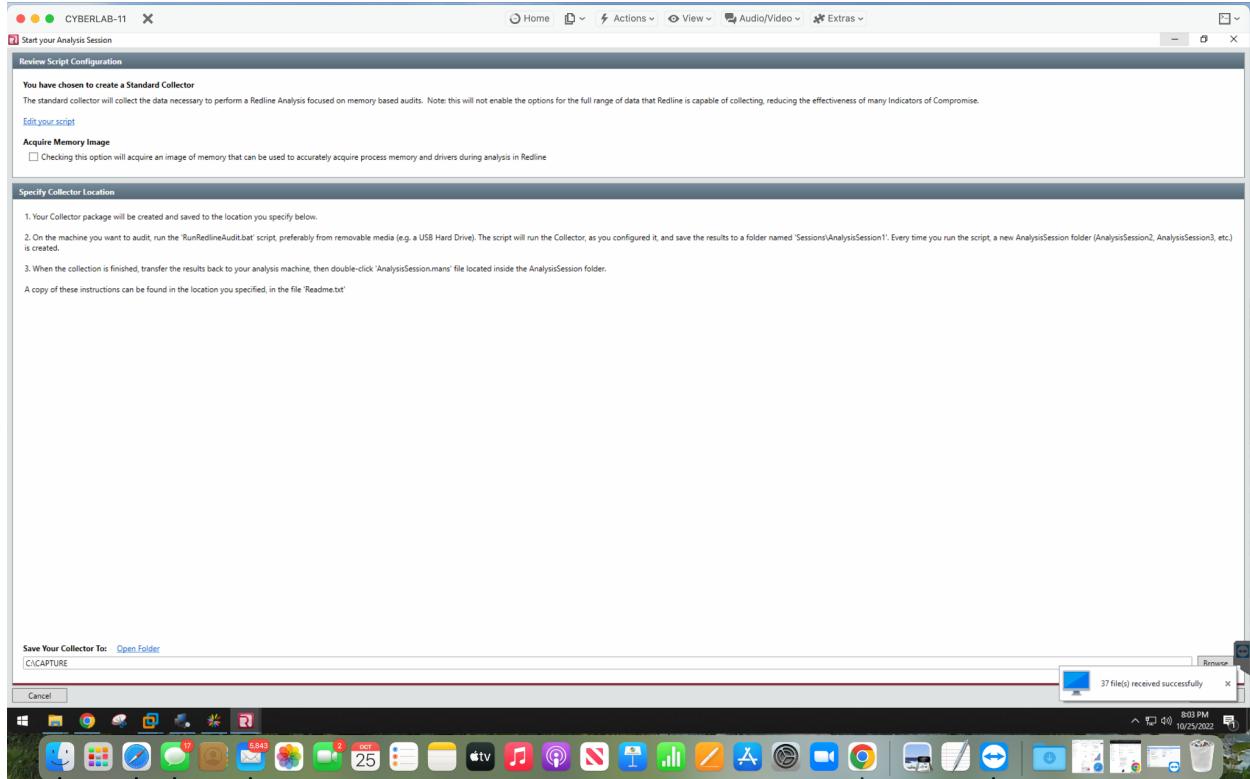
Memory Forensics

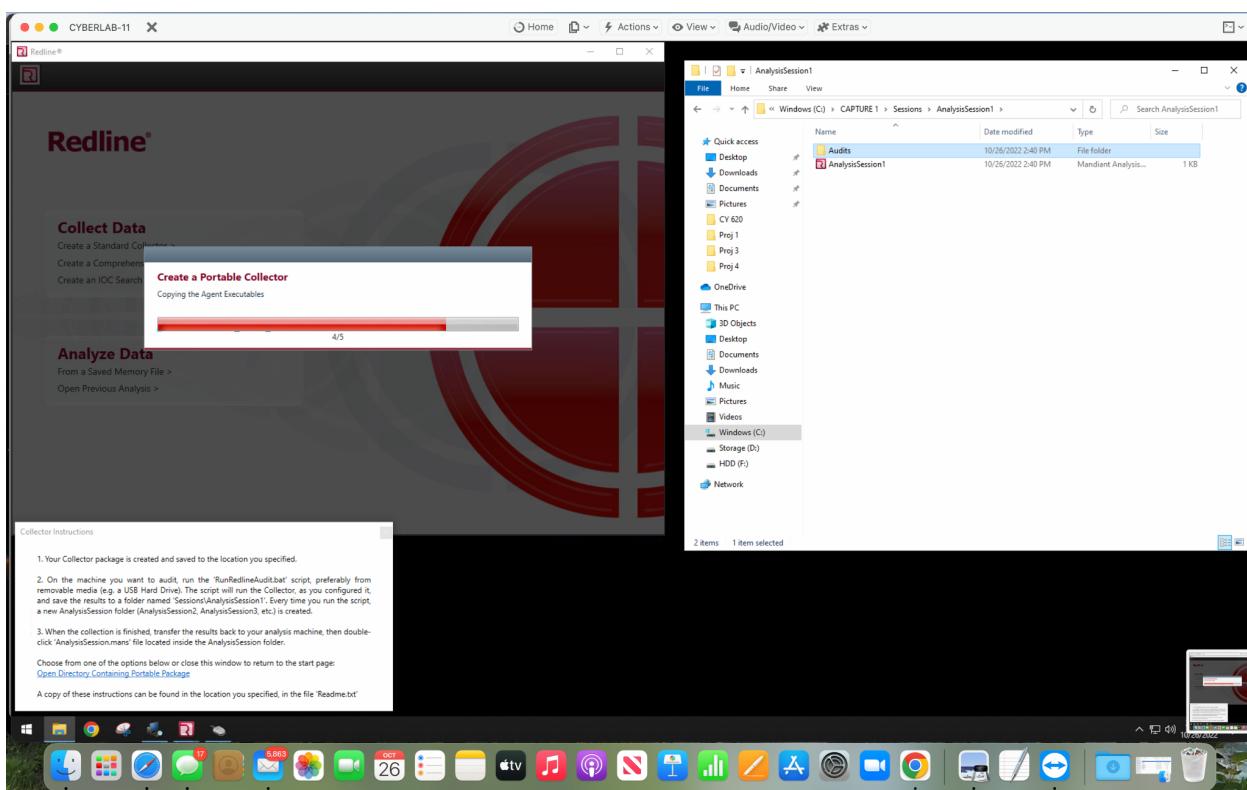
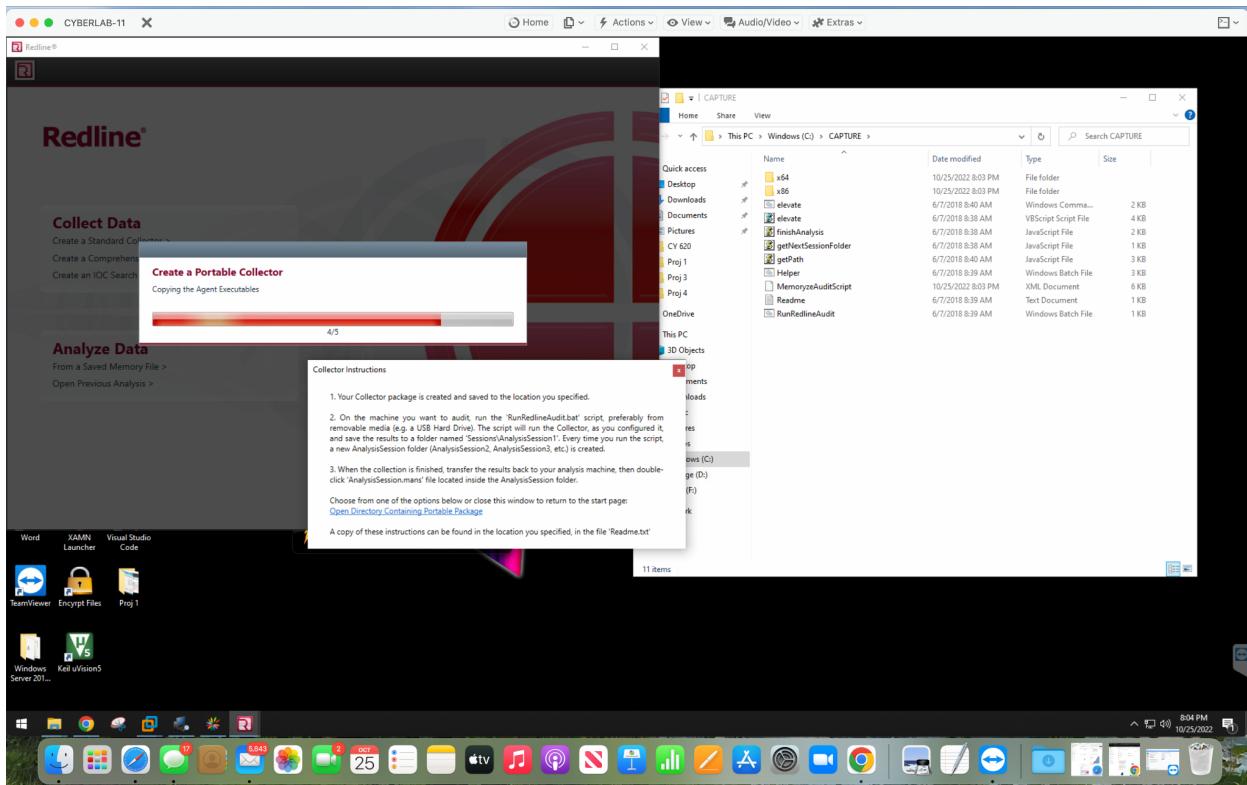
Overview: We will investigate memory in three parts in this project, using a tool called redline (Standard, Comprehensive, and IOC). Because comprehensive gathers data in greater depth, which takes time, standard and IOC recorded memory in less time than comprehensive. We will prepare reports on three (3) different features/capabilities, such as collections: standard, comprehensive, and IOC (for example, a report on malware analysis and what processes are running), using Redline, the digital forensics software that was given to you to install on your computer in class.



Standard Analysis:

- Create a standard collection of data.
- Now after you click on the standard collection, tick on it to acquire a memory image then provide an empty folder path.
- Then, after opening the file location and run the .bat file and wait until it is complete.
- Once the standard analysis is done it will create a report file for analyzing acquired memory.
- Now go to session open the file and Here we will not get the entire memory data in standard collection.
- Here we can see system info, Network adapters details, running processes, and much more.





CYBERLAB-11

Redline® - C:\CAPTURE\Sessions\AnalysisSession1\AnalysisSession1.mns

Home ▾ Actions ▾ View ▾ Audio/Video ▾ Extras ▾

Start Your Investigation

I am Reviewing a Triage Collection from HX

When you are starting with a piece of external information indicating that the host requires further examining, you should start your investigation by using the Timeline and its powerful filtering capabilities to quickly hone in on your investigative lead and from there find additional items of interest to follow. If your initial lead is a timeframe of suspicious activity identified by an IDS, you can use TimeWrinkles™ to filter all events that occurred around that timeframe. If your initial lead is malicious activity by a process or single user identified by an Indicator of Compromise, then you can use the Unique Process and Username filters to show only events that were generated by them.

I am Investigating a Host Based on an External Investigative Lead

When you are starting with a piece of external information indicating that the host requires further examining, you should start your investigation by using the Timeline and its powerful filtering capabilities to quickly hone in on your investigative lead and from there find additional items of interest to follow. If your initial lead is a timeframe of suspicious activity identified by an IDS, you can use TimeWrinkles™ to filter all events that occurred around that timeframe. If your initial lead is malicious activity by a process or single user identified by an Indicator of Compromise, then you can use the Unique Process and Username filters to show only events that were generated by them.

I am Reviewing Web History Data

When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can include sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline file filters to investigate any file downloads or cookies being sent around the same time period.

