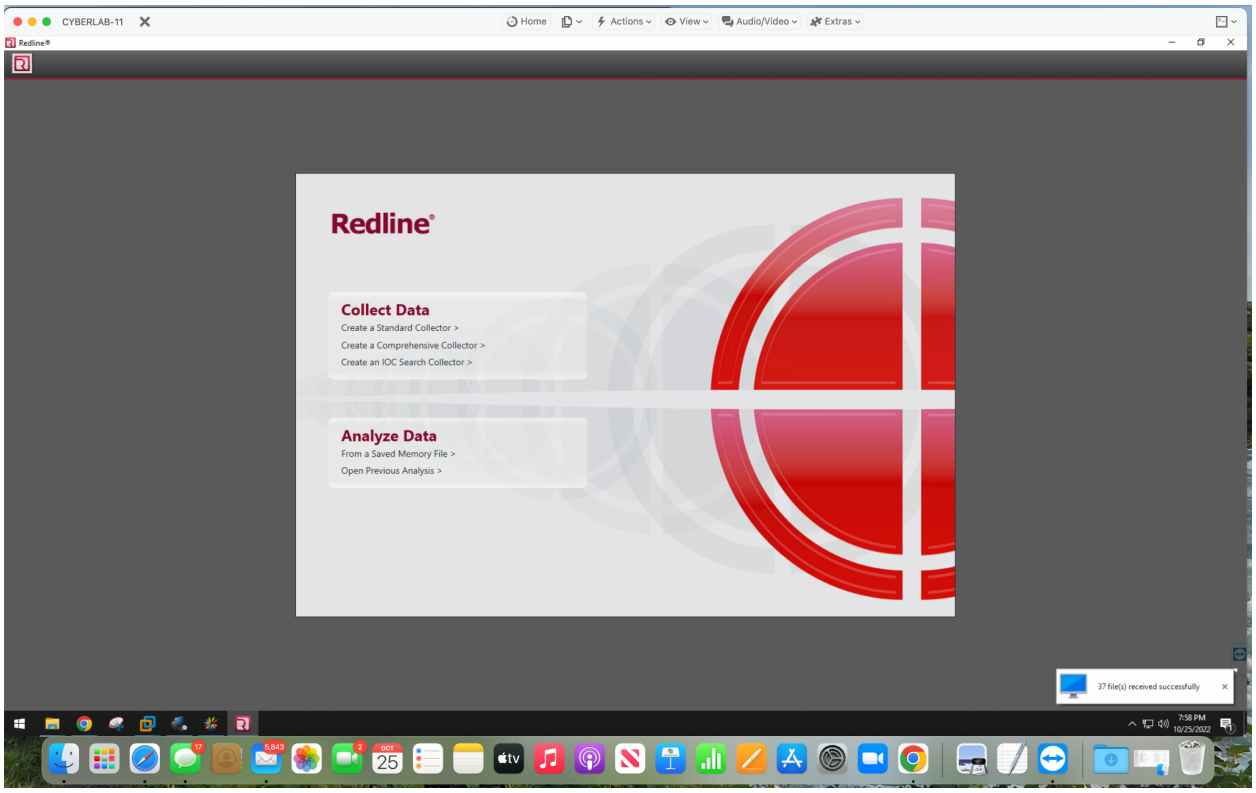
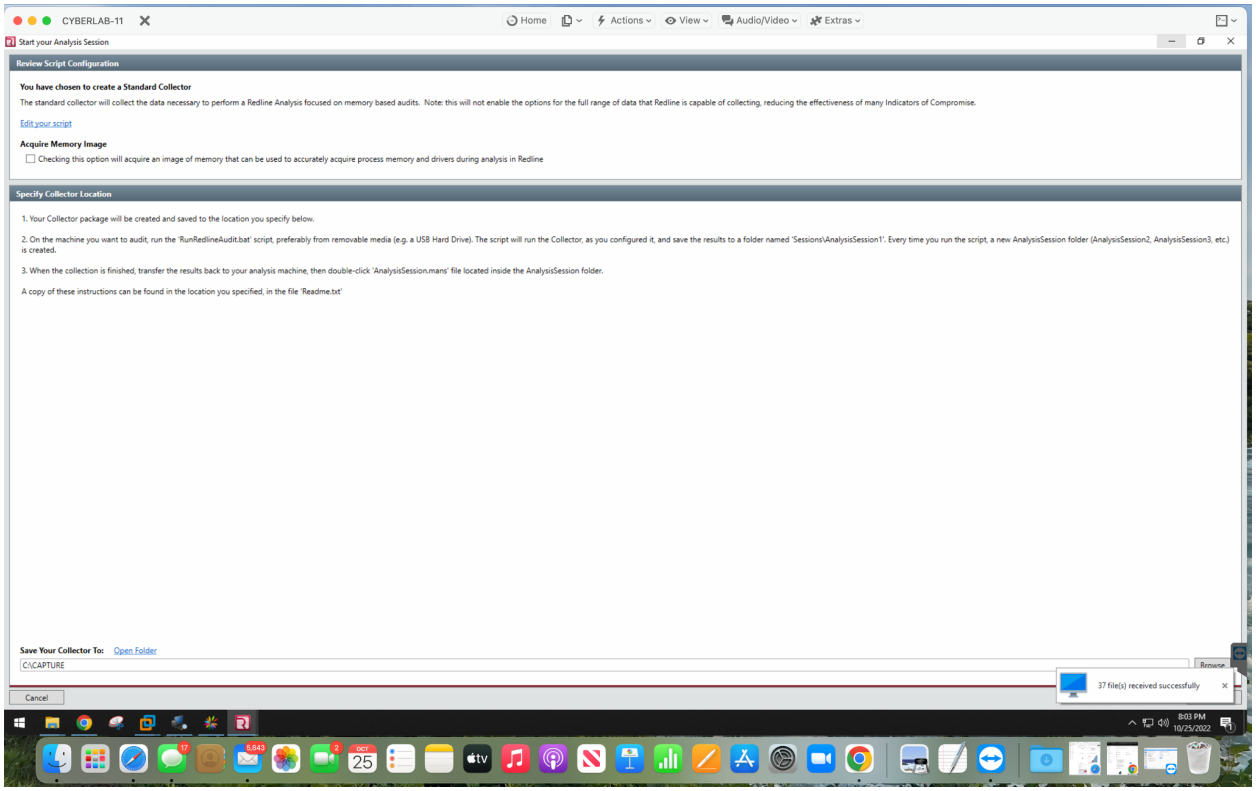
CY-640 - Cyber Crime and Forensics Labs
Nikhil Patel
Spring Trimester 2022
10/31/2022
Memory Forensics

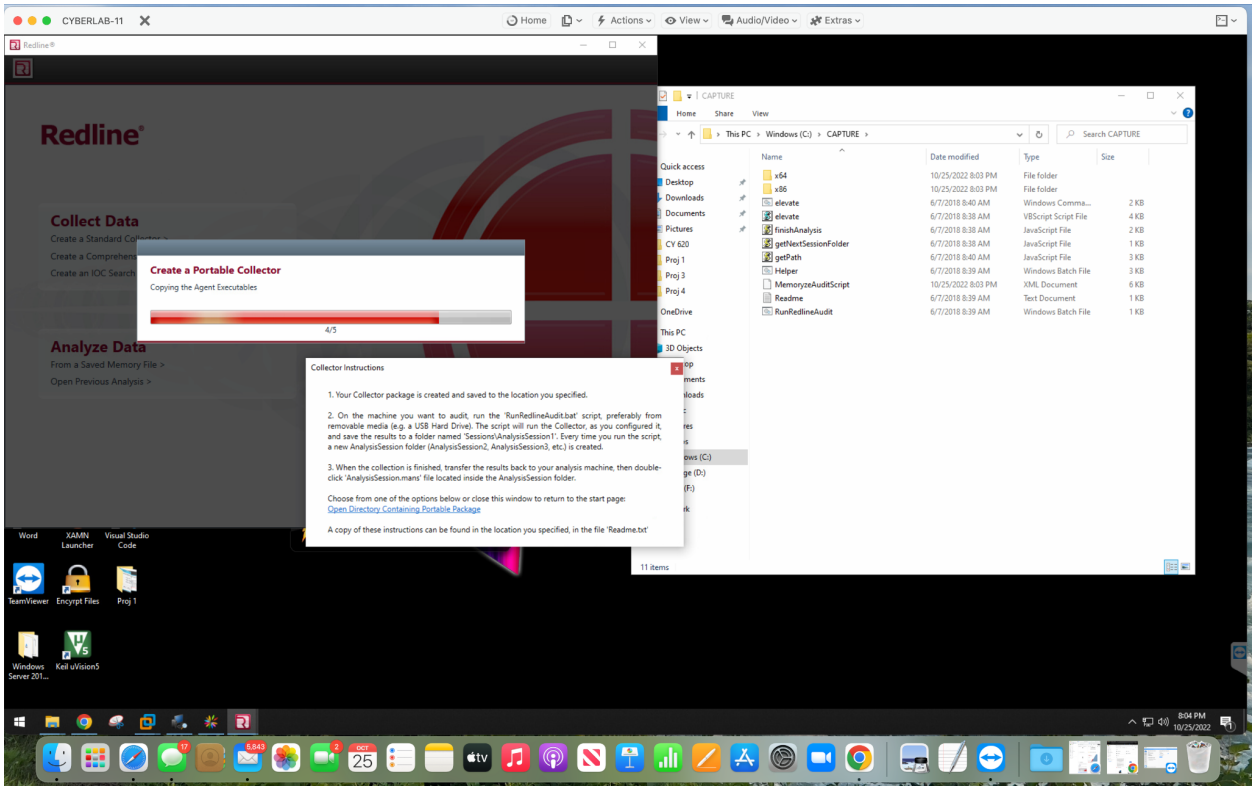
Overview: We will investigate memory in three parts in this project, using a tool called redline (Standard, Comprehensive, and IOC). Because comprehensive gathers data in greater depth, which takes time, standard and IOC recorded memory in less time than comprehensive. We will prepare reports on three (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.