I Want to Search My Data With a Set of Indicators of Compromise

When you have a set of Indicators of Compromise (IOC), you can use them to generate a report in Redline which identifies any forensic artifacts on the host you are analyzing that is described by the indicator definitions. Simply select 'Create a New IOC Report' and specify the location on disk that contains your indicator. When the report is finished you will find it underneath the IOC Reports tab to the left. For more information on IOCs visit <http://www.opensoc.org>

Host IOC Reports Not Collected

4:09 PM 10/26/2022

CYBERLAB-11

Redline® - C:\CAPTURE\Sessions\AnalysisSession1\AnalysisSession1.mns

Home ▾ Host ▾ Hierarchical Processes

Analysis Data

System Information

Processes

Hierarchical Processes

Timeline

Tags and Comments

Acquisition History

Review Processes Hierarchically

This view shows the relationship between all of the processes and their parent processes.

Process Name	PID	Path	Arguments	Username	Start Time	Kernel Tl.	User Time...	Hidden	Security...	SID Type
System	4			NT AUTHORITY\SYSTEM	2022-10-18 23:22:02	00:03:07	00:00:00		S-1-5-18	SidTypeWell
Registry	124			NT AUTHORITY\SYSTEM	2022-10-18 23:21:58Z	00:00:01	00:00:00		S-1-5-18	SidTypeWell
smss.exe	628			NT AUTHORITY\SYSTEM	2022-10-18 23:22:02	00:00:00	00:00:00		S-1-5-18	SidTypeWell
Memory Compression	2172			NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00:00:09	00:00:00		S-1-5-18	SidTypeWell
Explorer.EXE	596	C:\windows	C:\windows\Explorer.EXE	CYBERLAB-11\cybersecurity	2022-10-18 21:00:08Z	00:01:48	00:01:06		S-1-5-2...	SidTypeUser
osTrage2.exe	2732	C:\Users\cybersecurity\Downloads\osTrage2-20221025T20395...	"C:\Users\cybersecurity\Downloads\osTrage2-20221025T20395...	CYBERLAB-11\cybersecurity	2022-10-18 23:13:16Z	00:00:05	00:00:09		S-1-5-2...	SidTypeUser
WaveOutc4.exe	4580	C:\Program Files\Waves\MaxxAudio	"C:\Program Files\Waves\MaxxAudio	CYBERLAB-11\cybersecurity	2022-10-18 21:00:22Z	00:00:00	00:00:00		S-1-5-2...	SidTypeUser
RAVEg4.exe	6052	C:\Program Files\Reteck\Audio\HDA	"C:\Program Files\Reteck\Audio\HDA	CYBERLAB-11\cybersecurity	2022-10-18 21:00:22Z	00:00:00	00:00:00		S-1-5-2...	SidTypeUser
Mouseagle.exe	6064	F:\Assignment	"F:\Assignment\Mouseagle.exe"	CYBERLAB-11\cybersecurity	2022-10-18 00:09:48Z	00:00:00	00:00:00		S-1-5-2...	SidTypeUser
SecurityHealthStray.exe	9536	C:\Windows\System32	"C:\Windows\System32\SecurityH...	CYBERLAB-11\cybersecurity	2022-10-18 21:00:12Z	00:00:00	00:00:00		S-1-5-2...	SidTypeUser
RashGUI64.exe	9892	C:\Program Files\Reteck\Audio\HDA	"C:\Program Files\Reteck\Audio\HDA	CYBERLAB-11\cybersecurity	2022-10-18 21:00:12Z	00:00:00	00:00:00		S-1-5-2...	SidTypeUser
Redline.exe	100...	C:\Program Files (x86)\Redline	"C:\Program Files (x86)\Redline\Re...	CYBERLAB-11\cybersecurity	2022-10-18 23:56:15Z	00:01:06	00:02:18		S-1-5-2...	SidTypeUser
OneDrive.exe	107...	C:\Users\cybersecurity\AppData\Local\Microsoft\OneDrive	"C:\Users\cybersecurity\AppData\Loc...	CYBERLAB-11\cybersecurity	2022-10-18 21:00:23Z	00:00:00	00:00:01		S-1-5-2...	SidTypeUser
crss.exe	824			NT AUTHORITY\SYSTEM	2022-10-18 23:22:04Z	00:00:02	00:00:00		S-1-5-18	SidTypeWell
winnbg.exe	912			NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00:00:00	00:00:00		S-1-5-18	SidTypeWell
services.exe	984			NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00:00:13	00:00:03		S-1-5-18	SidTypeWell
svchost.exe	88	C:\Windows\System32	C:\windows\System32\svchost.e...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00:00:00	00:00:00		S-1-5-18	SidTypeWell
svchost.exe	980	C:\Windows\System32	C:\Windows\System32\svchost.e...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00:00:16	00:00:04		S-1-5-18	SidTypeWell
svchost.exe	1064	C:\Windows\System32	C:\Windows\System32\svchost.e...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00:00:00	00:00:00		S-1-5-18	SidTypeWell
svchost.exe	1116	C:\Windows\System32	C:\Windows\System32\svchost.e...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00:00:19	00:00:04		S-1-5-18	SidTypeWell
ApplicationFrameHost...	812	C:\Windows\System32	C:\Windows\System32\Application...	CYBERLAB-11\cybersecurity	2022-10-18 21:47:46Z	00:00:00	00:00:00		S-1-5-2...	SidTypeUser
RuntimeBroker.exe	2608	C:\Windows\System32	C:\Windows\System32\RuntimeBr...	CYBERLAB-11\cybersecurity	2022-10-18 23:37:03Z	00:00:00	00:00:00		S-1-5-2...	SidTypeUser
RuntimeBroker.exe	2968	C:\Windows\System32	C:\Windows\System32\RuntimeBr...	CYBERLAB-11\cybersecurity	2022-10-18 21:00:02	00:00:03	00:00:01		S-1-5-2...	SidTypeUser
mouscoreworker.exe	3180	C:\Windows\System32	C:\Windows\System32\mouscore...	NT AUTHORITY\SYSTEM	2022-10-18 22:00:50Z	00:00:03	00:00:00		S-1-5-18	SidTypeWell
RuntimeBroker.exe	3260	C:\Windows\System32	C:\Windows\System32\RuntimeBr...	CYBERLAB-11\cybersecurity	2022-10-18 21:00:19Z	00:00:01	00:00:00		S-1-5-2...	SidTypeUser
RuntimeBroker.exe	3684	C:\Windows\System32	C:\Windows\System32\RuntimeBr...	CYBERLAB-11\cybersecurity	2022-10-18 21:00:09Z	00:00:01	00:00:01		S-1-5-2...	SidTypeUser
DflHost.exe	5188	C:\Windows\System32	C:\Windows\System32\DFLHost.e...	CYBERLAB-11\cybersecurity	2022-10-18 21:33:00Z	00:00:00	00:00:00		S-1-5-2...	SidTypeUser
RuntimeBroker.exe	5720	C:\Windows\System32	C:\Windows\System32\RuntimeBr...	CYBERLAB-11\cybersecurity	2022-10-18 21:40:01Z	00:00:00	00:00:00		S-1-5-2...	SidTypeUser
wmpnse.exe	5868	C:\Windows\System32\webem	C:\Windows\System32\webem\wmp...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:07Z	00:00:00	00:00:00		S-1-5-18	SidTypeWell
SearchApp.exe	8748	C:\Windows\System32\Microsoft.Windows.Search_cw5n1h...	"C:\Windows\System32\Microsoft.W...	CYBERLAB-11\cybersecurity	2022-10-18 21:00:10Z	00:00:02	00:00:08		S-1-5-2...	SidTypeUser
Microsoft.Photos.exe	8908	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_20...	"C:\Program Files\WindowsApp...	CYBERLAB-11\cybersecurity	2022-10-18 21:37:02Z	00:00:00	00:00:00		S-1-5-2...	SidTypeUser
unsecapp.exe	103...	C:\Windows\System32\webem	C:\Windows\System32\webem\unse...	NT AUTHORITY\SYSTEM	2022-10-18 21:00:07Z	00:00:00	00:00:00		S-1-5-18	SidTypeWell

171 Items

Host IOC Reports Not Collected

4:09 PM 10/26/2022

Redline® - C:\CAPTURE\Sessions\AnalysisSession1\AnalysisSession1.mns

Home Host Timeline

Analysis Data

Timeline Configuration

Show All Select All

Files:

- Accessed
- Modified
- Changed
- FileNameCreated
- FileNameAccessed
- FileNameModified
- FileNameChanged
- PmInfoExportsExportsTimestamp
- PmInfoPmTimestamp

Processes:

- StartTime

Registry:

- Modified

Event Logs:

- GetTime
- WriteTime

Tasks:

- LastRunTime
- MostRecentRunTime
- CreationDate
- TriggerBegin
- TriggerEnd

User Account:

- LastLogin

System Information:

- SystemDate
- SystemTime
- NetworkInfo(DHCPleaseExpires
- NetworkInfo(DHCPleaseObtained

Ports:

- CreationTime

Prefetch:

- LastRun
- Created

Agent Events:

- FileWriteEventGenerated
- RegistryEventGenerated
- ReplyEventGenerated
- AddressResolutionAgentEventGenerated
- NetworkAgentEventGenerated
- ImageLoadAgentEventGenerated
- ImageLoadAgentEventDULGenerated