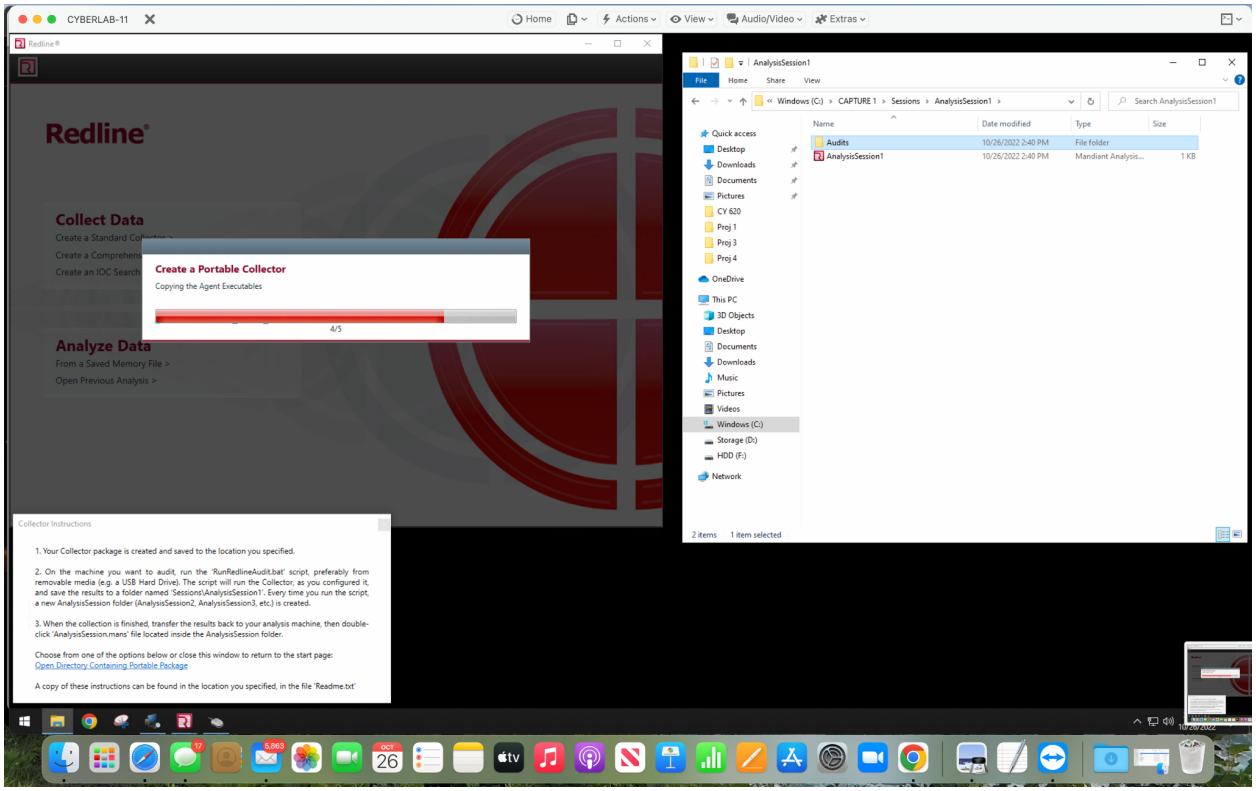


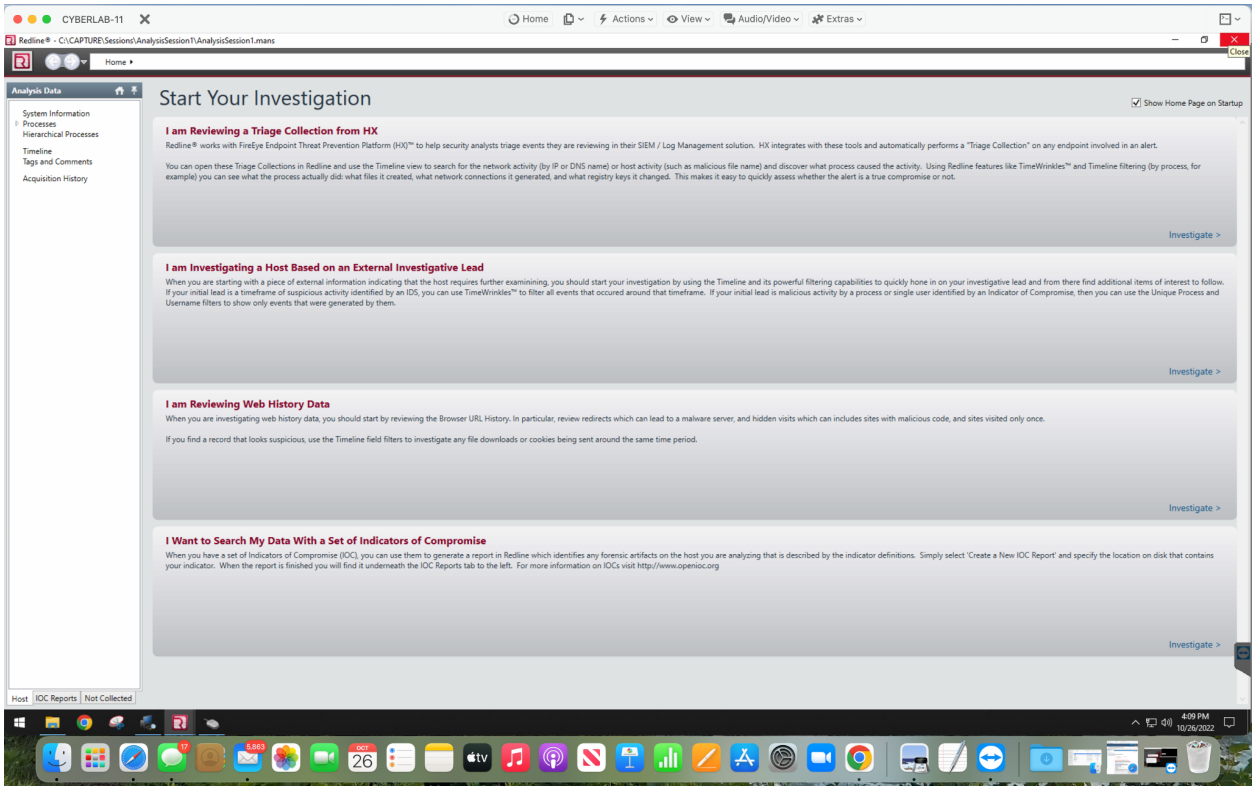
Standard Analysis:

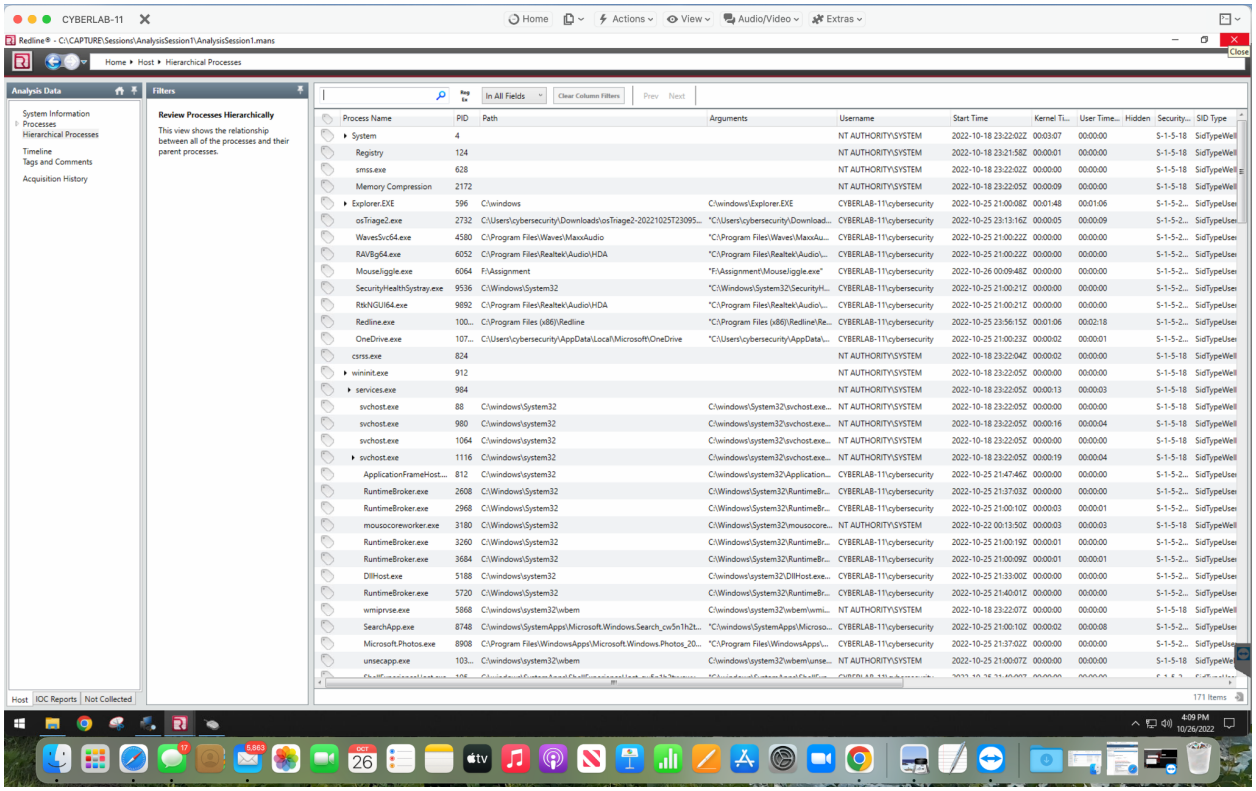
- Create a standard collection of data.
- Now after you click on the standard collection, tick on it to acquire a memory image then provide an empty folder path.