Fields: TimeCrunches™ 0 | TimeWrinkles™ 0

Enter string to find here... In All Fields Clear Column Filters Prev Next

Y	Timestamp	Field	Summary	Machine: CYBERLAB-11	Domain: SPC	OS: Windows 10 Enterprise 19044	Bitness: 64-bit	User: NT AUTHORITY\S
1	2022-10-18 23:21:58Z	System/InstallDate	Name: Registry	PID: 124	Path:	Arg:	Arg:	User: NT AUTHORITY\S
2	2022-10-18 23:21:58Z	Process/StartTime	Name: Registry	PID: 124	Path:	Arg:	Arg:	User: NT AUTHORITY\S
3	2022-10-18 23:22:02Z	Process/StartTime	Name: System	PID: 4	Path:	Arg:	Arg:	User: NT AUTHORITY\S
4	2022-10-18 23:22:02Z	Process/StartTime	Name: smss.exe	PID: 628	Path:	Arg:	Arg:	User: NT AUTHORITY\S
5	2022-10-18 23:22:02Z	Process/StartTime	Name: smss.exe	PID: 628	Path:	Arg:	Arg:	User: NT AUTHORITY\S
6	2022-10-18 23:22:02Z	Process/StartTime	Name: System	PID: 4	Path:	Arg:	Arg:	User: NT AUTHORITY\S
7	2022-10-18 23:22:04Z	Process/StartTime	Name: cors.exe	PID: 824	Path:	Arg:	Arg:	User: NT AUTHORITY\S
8	2022-10-18 23:22:04Z	Process/StartTime	Name: cors.exe	PID: 824	Path:	Arg:	Arg:	User: NT AUTHORITY\S
9	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1484	Path: C:\Windows\system32\svchost.exe -k netvds -s CetPropSvc	Arg: C:\Windows\system32\svchost.exe -k netvds -s CetPropSvc	Arg:	User: NT AUTHORITY\S
10	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1588	Path: C:\Windows\system32\svchost.exe -k LocalService\Network\Remote	Arg: C:\Windows\system32\svchost.exe -k LocalService\Network\Remote	Arg:	User: NT AUTHORITY\S
11	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 88	Path: C:\Windows\system32\svchost.exe -k netvds -g Themes	Arg: C:\Windows\system32\svchost.exe -k netvds -g Themes	Arg:	User: NT AUTHORITY\S
12	2022-10-18 23:22:05Z	Process/StartTime	Name: services.exe	PID: 984	Path:	Arg:	Arg:	User: NT AUTHORITY\S
13	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1412	Path: C:\Windows\system32\svchost.exe	Arg: C:\Windows\system32\svchost.exe -k NetworkService -s TermServ...	Arg:	User: NT AUTHORITY\S
14	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1584	Path: C:\Windows\system32\svchost.exe -k LocalSystem\Network\Remote	Arg: C:\Windows\system32\svchost.exe -k LocalSystem\Network\Remote	Arg:	User: NT AUTHORITY\S
15	2022-10-18 23:22:05Z	Process/StartTime	Name: win32k.exe	PID: 912	Path:	Arg:	Arg:	User: NT AUTHORITY\S
16	2022-10-18 23:22:05Z	Process/StartTime	Name: lsass.exe	PID: 992	Path: C:\Windows\system32\lsass.exe	Arg: C:\Windows\system32\lsass.exe	Arg:	User: NT AUTHORITY\S
17	2022-10-18 23:22:05Z	Process/StartTime	Name: MemoryCompressor	PID: 2172	Path:	Arg:	Arg:	User: NT AUTHORITY\S
18	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1116	Path: C:\Windows\system32\svchost.exe	Arg: C:\Windows\system32\svchost.exe -k DcomLaunch -p	Arg:	User: NT AUTHORITY\S
19	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 980	Path: C:\Windows\system32\svchost.exe -k LocalSystem\Network\Remote	Arg: C:\Windows\system32\svchost.exe -k LocalSystem\Network\Remote	Arg:	User: NT AUTHORITY\S
20	2022-10-18 23:22:05Z	Process/StartTime	Name: fontndrhost.exe	PID: 1148	Path:	Arg: "fontndrhost.exe"	Arg:	User: Font Driver Host
21	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1240	Path: C:\Windows\system32\svchost.exe	Arg: C:\Windows\system32\svchost.exe -k RPCSS -p	Arg:	User: NT AUTHORITY\S
22	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1470	Path: C:\Windows\system32\svchost.exe	Arg: C:\Windows\system32\svchost.exe -k LocalService -s W32Time	Arg:	User: NT AUTHORITY\S
23	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1384	Path: C:\Windows\system32\svchost.exe	Arg: C:\Windows\system32\svchost.exe -k DnsRaClient -p LM	Arg:	User: NT AUTHORITY\S
24	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1488	Path: C:\Windows\system32\svchost.exe -k LocalService -p nsl	Arg: C:\Windows\system32\svchost.exe -k LocalService -p nsl	Arg:	User: NT AUTHORITY\S
25	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1724	Path: C:\Windows\system32\svchost.exe	Arg: C:\Windows\system32\svchost.exe -k LocalSystem\Network\Remote	Arg:	User: NT AUTHORITY\S
26	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1612	Path: C:\Windows\system32\svchost.exe	Arg: C:\Windows\system32\svchost.exe -k LocalService\Network\Remote	Arg:	User: NT AUTHORITY\S
27	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1672	Path: C:\Windows\system32\svchost.exe	Arg: C:\Windows\system32\svchost.exe -k NetworkService -p Drv...	Arg:	User: NT AUTHORITY\S
28	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1764	Path: C:\Windows\system32\svchost.exe	Arg: C:\Windows\system32\svchost.exe -k LocalService\Network\Remote	Arg:	User: NT AUTHORITY\S
29	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1856	Path: C:\Windows\system32\svchost.exe -k LocalService\Network\Remote	Arg: C:\Windows\system32\svchost.exe -k LocalService\Network\Remote	Arg:	User: NT AUTHORITY\S
30	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1958	Path: C:\Windows\system32\svchost.exe -k NetworkService -p NlaSvc	Arg: C:\Windows\system32\svchost.exe -k NetworkService -p NlaSvc	Arg:	User: NT AUTHORITY\S
31	2022-10-18 23:22:05Z	Process/StartTime	Name: svchost.exe	PID: 1064	Path: C:\Windows\system32\svchost.exe	Arg: C:\Windows\system32\svchost.exe -k netvds -g -p ProfSoc	Arg:	User: NT AUTHORITY\S

342 Items

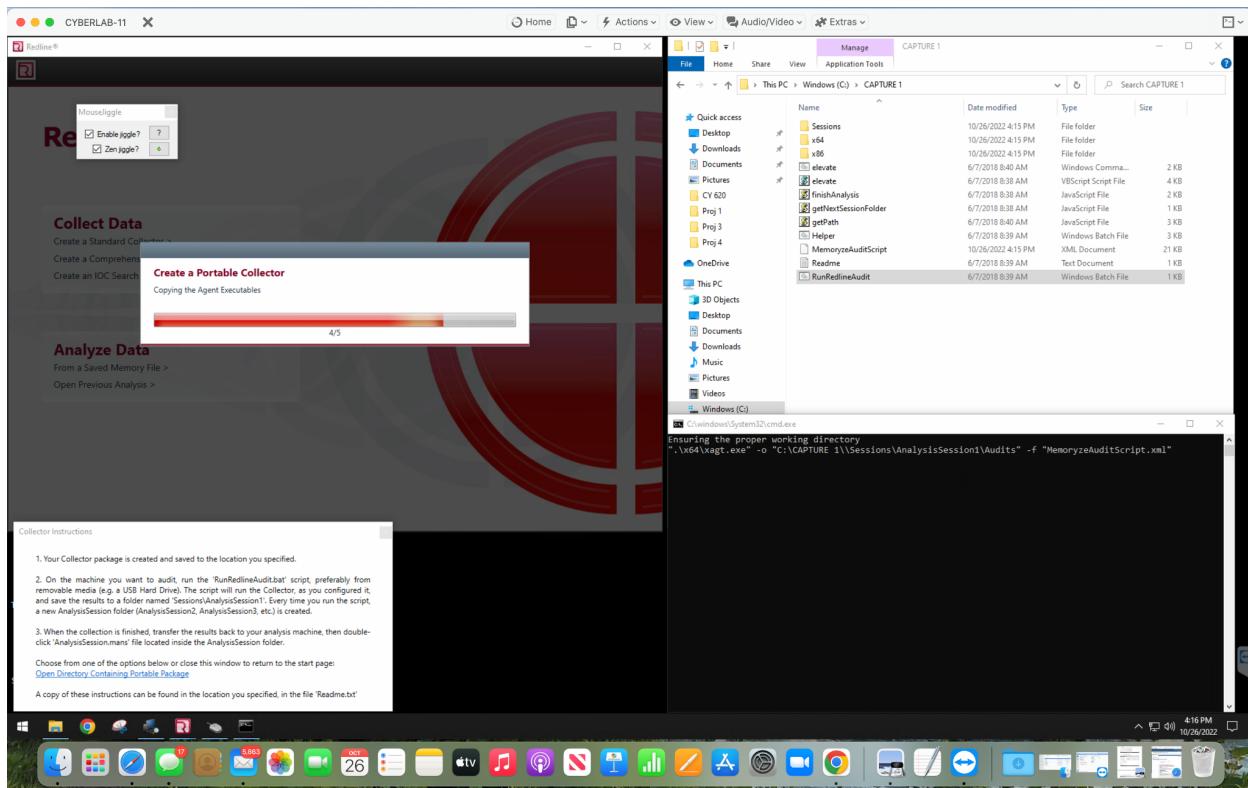
Host IOC Reports Not Collected

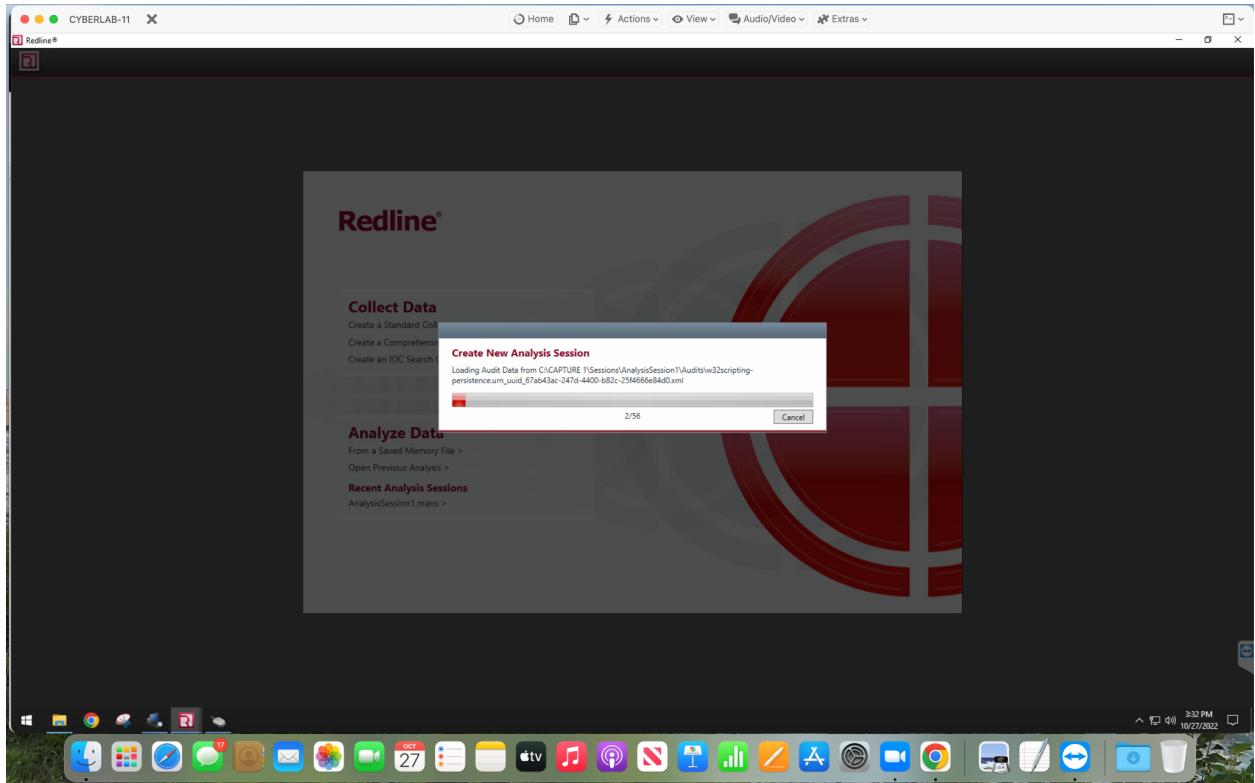
TimeCrunches™ 0 | TimeWrinkles™ 0

4:09 PM 10/26/2022

Comprehensive Analysis:

- It collects the most data that redline analyzes; it is typically utilized for a comprehensive analysis or when an expert only has one opportunity to get data from the system.
- Repeat the regular collection process with the exception of selecting the thorough collection option on the redline.
- It takes 7-8 hours approx. to get data from the computer, so be patient.
- After that, double-click on the report icon created by redline and wait 5-10 minutes for it to fully load into the redline. Then it will resemble this. Code within the RunRedlineAudit function.





The screenshot shows the Redline application window titled "CYBERLAB-11 - C:\CAPTURE\1\Session\AnalysisSession1.mans". The main menu bar includes Home, Actions, View, Audio/Video, and Extras. The left sidebar lists various data sources: System Information, Processes, Hierarchical Processes, File System, Registry, Windows Services, Persistence, Users, Tasks, Ports, DNS Entries, ARP Entries, Route Entries, Prefetch, Disks, Volumes, Registry Hives, Browser URL History, Cookie History, Form History, Timeline, Tags and Comments, and Acquisition History. The central content area is titled "Start Your Investigation" and contains three main sections: "I am Reviewing a Triage Collection from HX", "I am Investigating a Host Based on an External Investigative Lead", and "I am Reviewing Web History Data". Each section provides a brief description and an "Investigate >" button. At the bottom, there is a "I Want to Search My Data With a Set of Indicators of Compromise" section. The Mac OS X Dock at the bottom contains various application icons.