- Then, after opening the file location and run the .bat file and wait until it is complete.
- Once the standard analysis is done it will create 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.

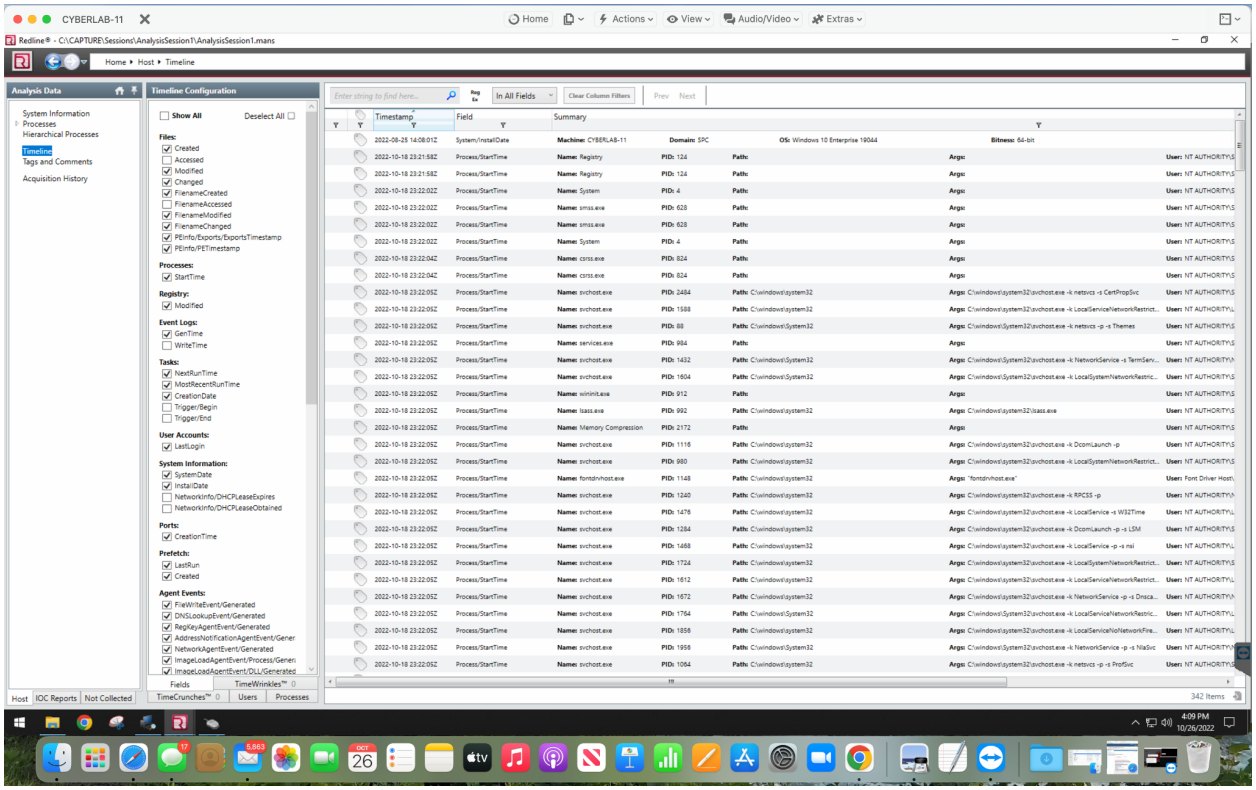



CYBERLAB-11
Redline
Collect Data
Analyze Data
From a Saved Memory File >
Open Previous Analysis >
Create a Portable Collector
Copying the Agent Executables
4/5
Collector Instructions
1. Your Collector package is created and saved to the location you specified.
2. On the machine you want to audit, run the 'RunRedlineAudit.bat' script, preferably from removable media (e.g. a USB Hard Drive). The script will run the Collector, as you configured it, and save the results to a folder named 'Sessions\AnalysisSession1'. Every time you run the script, a new AnalysisSession folder (AnalysisSession2, AnalysisSession3, etc.) is created.
3. When the collection is finished, transfer the results back to your analysis machine, then double-click 'AnalysisSession.mans' file located inside the AnalysisSession folder.
Choose from one of the options below or close this window to return to the start page:
Open Directory Containing Portable Package
A copy of these instructions can be found in the location you specified, in the file 'Readme.txt'
CAPTURE
11 items


CYBERLAB-11
Redline
Collect Data
Analyze Data
From a Saved Memory File >
Open Previous Analysis >
Create a Portable Collector
Copying the Agent Executables
4/5
Collector Instructions
1. Your Collector package is created and saved to the location you specified.
2. On the machine you want to audit, run the 'RunRedlineAudit.bat' script, preferably from removable media (e.g. a USB Hard Drive). The script will run the Collector, as you configured it, and save the results to a folder named 'Sessions\AnalysisSession1'. Every time you run the script, a new AnalysisSession folder (AnalysisSession2, AnalysisSession3, etc.) is created.
3. When the collection is finished, transfer the results back to your analysis machine, then double-click 'AnalysisSession.mans' file located inside the AnalysisSession folder.
Choose from one of the options below or close this window to return to the start page:
Open Directory Containing Portable Package
A copy of these instructions can be found in the location you specified, in the file 'Readme.txt'
AnalysisSession1
Audits
AnalysisSession1
2 items
1 item selected

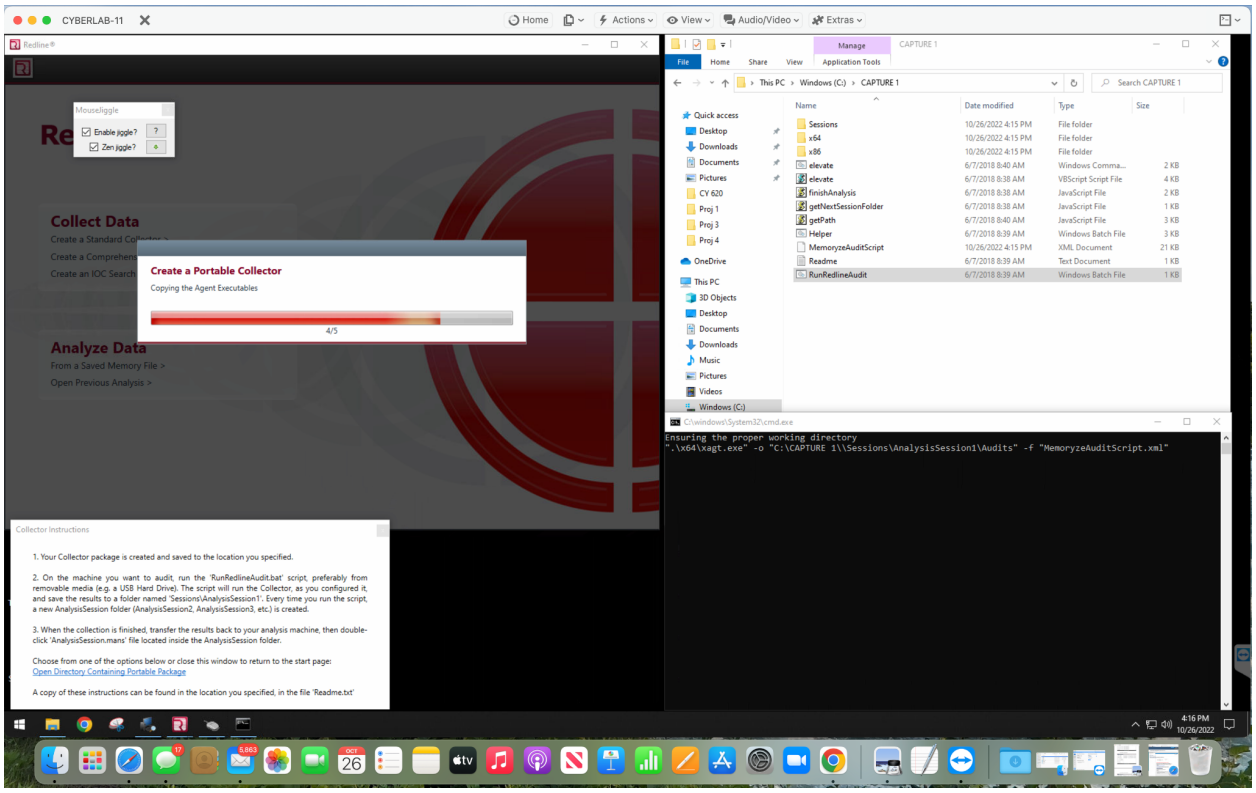

CYBERLAB-11
Home
Actions
View
Audio/Video
Extras
Redline® - C:\CAPTURE\Sessions\AnalysisSession1\AnalysisSession1.mans
Close
Home
Analysis Data
System Information
Processes
Hierarchical Processes
Timeline
Tags and Comments
Acquisition History
Start Your Investigation
Show Home Page on Startup
I am Reviewing a Triage Collection from HX
Redline® works with FireEye Endpoint Threat Prevention Platform (HX)™ to help security analysts triage events they are reviewing in their SIEM / Log Management solution. HX integrates with these tools and automatically performs a "Triage Collection" on any endpoint involved in an alert.