Redline - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home > Host > Processes

Analysis Data

Process Name	PID	Path	Arguments	Username	Start Time	Kernel Ti...	User Ti...	Hidden	Security...	SID Type	Parent Name	Par...	MDS
svchost.exe	2484	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-25 23:22:05Z	00000000	00000000		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
SearchIndexer.exe	120...	C:\windows\system32	C:\windows\system32\SearchIndex...	NT AUTHORITY\SYSTEM	2022-10-25 23:58:53Z	00000014	00000027		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	1588	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\LOCAL SERV...	2022-10-18 23:22:05Z	00000001	00000001		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
System	4			NT AUTHORITY\SYSTEM	2022-10-18 23:22:00Z	00000004	00000000		S-1-5-18	SidTypeWellKn...	0		
svchost.exe	3784	C:\windows\System32	C:\windows\System32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00000000	00000018		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	88	C:\windows\System32	C:\windows\System32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00000000	00000000		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
crrss.exe	824			NT AUTHORITY\SYSTEM	2022-10-18 23:22:04Z	00000000	00000000		S-1-5-18	SidTypeWellKn...		760	
Registry	124			NT AUTHORITY\SYSTEM	2022-10-18 23:21:58Z	00000001	00000000		S-1-5-18	SidTypeWellKn...	System	4	
WavesSvcd4.exe	4580	C:\Program Files\Waves\MaxxAudio	*C:\Program Files\Waves\MaxxAudio...	CYBERLAB-11\cybersecurity	2022-10-18 21:00:22Z	00000000	00000000		S-1-5-2...	SidTypeUser	Explorer.EXE	596	- 886...
sms.exe	628			NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00000000	00000000		S-1-5-18	SidTypeWellKn...		4	
services.exe	984			NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00000024	00000007		S-1-5-18	SidTypeWellKn...	wininit.exe	912	
svchost.exe	1432	C:\windows\System32	C:\windows\System32\svchost.exe...	NT AUTHORITY\NETWORK SE...	2022-10-18 23:22:05Z	00000002	00000004		S-1-5-20	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	1604	C:\windows\System32	C:\windows\System32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00000000	00000000		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
wininit.exe	912			NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00000000	00000000		S-1-5-18	SidTypeWellKn...		760	
armvsc.exe	3772	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0	*C:\Program Files (x86)\Common F...	CYBERLAB-11\cybersecurity	2022-10-18 23:22:06Z	00000000	00000000		S-1-5-2...	SidTypeUser		596	- 861...
lsass.exe	990	C:\windows\system32	C:\windows\system32\lsass.exe	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00000026	00000031		S-1-5-18	SidTypeWellKn...	wininit.exe	912	- 289d...
Memory Compression	2172			NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00000111	00000007		S-1-5-18	SidTypeWellKn...	System	4	
svchost.exe	1116	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	0000027	00000010		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	980	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	0000018	00000006		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
fontdhost.exe	1148	C:\windows\system32	*Font Driver Host\UMPD-O	Font Driver Host\UMPD-O	2022-10-18 23:22:05Z	00000000	00000000		S-1-5-9...	SidTypeWellKn...	wininit.exe	912	- 243f...
svchost.exe	3400	C:\windows\System32	C:\windows\System32\svchost.exe...	NT AUTHORITY\LOCAL SERV...	2022-10-18 23:22:06Z	00000000	00000000		S-1-5-19	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	1240	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\NETWORK SE...	2022-10-18 23:22:05Z	00000115	00000021		S-1-5-20	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	1476	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\LOCAL SERV...	2022-10-18 23:22:05Z	00000000	00000000		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	1284	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	0000068	00000006		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	1468	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\LOCAL SERV...	2022-10-18 23:22:05Z	00000000	00000000		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	3472	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:06Z	00000005	00000015		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	1724	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:05Z	00000000	00000005		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
RtkNGUI4.exe	9892	C:\Program Files\Realek\Audio\HDA	*C:\Program Files\Realek\Audio\HDA...	CYBERLAB-11\cybersecurity	2022-10-25 10:00:17Z	00000000	00000000		S-1-5-2...	SidTypeUser	Explorer.EXE	596	- 408...
svchost.exe	1612	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\LOCAL SERV...	2022-10-18 23:22:05Z	00000000	00000000		S-1-5-19	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	2316	C:\windows\System32	C:\windows\System32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:06Z	00000000	00000000		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	3036	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:06Z	00000000	00000000		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...
svchost.exe	2892	C:\windows\system32	C:\windows\system32\svchost.exe...	NT AUTHORITY\SYSTEM	2022-10-18 23:22:06Z	00000001	00000000		S-1-5-18	SidTypeWellKn...	services.exe	984	b718...

Host IOC Reports Not Collected Hide Whitelisted Items 174 items 3:51 PM 10/27/2022

Redline - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home > Host > System Information > Full Detailed Information

Analysis Data

Operating System

Operating System:	Windows 10 Enterprise 19044
Patch Level:	Windows 10 Enterprise
OS Build:	19044
Product ID:	00000101-1001-4A24-8...
System Directory:	C:\Windows\system32
Install Date:	2022-08-25 14:08:01Z
OS Bitness:	64-bit

Machine Information

Machine Name:	CYBERLAB-11
HostName:	CYBERLAB-11
System Date:	2022-10-26 20:29:42Z
Time Zone DST:	Eastern Standard Time
Time Zone Standard:	Eastern Standard Time
Processor Identity:	Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz
Processor Type:	Multiprocessor
Processor Manufacturer:	4GHz Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz
Primary IP Address:	192.168.1.163
Total Physical Memory:	31.89 Gigabytes
Available Physical Memory:	26.48 Gigabytes
Disk Free:	C:\ 4.67 GiB
Uptime:	7.21:07:42

User Information

Registered Owner:	Eduardo Rodriguez
Registered Organization:	Saint Peter's University
Domains:	SPC
Logged in User:	cybersecurity
Logged on User:	Font Driver Host\UMPD-0\SPC\CYBERLAB-11

BIOS Information

BIOS Date String:	Not Available
BIOS Version:	Not Available
BIOS Type:	Not Available

HX Information

Application Version:	22.41.5
Application Configuration Hash:	22.41.5.0
Cloud Hash:	00000000000000000000000000000000
Containment State:	normal
State Agent Status:	Unknown

Details Duplicates Tags & Comments

Host IOC Reports Not Collected 3:51 PM 10/27/2022

Redline® - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home ▸ Host ▸ File System ▸

Analysis Data

Filters

Enter string to find here... In All Fields Clear Column Filters Prev Next

Full Path	File Name	Size	Persist	Created	Modified	Accessed	Changed	Attributes	User...
c:\Windows\System32\securityhealthsystray.exe	securityhealthsystray.exe	8.803 Kilobytes	✓	2022-08-25 17:25:01Z	2018-10-31 16:43:46Z	2022-10-26 21:06:26Z	2022-10-25 20:55:48Z	Archive	NT SERV
c:\program files\Realtek\Audio\HDA\rkngui64.exe	rkngui64.exe	8.803 Kilobytes	✓	2022-08-25 17:25:01Z	2018-10-31 16:43:46Z	2022-10-26 21:06:26Z	2022-10-25 20:55:48Z	Archive	BUILTIN
c:\program files\Realtek\Audio\HDA\RAV8g64.exe	RAV8g64.exe	1.42 Megabytes	✓	2022-08-25 17:24:55Z	2018-10-31 16:43:42Z	2022-10-26 21:06:26Z	2022-10-25 20:55:34Z	Archive	BUILTIN
c:\program files\Waves\maxxaudio\wavevsc64.exe	wavevsc64.exe	706.961 Kilobytes	✓	2017-01-26 21:41:48Z	2017-07-26 21:41:48Z	2022-10-26 21:06:26Z	2022-10-25 20:55:49Z	Archive	NT AUTH
c:\Windows\System32\msv1_0.dll	msv1_0.dll	531.328 Kilobytes	✓	2022-08-26 17:01:15Z	2021-09-07 11:12:15Z	2022-10-26 21:06:27Z	2022-10-19 09:02:08Z	Archive	NT SERV
c:\Windows\System32\secdll.dll	secdll.dll	336.5 Kilobytes	✓	2022-10-18 17:01:03Z	2022-10-18 17:01:03Z	2022-10-26 21:06:27Z	2022-10-18 23:21:34Z	Archive	NT SERV
c:\Windows\System32\wow4cpu.dll	wow4cpu.dll	20.79 Kilobytes	✓	2021-05-07 11:11:52Z	2021-05-07 11:12:15Z	2022-10-26 21:06:27Z	2022-10-25 20:54:31Z	Archive	NT SERV
c:\Windows\System32\advapi32.dll	advapi32.dll	683.516 Kilobytes	✓	2022-10-18 17:01:12Z	2022-10-18 17:01:12Z	2022-10-26 21:06:27Z	2022-10-25 23:23:00Z	Archive	NT SERV
c:\Windows\System32\cbcqnt.dll	cbcqnt.dll	687.461 Kilobytes	✓	2022-10-18 17:01:22Z	2022-10-18 17:01:22Z	2022-10-26 21:06:27Z	2022-10-25 23:24:28Z	Archive	NT SERV
c:\Windows\System32\combase.dll	combase.dll	3.341 Megabytes	✓	2022-10-18 17:01:23Z	2022-10-18 17:01:23Z	2022-10-26 21:06:27Z	2022-10-25 23:23:00Z	Archive	NT SERV
c:\Windows\System32\configd32.dll	configd32.dll	8.8 Kilobytes	✓	2022-08-26 16:53:36Z	2022-08-26 16:53:36Z	2022-10-26 21:06:28Z	2022-10-25 20:55:34Z	Archive	NT SERV
c:\Windows\System32\comi2.dll	comi2.dll	476.664 Kilobytes	✓	2021-05-07 11:11:56Z	2021-05-07 11:11:56Z	2022-10-26 21:06:29Z	2022-10-25 20:54:31Z	Archive	NT SERV
c:\Windows\System32\difapi.dll	difapi.dll	347 Kilobytes	✓	2019-12-07 09:05Z	2019-12-07 09:05Z	2022-10-26 21:06:29Z	2022-10-18 17:02:10Z	Archive	NT SERV
c:\Windows\System32\gdi32.dll	gdi32.dll	160.438 Kilobytes	✓	2022-10-18 17:01:16Z	2022-10-18 17:01:16Z	2022-10-26 21:06:29Z	2022-10-25 23:23:00Z	Archive	NT SERV
c:\Windows\System32\gdiplus.dll	gdiplus.dll	1.63 Megabytes	✓	2022-10-18 17:01:28Z	2022-10-18 17:01:28Z	2022-10-26 21:06:29Z	2022-10-18 23:21:36Z	Archive	NT SERV
c:\Windows\System32\imagehlp.dll	imagehlp.dll	104.891 Kilobytes	✓	2022-04-04 03:36Z	2022-04-04 03:36Z	2022-10-26 21:06:29Z	2022-10-25 20:55:34Z	Archive	NT SERV
c:\Windows\System32\imm32.dll	imm32.dll	181.102 Kilobytes	✓	2021-05-07 11:12:13Z	2021-05-07 11:12:13Z	2022-10-26 21:06:30Z	2022-10-25 20:55:34Z	Archive	NT SERV
c:\Windows\System32\kernel32.dll	kernel32.dll	748.047 Kilobytes	✓	2022-08-26 16:53:45Z	2022-08-26 16:53:45Z	2022-10-26 21:06:29Z	2022-10-25 20:54:31Z	Archive	NT SERV
c:\Windows\System32\mscnd.dll	mscnd.dll	1.076 Megabytes	✓	2022-10-18 17:01:26Z	2022-10-18 17:01:26Z	2022-10-26 21:06:30Z	2022-10-25 23:40:33Z	Archive	NT SERV
c:\Windows\System32\msvcrt.dll	msvcrt.dll	622.422 Kilobytes	✓	2021-05-07 11:12:02Z	2021-05-07 11:12:02Z	2022-10-26 21:06:31Z	2022-10-25 20:54:31Z	Archive	NT SERV
c:\Windows\System32\normaliz.dll	normaliz.dll	6 Kilobytes	✓	2021-05-07 11:12:42Z	2021-05-07 11:12:42Z	2022-10-26 21:06:31Z	2022-10-25 20:55:37Z	Archive	NT SERV
c:\Windows\System32\nsdl.dll	nsdl.dll	24.211 Kilobytes	✓	2021-05-07 11:12:12Z	2021-05-07 11:12:12Z	2022-10-26 21:06:31Z	2022-10-25 20:54:31Z	Archive	NT SERV
c:\Windows\System32\ole32.dll	ole32.dll	1.158 Megabytes	✓	2021-09-15 03:36Z	2021-09-15 03:36Z	2022-10-26 21:06:31Z	2022-10-25 20:54:31Z	Archive	NT SERV
c:\Windows\System32\oleaut32.dll	oleaut32.dll	812.055 Kilobytes	✓	2021-06-04 03:33Z	2021-06-04 03:33Z	2022-10-26 21:06:31Z	2022-10-25 20:54:31Z	Archive	NT SERV
c:\Windows\System32\oapi.dll	oapi.dll	18.695 Kilobytes	✓	2021-05-07 11:12:23Z	2021-05-07 11:12:23Z	2022-10-26 21:06:31Z	2022-10-25 20:55:05Z	Archive	NT SERV
c:\Windows\System32\pcrctd.dll	pcrctd.dll	1.141 Megabytes	✓	2022-08-26 16:53:34Z	2022-08-26 16:53:34Z	2022-10-26 21:06:31Z	2022-10-25 20:54:31Z	Archive	NT SERV
c:\Windows\System32\psched.dll	psched.dll	615.914 Kilobytes	✓	2022-08-26 16:53:34Z	2022-08-26 16:53:34Z	2022-10-26 21:06:31Z	2022-10-25 20:54:31Z	Archive	NT SERV
c:\Windows\System32\setupapi.dll	setupapi.dll	4.461 Megabytes	✓	2022-08-26 16:53:43Z	2022-08-26 16:53:43Z	2022-10-26 21:06:42Z	2022-10-25 20:54:31Z	Archive	NT SERV
c:\Windows\System32\SHCore.dll	SHCore.dll	684.469 Kilobytes	✓	2022-08-26 16:53:27Z	2022-08-26 16:53:27Z	2022-10-26 21:06:37Z	2022-10-25 20:54:31Z	Archive	NT SERV
c:\Windows\System32\shell32.dll	shell32.dll	7.291 Megabytes	✓	2022-10-18 17:01:26Z	2022-10-18 17:01:26Z	2022-10-26 21:06:52Z	2022-10-25 23:23:00Z	Archive	NT SERV
c:\Windows\System32\shlwapi.dll	shlwapi.dll	335.43 Kilobytes	✓	2022-10-18 17:01:26Z	2022-10-18 17:01:26Z	2022-10-26 21:07:08Z	2022-10-25 23:09:22Z	Archive	NT SERV
c:\Windows\System32\user32.dll	user32.dll	1.616 Megabytes	✓	2022-10-18 17:01:19Z	2022-10-18 17:01:19Z	2022-10-26 21:07:08Z	2022-10-25 23:23:00Z	Archive	NT SERV