You can open these Triage Collections in Redline and use the Timeline view to search for the network activity (by IP or DNS name) or host activity (such as malicious file name) and discover what process caused the activity. Using Redline features like TimeWrinkles™ and Timeline filtering (by process, for example) you can see what the process actually did: what files it created, what network connections it generated, and what registry keys it changed. This makes it easy to quickly assess whether the alert is a true compromise or not.
Investigate >
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 occured 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.
Investigate >
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 includes sites with malicious code, and sites visited only once.
If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.
Investigate >
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.openioc.org
Investigate >
Host
IOC Reports
Not Collected
4:09 PM
10/26/2022

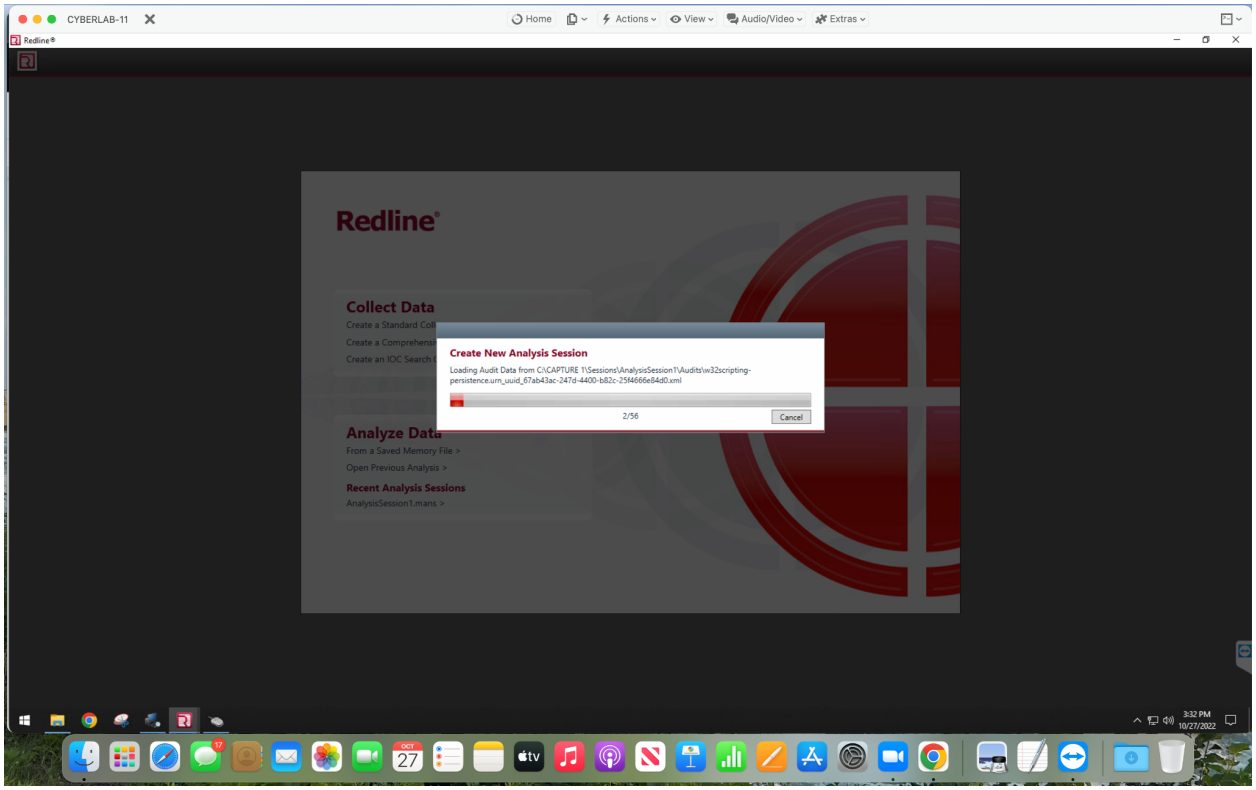

CYBERLAB-11
Home
Actions
View
Audio/Video
Extras
Redline® - C:\CAPTURE\Sessions\AnalysisSession1\AnalysisSession1.mans
Close
Home ▸ Host ▸ Hierarchical Processes
Analysis Data
System Information
Processes
Hierarchical Processes
Timeline
Tags and Comments
Acquisition History
Filters
Review Processes Hierarchically
This view shows the relationship between all of the processes and their parent processes.