Host IDC Reports Not Collected Apply Selections Recursively Hide Whitelisted Items 571,681 items 3:51 PM 10/27/2022

Redline® - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home ▸ Host ▸ Registry

Analysis Data

Filters

Enter string to find here... In All Fields Clear Column Filters Prev Next

Path	Type	Text Value	Username	Security...	Modified	Reported Length	Persist	Value Name	Hive
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\swindrl\system32\Sec...	REG_EXPAND_SZ	%windrl\system32\Sec...	NT AUTHORITY\SYSTEM	S-1-5-18	2022-08-23 17:06:57Z	88 Bytes	✓	SecurityHealth	HKEY_LOCAL_M
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\REG_SZ	"C:\Program Files\Rea...	NT AUTHORITY\SYSTEM	S-1-5-18	2022-08-23 17:06:57Z	108 Bytes	✓	RHID\VCpl	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\REG_SZ	"C:\Program Files\Rea...	NT AUTHORITY\SYSTEM	S-1-5-18	2022-08-23 17:06:57Z	160 Bytes	✓	RHID\Vbg_MAX06	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\REG_SZ	"C:\Program Files\Wav...	NT AUTHORITY\SYSTEM	S-1-5-18	2022-08-23 17:06:57Z	100 Bytes	✓	WavesSrc	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\Software\Classes\battlefield_shooter\REG_SZ	%"1%"	NT AUTHORITY\SYSTEM	S-1-5-18	2019-12-07 09:17:32Z	16 Bytes	✓			HKEY_LOCAL_M
HKEY_LOCAL_MACHINE\Software\Classes\Wow6432Node\Microsoft\REG_DWORD	0	NT AUTHORITY\SYSTEM	S-1-5-18	2022-08-12 15:09:15Z	4 Bytes	✓	DisableExceptionChain\va...	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\REG_QWORD	256	NT AUTHORITY\SYSTEM	S-1-5-18	2022-05-11 09:17:52Z	8 Bytes	✓	MitigationOptions	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\REG_DWORD	1	BUILTIN\Administrators	S-1-5-1...	2021-05-07 12:47:15Z	4 Bytes	✓	MaxLoaderThreads	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\REG_QWORD	4294967296	NT AUTHORITY\SYSTEM	S-1-5-18	2019-12-07 09:17:22Z	8 Bytes	✓	MitigationOptions	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\REG_QWORD	1677732	NT AUTHORITY\SYSTEM	S-1-5-18	2021-11-10 04:44:32Z	8 Bytes	✓	MitigationOptions	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\REG_DWORD	1118481	NT AUTHORITY\SYSTEM	S-1-5-18	2019-12-07 09:17:22Z	8 Bytes	✓	MitigationOptions	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\REG_QWORD	2097152	NT AUTHORITY\SYSTEM	S-1-5-18	2019-10-09 07:17:22Z	8 Bytes	✓	MitigationOptions	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\REG_DWORD	32768	NT AUTHORITY\SYSTEM	S-1-5-18	2019-12-07 09:17:22Z	4 Bytes	✓	MinimumStackCommitt...	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	msv__0	NT AUTHORITY\SYSTEM	S-1-5-18	2022-10-18 23:22:05Z	16 Bytes	✓	Authentication Packages	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	secl__0	NT AUTHORITY\SYSTEM	S-1-5-18	2022-10-18 23:22:05Z	8 Bytes	✓	Notification Packages	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	REG_MULTI_SZ	NT AUTHORITY\SYSTEM	S-1-5-18	2022-10-18 23:22:05Z	8 Bytes	✓	Security Packages	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	wow64cpu.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	26 Bytes	✓	_wow64cpu	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	wow64mb.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	26 Bytes	✓	_wow64mb	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	xtai__0	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	22 Bytes	✓	_xtai__0	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	advapi32.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	26 Bytes	✓	advapi32	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	cbcqnt.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	24 Bytes	✓	cbcqnt	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	combase.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	24 Bytes	✓	combase	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	COMOLG32.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	26 Bytes	✓	COMOLG32	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	comi2.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	20 Bytes	✓	comi2	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	difapi.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	24 Bytes	✓	DifApi	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	gdi32.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	20 Bytes	✓	gdi32	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	gdplus.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	24 Bytes	✓	gdplus	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	IMAGEHLP.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	26 Bytes	✓	IMAGEHLP	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	IMM32.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	20 Bytes	✓	IMM32	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	kern32.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	26 Bytes	✓	kern32	HKEY_LOCAL_M	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\REG_MULTI_SZ	MSVCR7.dll	NT SERVICE\TrustedInstaller	S-1-5-8...	2019-12-07 09:15:08Z	22 Bytes	✓	MSVCR7	HKEY_LOCAL_M	

Host IDC Reports Not Collected Apply Selections Recursively 1,653,535 items 3:52 PM 10/27/2022

Redline® - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home > Host > Users

Analysis Data

Enter string to find here... In All Fields Prev Next

Username	SID	SID Type	Full Name	Description	Last Login	Disable	Locker	Passw.	User Pass.	Group Names	Home Directory	Script Path*
admin	S-1-5-2...	SidTypeUser	CYBERLAB-11\admin	Built-in account for administering the c...	2022-08-29 17:23:55Z	✓	✓	1149.04...	None	Administrators;Users		
Administrator	S-1-5-2...	SidTypeUser	CYBERLAB-11\Administr...	Built-in account for administering the c...	2022-08-26 14:33:07Z	✓	✓	62.1038.13	None	Administrators		
cybersecurity	S-1-5-2...	SidTypeUser	CYBERLAB-11\cybersecu...		2022-10-25 21:00:00Z	✓	✓	50.0732.25	None	Administrators;Users		
DefaultAccount	S-1-5-2...	SidTypeUser	CYBERLAB-11\DefaultAcc...	A user account managed by the system.	1970-01-01 00:00:00Z	✓	✓	0000000	None	System Managed...		
Guest	S-1-5-2...	SidTypeUser	CYBERLAB-11\Guest	Built-in account for guest access to the...	1970-01-01 00:00:00Z	✓	✓	0000000	None	Guests		
WDAGUtilityAccount	S-1-5-2...	SidTypeUser	CYBERLAB-11\WDAGUI...	A user account managed and used by the...	1970-01-01 00:00:00Z	✓	✓	1160.06...	None			
DWM-3	S-1-5-9...	SidTypeUser	Window Manager\DW...	Font Driver Host\UMD-3				0000000				
UMD-3	S-1-5-9...	SidTypeUser	Font Driver Host\UMD-3	Font Driver Host\UMD-3				0000000				
LOCAL SERVICE	S-1-5-19	SidTypeWellKnownGroup	NT AUTHORITY\LOCAL...					0000000				
CYBERLAB-11\$			\$P\$CYBERLAB-11\$					0000000				
UMFD-0	S-1-5-9...	SidTypeUser	Font Driver Host\UMFD-0	Font Driver Host\UMFD-0				0000000				

Host IOC Reports Not Collected

3:52 PM 10/27/2022

Redline® - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home > Host > Tasks

Analysis Data

Enter string to find here... In All Fields Prev Next

Name	Comment	Status	Priority	Ext...	Creator	Account Name	Virtual Path	Account Run Le...	Account Logon...	Flags	Appli...
Adobe Acrobat Update...	This task keeps your Ado...	SCHED_5_TASK...	HIGH_PRIORITY...	0	Adobe Systems Incorporated		\Adobe Acrobat Update Task	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
CCleanerSkiCAC...	admin	SCHED_5_TASK...	HIGH_PRIORITY...	267...	CCleanerSkiCAC - admin		\CCleanerSkiCAC - admin	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
GoogleUpdateTaskMachine...	Keeps your Google softw...	SCHED_5_TASK...	HIGH_PRIORITY...	0	SYSTEM		\GoogleUpdateTaskMachineCore	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
GoogleUpdateTaskMachine...	Keeps your Google softw...	SCHED_5_TASK...	HIGH_PRIORITY...	0	SYSTEM		\GoogleUpdateTaskMachineUA	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
MicrosoftEdgeUpdateTask...	Keeps your Microsoft sof...	SCHED_5_TASK...	HIGH_PRIORITY...	0	SYSTEM		\MicrosoftEdgeUpdateTaskMachineCore\TaskId43138a092e2f	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
MicrosoftEdgeUpdateTask...	Keeps your Microsoft sof...	SCHED_5_TASK...	HIGH_PRIORITY...	0	SYSTEM		\MicrosoftEdgeUpdateTaskMachineUA	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
npcapwatchdog	Ensure Npcap service is c...	SCHED_5_TASK...	HIGH_PRIORITY...	0	SYSTEM		\npacketwatchdog	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
OneDrive Reporting Task...	OneDrive Reporting Task...	SCHED_5_TASK...	HIGH_PRIORITY...	0	Microsoft Corporation	admin	\OneDrive Reporting Task-5-1-5-21-2052132785-1385840126...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
OneDrive Reporting Task...	OneDrive Reporting Task...	SCHED_5_TASK...	HIGH_PRIORITY...	0	Microsoft Corporation	cybersecurity	\OneDrive Reporting Task-5-1-5-21-2052132785-1385840126...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
OneDrive Reporting Task...	OneDrive Reporting Task...	SCHED_5_TASK...	HIGH_PRIORITY...	0	Microsoft Corporation	Administrator	\OneDrive Reporting Task-5-1-5-21-2052132785-1385840126...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
OneDrive Standalone Up...	OneDrive Standalone Up...	SCHED_5_TASK...	HIGH_PRIORITY...	267...	Microsoft Corporation	admin	\OneDrive Standalone Update Task-5-1-5-21-2052132785-1385840126...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
OneDrive Standalone Up...	OneDrive Standalone Up...	SCHED_5_TASK...	HIGH_PRIORITY...	214...	Microsoft Corporation	cybersecurity	\OneDrive Standalone Update Task-5-1-5-21-2052132785-1385840126...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
RtbdVb8g.PushButton	RtbdVb8g.PushButton	SCHED_5_TASK...	HIGH_PRIORITY...	267...	Realtek	Administrator	\RtbdVb8g.PushButton	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
Office Automatic Update...	This task ensures that yo...	SCHED_5_TASK...	HIGH_PRIORITY...	0	Microsoft Office	SYSTEM	\Microsoft\Office\Office Automatic Updates 2.0	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
Office ClickToRun Service...	This task monitors the st...	SCHED_5_TASK...	HIGH_PRIORITY...	0	Microsoft Office	SYSTEM	\Microsoft\Office\Office ClickToRun Service Monitor	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
OfficeBackgroundTask...	This task initiates Office...	SCHED_5_TASK...	HIGH_PRIORITY...	0	Microsoft Office		\Microsoft\Office\OfficeBackgroundTaskHandler\Logs	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
OfficeBackgroundTask...	This task initiates Office...	SCHED_5_TASK...	HIGH_PRIORITY...	0	Microsoft Office		\Microsoft\Office\OfficeBackgroundTaskHandler\Registration	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
OfficeTelemetryAgent...	This task initiates the bac...	SCHED_5_TASK...	HIGH_PRIORITY...	0	Microsoft\Office\OfficeTelemetryAgent\FallBack2016			TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
OfficeTelemetryAgentLo...	This task initiates Office...	SCHED_5_TASK...	HIGH_PRIORITY...	0	Microsoft\Office\OfficeTelemetryAgent\LogOn2016			TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
.NET Framework NGEN...		SCHED_5_TASK...	HIGH_PRIORITY...	0	SYSTEM		\Microsoft\Windows\NET Framework\NET Framework NGEN...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
.NET Framework NGEN...		SCHED_5_TASK...	HIGH_PRIORITY...	0	SYSTEM		\Microsoft\Windows\NET Framework\NET Framework NGEN...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
.NET Framework NGEN...		SCHED_5_TASK...	HIGH_PRIORITY...	0	SYSTEM		\Microsoft\Windows\NET Framework\NET Framework NGEN...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_HIDDEN...	
.NET Framework NGEN...		SCHED_5_TASK...	HIGH_PRIORITY...	0	SYSTEM		\Microsoft\Windows\NET Framework\NET Framework NGEN...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_HIDDEN...	
AD RMS Rights Policy Te...	Updates the AD RMS rig...	SCHED_5_TASK...	HIGH_PRIORITY...	267...	Microsoft Corporation		\Microsoft\Windows\Active Directory Rights Management Se...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_KILL_ON_IDLE...	
AD RMS Rights Policy Te...	Updates the AD RMS rig...	SCHED_5_TASK...	HIGH_PRIORITY...	267...	Microsoft Corporation		\Microsoft\Windows\Active Directory Rights Management Se...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
EDP Policy Manager	This task performs steps...	SCHED_5_TASK...	HIGH_PRIORITY...	267...	Microsoft Corporation	LOCAL SERVICE	\Microsoft\Windows\Appl\EDP Policy Manager	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
PolicyConverter	Converts the software re...	SCHED_5_TASK...	HIGH_PRIORITY...	267...	Microsoft Corporation	SYSTEM	\Microsoft\Windows\Appl\PolicyConverter	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_KILL_ON_IDLE...	
VerifiedPublisherCertStor...	Inspects the Appl certifi...	SCHED_5_TASK...	HIGH_PRIORITY...	267...	Microsoft Corporation	LOCAL SERVICE	\Microsoft\Windows\Appl\VerifiedPublisherCertStoreCheck	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_KILL_ON_IDLE...	
Microsoft Compatibility...	\$!\$@%SystemRoot%\syst...	SCHED_5_TASK...	HIGH_PRIORITY...	0	\$!\$@%SystemRoot%\system32...	SYSTEM	\Microsoft\Windows\Application Experience\Microsoft Comp...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
PuaPatch0Task	Updates compatibility da...	SCHED_5_TASK...	HIGH_PRIORITY...	0	Microsoft Corporation	SYSTEM	\Microsoft\Windows\Application Experience\PuaPatch0Task	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	
ProgramDataUpdater	\$!\$@%SystemRoot%\syst...	SCHED_5_TASK...	HIGH_PRIORITY...	0	\$!\$@%SystemRoot%\system32...	SYSTEM	\Microsoft\Windows\Application Experience\ProgramDataUpd...	TASK_RUNLEVEL...	TASK_LOGON...	TASK_FLAG_DISABLED...	

Host IOC Reports Not Collected

3:52 PM 10/27/2022

Redline - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home > Host > DNS Entries > Full Detailed Information

DNS Entry

Analysis Data

- System Information
- Processes
- Hierarchical Processes
- File System
- Registry
- Windows Services
- Persistence
- Users
- Tasks
- Ports
- DNS Entries
- ARP Entries
- Route Entries
- Prefetch
- Disks
- Volumes
- Registry Hives
- Browser URL History
- Cookie History
- Form History
- Timeline
- Tags and Comments
- Acquisition History

DNS Entry

Host:	94.204.194.173.in-addr.arpa
Record Name:	94.204.194.173.in-addr.arpa
Record Type:	PTR
Flags:	Arpaer
Data Length:	8 Bytes
Time To Live:	020444

Record Data

Host:	94.204.194.1e100.net
IPv4 Address:	Not Available
IPv6 Address:	Not Available
Address Type:	Not Available
Primary Server Name:	Not Available
Administrator Name:	Not Available
Geo-Location:	Not Available
Referer:	Not Available
Retry:	Not Available
Expire:	Not Available
Expiration Date:	Not Available
Default Time To Live:	Not Available
Original Time To Live:	Not Available
Mailbox Name:	Not Available
Mailbox Owners Name:	Not Available
MX Host:	Not Available
Preference:	Not Available
Binmask:	Not Available
Algorithm:	Not Available
Protocol:	Not Available
Key Name:	Not Available
Key Length:	Not Available
Key Flags:	Not Available
Key Tag:	Not Available
Signature:	Not Available
Date Signed:	Not Available
Type Covered:	Not Available
Label Count:	Not Available
Next Host:	Not Available
Target Host:	Not Available
Priority:	Not Available
Weight:	Not Available
Port:	Not Available
Order:	Not Available
Service:	Not Available
Regular Expression:	Not Available
Replacement:	Not Available
Digest Type:	Not Available
Digest Length:	Not Available
Creation Date:	Not Available
Error:	Not Available
Mode:	Not Available
Signature Length:	Not Available
Fudge Time:	Not Available
Original XID:	Not Available
Mapping Flag:	Not Available
Lookup Timeout:	Not Available

Host **IOC Reports** **Not Collected**

3:52 PM 10/27/2022

Redline - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home > Host > ARP Entries

Analysis Data

- System Information
- Processes
- Hierarchical Processes
- File System
- Registry
- Windows Services
- Persistence
- Users
- Tasks
- Ports
- DNS Entries
- ARP Entries
- Route Entries
- Prefetch
- Disks
- Volumes
- Registry Hives
- Browser URL History
- Cookie History
- Form History
- Timeline
- Tags and Comments
- Acquisition History

ARP Entries

Cache Type	IPv4 Address	MAC Address	State	ARP Interface	Interface Type	IsRout...	Last Rec...	Last Unre...
Static	224.0.22	00-00-00-00-00-00	127.0.0.1					
Static	224.0.251	00-00-00-00-00-00	127.0.0.1					
Static	224.0.252	00-00-00-00-00-00	127.0.0.1					
Static	239.25.252.250	00-00-00-00-00-00	127.0.0.1					
Invalid	169.254.255.255	00-00-00-00-00-00	192.168.1.163					
Dynamic	192.168.1.1	00-0c-29-18-72-fd	192.168.1.163					
Dynamic	192.168.1.153	48-4d-7e-ee-35-4e	192.168.1.163					
Dynamic	192.168.1.155	48-4d-7e-ee-3c-0e	192.168.1.163					
Dynamic	192.168.1.157	48-4d-7e-ed-ea-86	192.168.1.163					
Dynamic	192.168.1.164	48-4d-7e-ee-3b-2e	192.168.1.163					
Dynamic	192.168.1.166	48-4d-7e-ee-37-e0	192.168.1.163					
Dynamic	192.168.1.167	48-4d-7e-ee-39-60	192.168.1.163					
Dynamic	192.168.1.168	48-4d-7e-ed-e5-7e	192.168.1.163					
Dynamic	192.168.1.169	48-4d-7e-ee-3b-2e	192.168.1.163					
Dynamic	192.168.1.226	6c-2b-59-e0-b6-05	192.168.1.163					
Dynamic	192.168.1.227	78-2b-4f-e8-a9-2e	192.168.1.163					
Dynamic	192.168.1.240	48-4d-7e-ee-38-73	192.168.1.163					
Static	192.168.1.255	ff-ff-ff-ff-ff-ff	192.168.1.163					
Static	224.0.22	01-00-5e-00-00-16	192.168.1.163					
Static	224.0.251	01-00-5e-00-00-fb	192.168.1.163					
Static	224.0.252	01-00-5e-00-00-fc	192.168.1.163					
Static	239.25.252.250	01-00-5e-7f-ff-ff	192.168.1.163					
Static	251.25.252.250	ff-ff-ff-ff-ff-ff	192.168.1.163					
Static	192.168.126.255	ff-ff-ff-ff-ff-ff	192.168.126.1					
Static	224.0.22	01-00-5e-00-00-16	192.168.126.1					
Static	224.0.251	01-00-5e-00-00-fb	192.168.126.1					
Static	224.0.252	01-00-5e-00-00-fc	192.168.126.1					
Static	239.25.252.250	01-00-5e-7f-ff-ff	192.168.126.1					
Static	251.25.252.250	ff-ff-ff-ff-ff-ff	192.168.126.1					
Static	192.168.145.120	ff-ff-ff-ff-ff-ff	192.168.145.1					
Invalid	192.168.145.128	00-0c-29-30-71-e3	192.168.145.1					
Dynamic	192.168.145.130	00-00-00-00-00-00	192.168.145.1					
Dynamic	192.168.145.131	00-0c-29-f9-9e-b	192.168.145.1					
Static	192.168.145.255	ff-ff-ff-ff-ff-ff	192.168.145.1					
Static	224.0.22	01-00-5e-00-00-16	192.168.145.1					

Host **IOC Reports** **Not Collected**

3:53 PM 10/27/2022

Redline® - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home > Host > Disks

Analysis Data

Disk Name Disk Size

- \PhysicalDrive0 931.513 Gigabytes
- \PhysicalDrive1 931.513 Gigabytes
- \CdRom0

IOC Reports Not Collected

Host IOC Reports Not Collected

3:53 PM 10/27/2022

This screenshot shows the Redline software interface for disk analysis. The main window displays a table of disk information with columns for Disk Name and Disk Size. Three drives are listed: \PhysicalDrive0, \PhysicalDrive1, and \CdRom0, all showing 931.513 Gigabytes. The left sidebar contains a navigation tree with various system and network monitoring categories like Processes, File System, Registry, and DNS Entries.