In All Fields
Clear Column Filters
Prev
Next
Process Name | PID | Path | Arguments | Username | Start Time | Kernel Ti... | User Time... | Hidden | Security... | SID Type
System | 4 | | | NT AUTHORITY\SYSTEM | 2022-10-18 23:22:02Z | 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 23:22:02Z | 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 | 2022-10-25 21:00:08Z | 00:01:48 | 00:01:06 | | S-1-5-2... | SidTypeUser
osTriage2.exe | 2732 | C:\Users\cybersecurity\Downloads\osTriage2-20221025T23095... | "C:\Users\cybersecurity\Download... | CYBERLAB-11\cybersecurity | 2022-10-25 23:13:16Z | 00:00:05 | 00:00:09 | | S-1-5-2... | SidTypeUser
WavesSvc64.exe | 4580 | C:\Program Files\Waves\MaxxAudio | "C:\Program Files\Waves\MaxxAu... | CYBERLAB-11\cybersecurity | 2022-10-25 21:00:22Z | 00:00:00 | 00:00:00 | | S-1-5-2... | SidTypeUser
RAVBg64.exe | 6052 | C:\Program Files\Realtek\Audio\HDA | "C:\Program Files\Realtek\Audio\... | CYBERLAB-11\cybersecurity | 2022-10-25 21:00:22Z | 00:00:00 | 00:00:00 | | S-1-5-2... | SidTypeUser
MouseJiggle.exe | 6064 | F:\Assignment | "F:\Assignment\MouseJiggle.exe" | CYBERLAB-11\cybersecurity | 2022-10-26 00:09:48Z | 00:00:00 | 00:00:00 | | S-1-5-2... | SidTypeUser
SecurityHealthSystray.exe | 9536 | C:\Windows\System32 | "C:\Windows\System32\SecurityH... | CYBERLAB-11\cybersecurity | 2022-10-25 21:00:21Z | 00:00:00 | 00:00:00 | | S-1-5-2... | SidTypeUser
RtkNGUI64.exe | 9892 | C:\Program Files\Realtek\Audio\HDA | "C:\Program Files\Realtek\Audio\... | CYBERLAB-11\cybersecurity | 2022-10-25 21:00:21Z | 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 | 2022-10-25 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\... | CYBERLAB-11\cybersecurity | 2022-10-25 21:00:23Z | 00:00:02 | 00:00:01 | | S-1-5-2... | SidTypeUser
csrss.exe | 824 | | | NT AUTHORITY\SYSTEM | 2022-10-18 23:22:04Z | 00:00:02 | 00:00:00 | | S-1-5-18 | SidTypeWell
wininit.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.exe... | 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.exe... | 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.exe... | 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.exe... | 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 | 2022-10-25 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 | 2022-10-25 21:37:03Z | 00:00:00 | 00:00:00 | | S-1-5-2... | SidTypeUser
RuntimeBroker.exe | 2968 | C:\Windows\System32 | C:\Windows\System32\RuntimeBr... | CYBERLAB-11\cybersecurity | 2022-10-25 21:00:10Z | 00:00:03 | 00:00:01 | | S-1-5-2... | SidTypeUser