Redline® - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home > Host > Volumes

Analysis Data

Drive Name Volume Name Type Device Path File System Name Bytes per Sector Sectors per Total Allo Available Serial Number Creation Time Mount File System

Drive	Name	Volume Name	Type	Device Path	File System Name	Bytes per Sector	Sectors per	Total Allo.	Available	Serial Number	Creation Time	Mount	File System
F	HDD	\\?\Volume[a]56bcc22-27... DRIVE_FIXED	Device\HarddiskVolume3		NTFS	512 Bytes	8	244,029...	243,047...	110961814	2022-08-29 17:13:09Z	✓	FILE_CASE
D	Storage	\\?\Volume[e]e50341-46...	DRIVE_FIXED	Device\HarddiskVolume7	NTFS	512 Bytes	8	127,540...	76,103,644	1551697619	2022-08-25 17:24:10Z	✓	FILE_CASE
C	Windows	\\?\Volume[a]a9990fa-34...	DRIVE_FIXED	Device\HarddiskVolume6	NTFS	512 Bytes	8	115,199...	22,543,198	377278907	2022-08-25 17:24:09Z	✓	FILE_CASE
	Recovery	\\?\Volume[3558bd5d13...	DRIVE_FIXED	Device\HarddiskVolume8	NTFS	512 Bytes	8	1,288,703...	1,091,487	3464353988	2022-08-25 17:24:11Z	✓	FILE_CASE
	BOOT	\\?\Volume[c]0900-106-71...	DRIVE_FIXED	Device\HarddiskVolume1	FAT32	512 Bytes	8	126,120...	115,506	3632537779	1601-01-01 00:00:00Z	✓	FILE_CASE
	BOOT	\\?\Volume[b]8c17975-7c...	DRIVE_FIXED	Device\HarddiskVolume4	FAT32	512 Bytes	8	126,720...	119,666	1484557297	1601-01-01 00:00:00Z	✓	FILE_CASE
										377278907	2022-08-25 17:24:09Z		
										110961814	2022-08-29 17:13:09Z		
										1551697619	2022-08-25 17:24:10Z		
										3324626092	1601-01-01 00:00:00Z		
										2457992776	1601-01-01 00:00:00Z		

IOC Reports Not Collected

Host IOC Reports Not Collected

3:53 PM 10/27/2022

This screenshot shows the Redline software interface for volume analysis. The main window displays a table of volume information with columns for Drive, Name, Volume Name, Type, Device Path, File System Name, Bytes per Sector, Sectors per, Total Allo., Available, Serial Number, Creation Time, Mount, and File System. The table lists several volumes including F (HDD), D (Storage), C (Windows), Recovery, and two additional volumes. The left sidebar contains a navigation tree with categories like Processes, File System, Registry, and DNS Entries.

Redline® - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home > Host > Browser URL History

Analysis Data

Review Browser URL History

When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review URLs which can lead to a malware server, and hidden visits which can include sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field filter to investigate any file downloads or cookies being sent around the same time period.

All URL Records
Shows all URL records.

Redirects
Shows all URL records for visit types that were a variation of a redirect, which is often used to source a user from one website before they reach a malware staging server.

Visit From
Shows all records generated after the user first viewed another page, which can be valuable information in determining a sequence of events.

Visited Once
Shows only records that had exactly one visit; rarely visited sites are an indication of suspicious activity.

Visited Bookmarked URLs
Shows only records that were visited from a bookmark; bookmarked sites are an indication of preferential treatment.

Typed URLs
Shows only records that were visited after the user typed in the URL, which indicates that the user was aware of the site.

Hidden Visits
Shows all records accessed without the user's direct knowledge, including hidden Iframes often used by embedded ad sites which could be potentially infected with malicious obfuscated javascript.

Filters

Enter string to find here... In All Fields Clear Column Filters Prev Next

Visit Type	URL	Page Title	Hostname	Typed	Visit From	Visit Count	First Visit Date	Last Visit Date	Last Visit I...
URL	https://support.microsoft.com/en-us/windows?ui=en...					0	2020-10-28 20:43:22		
URL	https://www.youtube.com/ad_companionAdvertiser...					0	2020-10-28 20:48:59Z		
URL	https://www.youtube.com/watch?v=MfydPNtVx0					0	2020-10-28 20:52:07Z		
URL	https://www.youtube.com/					0	2020-10-28 20:41:41Z		
URL	https://www.youtube.com/results?search_query=how...					0	2020-10-28 20:41:37Z		
URL	https://www.youtube.com/embed/controls/0kenab...					0	2020-10-28 20:41:38Z		
URL	https://www.youtube.com/watch?v=WngcogkqL_U					0	2020-10-28 20:49:39Z		
URL	https://www.youtube.com/watch?v=Gc4XmW9CA					0	2020-10-28 20:56:06Z		
URL	https://www.youtube.com/watch?v=Gj0PxhGUU					0	2020-10-28 20:42:03Z		
URL	https://www.bing.com/search?q=how+to+get+help+...					0	2020-09-30 18:03:42Z		
URL	https://www.bing.com/search?q=systeminform...					0	2020-10-28 20:41:38Z		
URL	https://support.microsoft.com/					0	2020-10-28 20:40:31Z		
URL	https://support.microsoft.com/en-us/windows?ui=en...					0	2020-10-28 20:40:33Z		
URL	https://www.youtube.com/watch?v=MfydPNtVx0					0	2020-10-28 20:52:05Z		
URL	https://www.youtube.com/					0	2020-10-28 20:41:37Z		
URL	https://www.youtube.com/results?search_query=how...					0	2020-10-28 20:41:56Z		
URL	https://www.youtube.com/watch?v=WngcogkqL_U					0	2020-10-28 20:49:38Z		
URL	https://www.youtube.com/watch?v=Gc4XmW9CA					0	2020-10-28 20:56:05Z		
URL	https://www.youtube.com/watch?v=Gj0PxhGUU					0	2020-10-28 20:42:00Z		
URL	https://www.msn.com/					0	2020-09-30 18:08:44Z		
URL	https://www.bing.com/					0	2020-09-30 18:03:41Z		
URL	https://www.bing.com/r/17/q/nj650pjhq1n.log...					0	2022-08-29 17:10:58Z		
URL	https://www.bing.com/th?id=OOSC.TOO154D10C490B...					0	2022-08-29 17:24:04Z		
URL	https://www.bing.com/th?id=OOSWG.2bb2aa6f-B10...					0	2022-08-29 17:24:04Z		
URL	https://www.bing.com/r/5pjq/njAnesLVWhzHn2f...					0	2022-08-29 17:24:00Z		
URL	https://www.bing.com/th?id=OOSWG.2f72655-c26...					0	2022-08-29 17:24:01Z		
URL	https://www.bing.com/r/17/q/njFltEdhNqTYdee...					0	2022-08-29 17:24:00Z		
URL	https://www.bing.com/th?id=OOSC.TOO154D92AE1...					0	2022-08-29 17:24:04Z		
URL	https://www.bing.com/th?id=OOSWG.8e131820-e...					0	2022-08-29 17:24:01Z		
URL	https://www.bing.com/th?id=ALSTUF9F94863AE3047F...					0	2022-08-29 17:24:04Z		
URL	https://fp-as.azureedge.net/app/trans.g/f1f84ec08...					0	2022-08-29 17:12:27Z		
URL	https://fp-as.azureedge.net/app/trans.g/f776acfbac54...					0	2022-08-29 17:12:27Z		

Host IDC Reports Not Collected

3:53 PM 10/27/2022

Redline® - C:\CAPTURE\1\Sessions\AnalysisSession1\AnalysisSession1.mans

Home > Host > Form History > Full Detailed Information

Analysis Data

Form Information

Type:	Normal
Field Name:	searcher-history
Field Value:	duck
Username Field Name:	Not Available
Username Field Value (Possibly Encrypted):	Not Available
Password Field Name:	Not Available
Password Field Value (Encrypted):	Not Available
Encryption Application GUID:	Not Available
Submission URL:	Not Available
Hostname:	Not Available
HTTP Method:	Not Available
# of Times Used:	1

Form Timestamps

Last Used:	2022-04-27 20:16:44Z
First Used:	2022-04-27 20:16:46Z
Creation Date:	Not Available

Browser

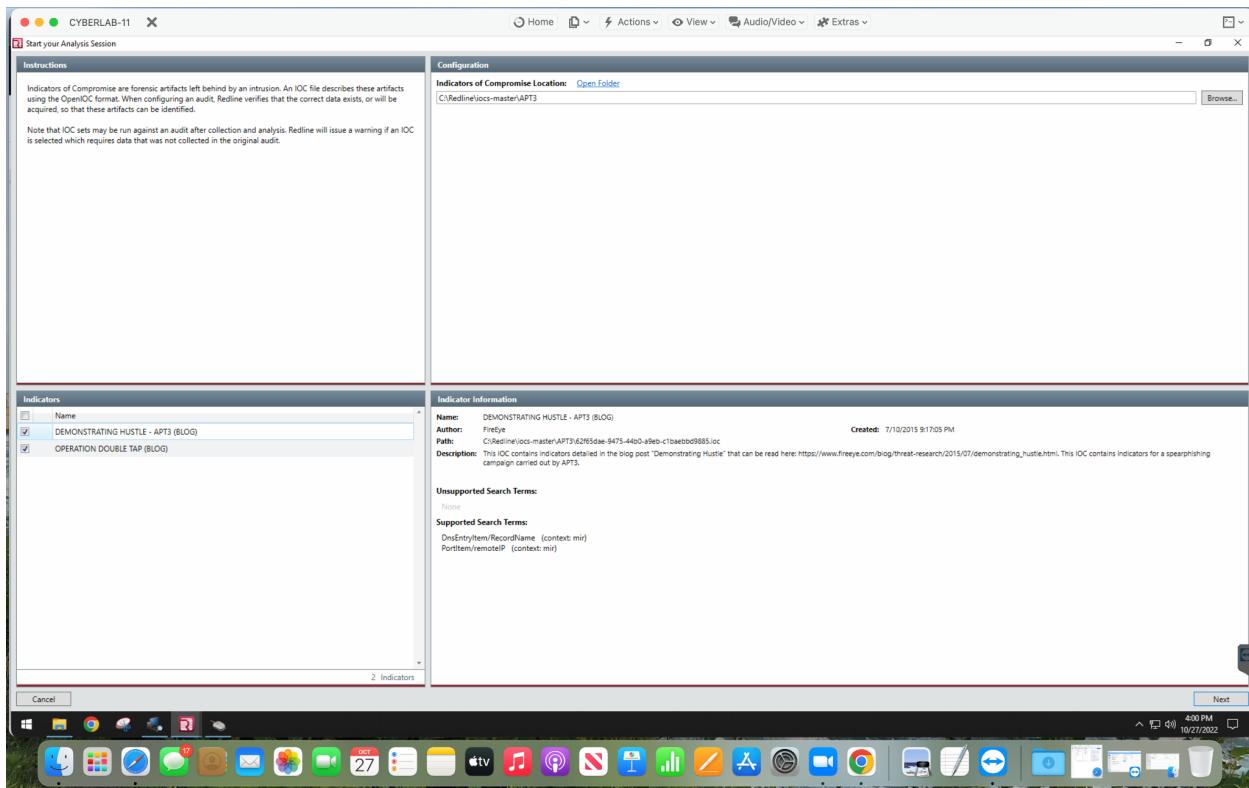
Browser Name:	Firefox
Browser Version:	106.0.1 (64-bit) en-US
Profile:	c98@2fa.default-release
Username:	cybersecurity

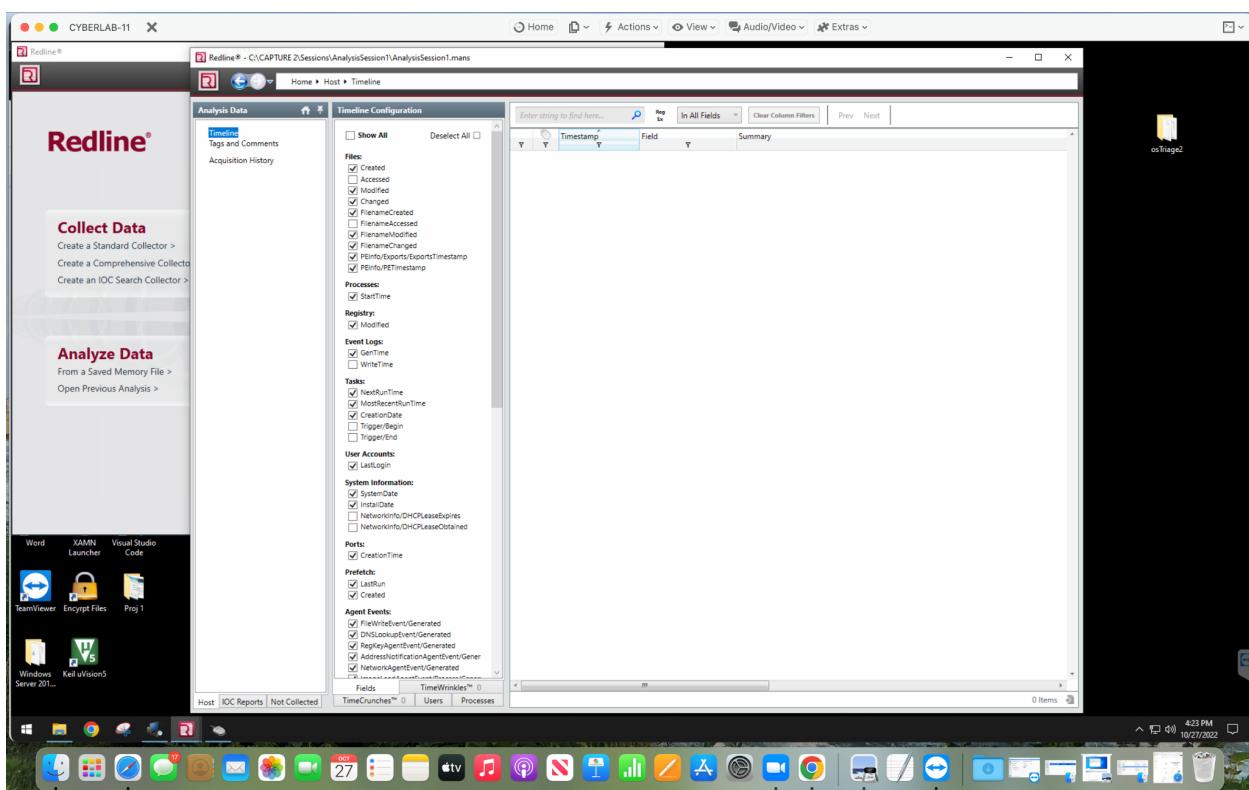
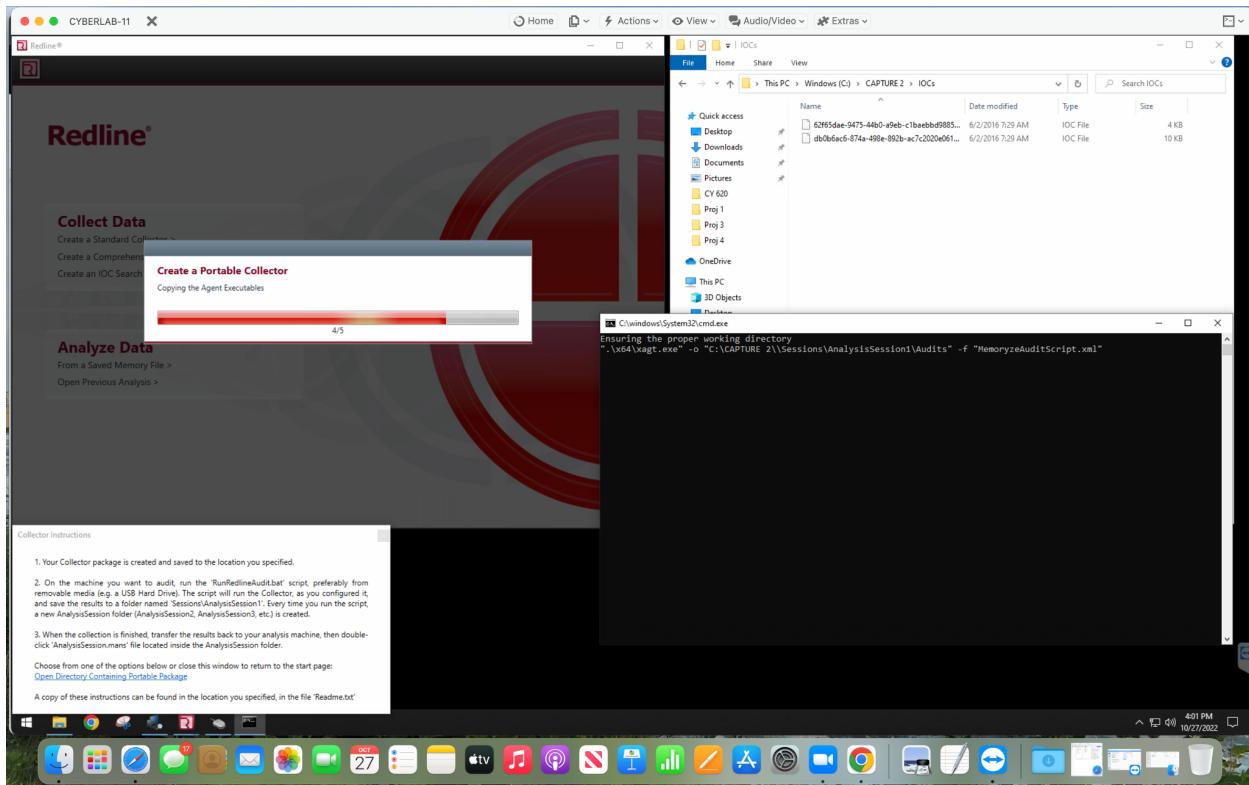
Details Duplicates Tags and Comments

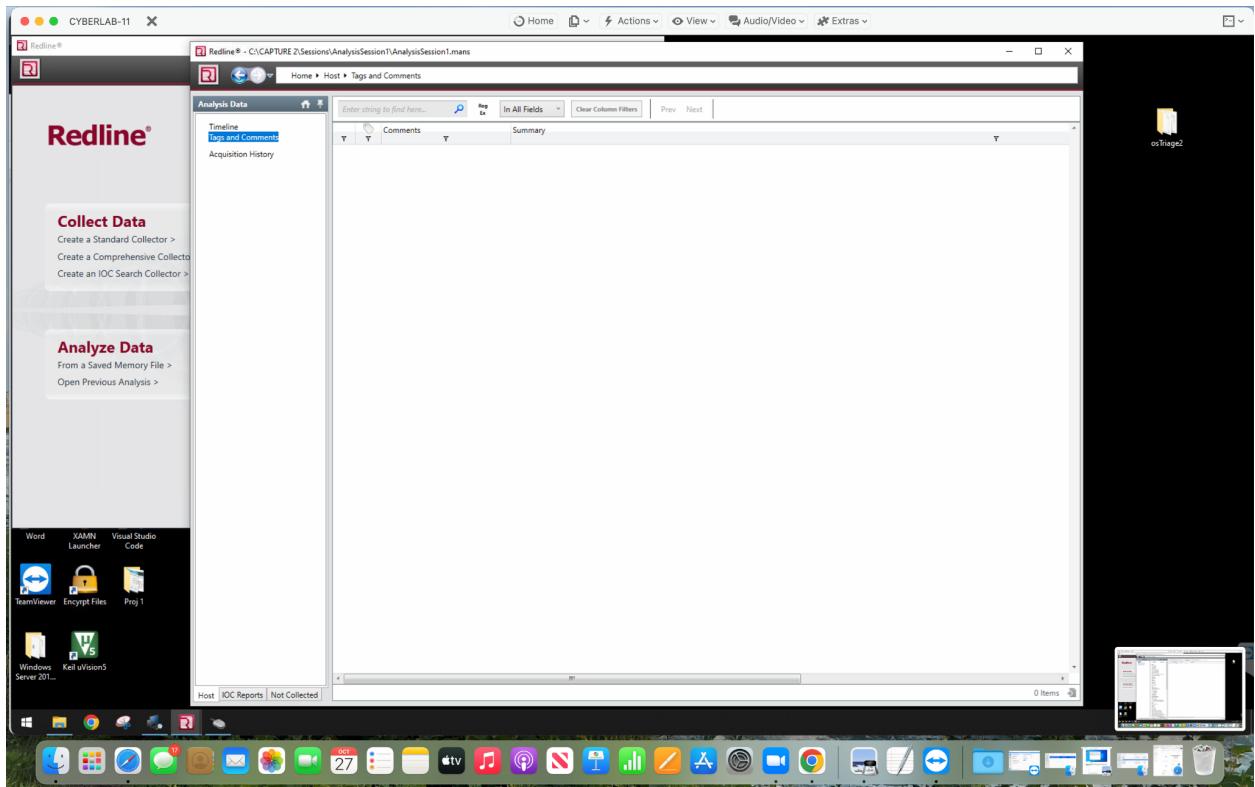
3:54 PM 10/27/2022

IOC (an indicator of compromise):

- IOCs are forensic artifacts of an intrusion discovered by the host. It looks for a certain compromise artifact signature provided by the host. Traditional forensic items like as MD5 hashes, compilation times, file size, path location, registry keys, and many more can be used. The most complicated IOCs employed more advanced forensic techniques.
- When data is imported or when an analysis session is formed, Redline generates an IOC report.
- IOCs are simply detected attacker activities.
- It is usually straightforward to assess information that is less expensive to gather or calculate.
- Create a report after adding the IOC folder. (Please keep in mind that if no data is altered, the report will be blank.)







Conclusion: By doing these three different types of memory collection, we can see that standard collection only collects data quickly, whereas comprehensive collection collects deep analysis and retrieves more in-depth. Both have advantages; if an expert has limited time, he should collect standard collection; if he has unlimited time, he should collect a comprehensive analysis; and IOC indicates whether or not there are any changes after data collection.