mousocoreworker.exe | 3180 | C:\Windows\System32 | C:\Windows\System32\mousocore... | NT AUTHORITY\SYSTEM | 2022-10-22 00:13:50Z | 00:00:03 | 00:00:03 | | S-1-5-18 | SidTypeWell
RuntimeBroker.exe | 3260 | C:\Windows\System32 | C:\Windows\System32\RuntimeBr... | CYBERLAB-11\cybersecurity | 2022-10-25 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 | 2022-10-25 21:00:09Z | 00:00:01 | 00:00:01 | | S-1-5-2... | SidTypeUser
DllHost.exe | 5188 | C:\windows\system32 | C:\windows\system32\DllHost.exe... | CYBERLAB-11\cybersecurity | 2022-10-25 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 | 2022-10-25 21:40:01Z | 00:00:00 | 00:00:00 | | S-1-5-2... | SidTypeUser
wmiprvse.exe | 5868 | C:\windows\system32\wbem | C:\windows\system32\wbem\wmi... | 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\SystemApps\Microsoft.Windows.Search_cw5n1h2t... | "C:\windows\SystemApps\Microso... | CYBERLAB-11\cybersecurity | 2022-10-25 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\WindowsApps\... | CYBERLAB-11\cybersecurity | 2022-10-25 21:37:02Z | 00:00:00 | 00:00:00 | | S-1-5-2... | SidTypeUser
unsecapp.exe | 103... | C:\windows\system32\wbem | C:\windows\system32\wbem\unse... | NT AUTHORITY\SYSTEM | 2022-10-25 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

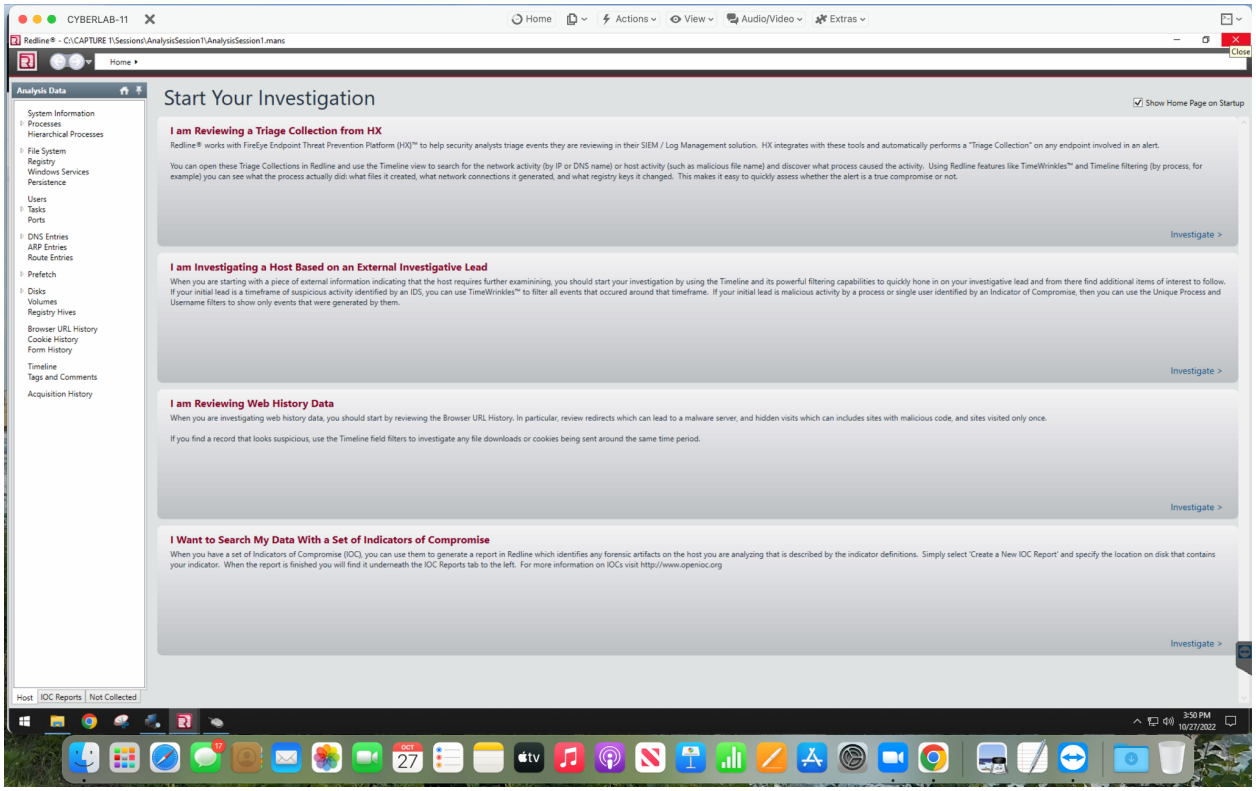

CYBERLAB-11
Home
Actions
View
Audio/Video
Extras
Redline® - C:\CAPTURE\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Timeline
Analysis Data
System Information
Processes
Hierarchical Processes
Timeline
Tags and Comments
Acquisition History
Timeline Configuration
Show All
Deselect All
Files:
Created
Accessed
Modified
Changed
FilenameCreated
FilenameAccessed
FilenameModified
FilenameChanged
PEInfo/Exports/ExportsTimestamp
PEInfo/PETimestamp
Processes:
StartTime
Registry:
Modified
Event Logs:
GenTime
WriteTime
Tasks:
NextRunTime
MostRecentRunTime
CreationDate
Trigger/Begin
Trigger/End
User Accounts:
LastLogin
System Information:
SystemDate
InstallDate
NetworkInfo/DHCPLeaseExpires
NetworkInfo/DHCPLeaseObtained
Ports:
CreationTime
Prefetch:
LastRun
Created
Agent Events:
FileWriteEvent/Generated
DNSLookupEvent/Generated
RegKeyAgentEvent/Generated
AddressNotificationAgentEvent/Gener
NetworkAgentEvent/Generated
ImageLoadAgentEvent/Process/Gener
ImageLoadAgentEvent/DLL/Generated
Fields
TimeWrinkles™ 0
TimeCrunches™ 0
Users
Processes
Host
IOC Reports
Not Collected
In All Fields
Clear Column Filters
Prev
Next
Timestamp
Field
Summary
342 Items
4:09 PM
10/26/2022

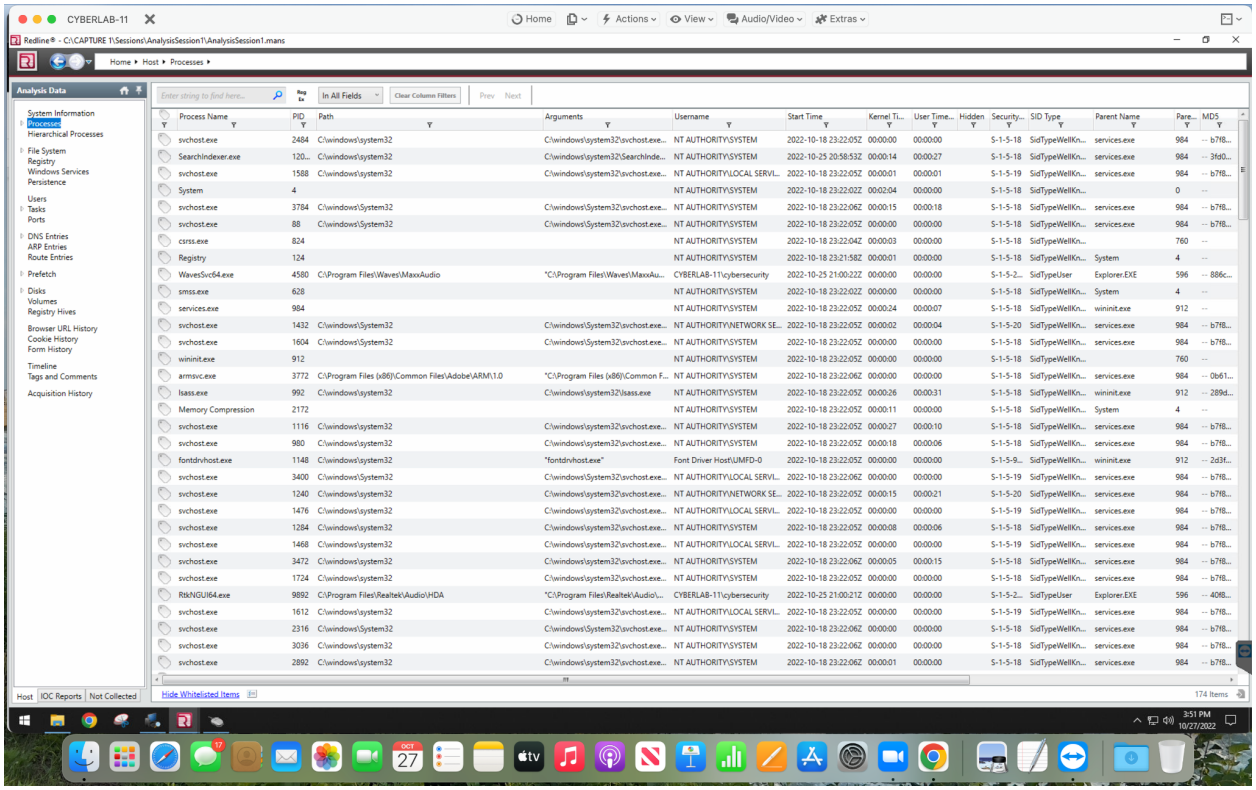
Comprehensive Analysis:

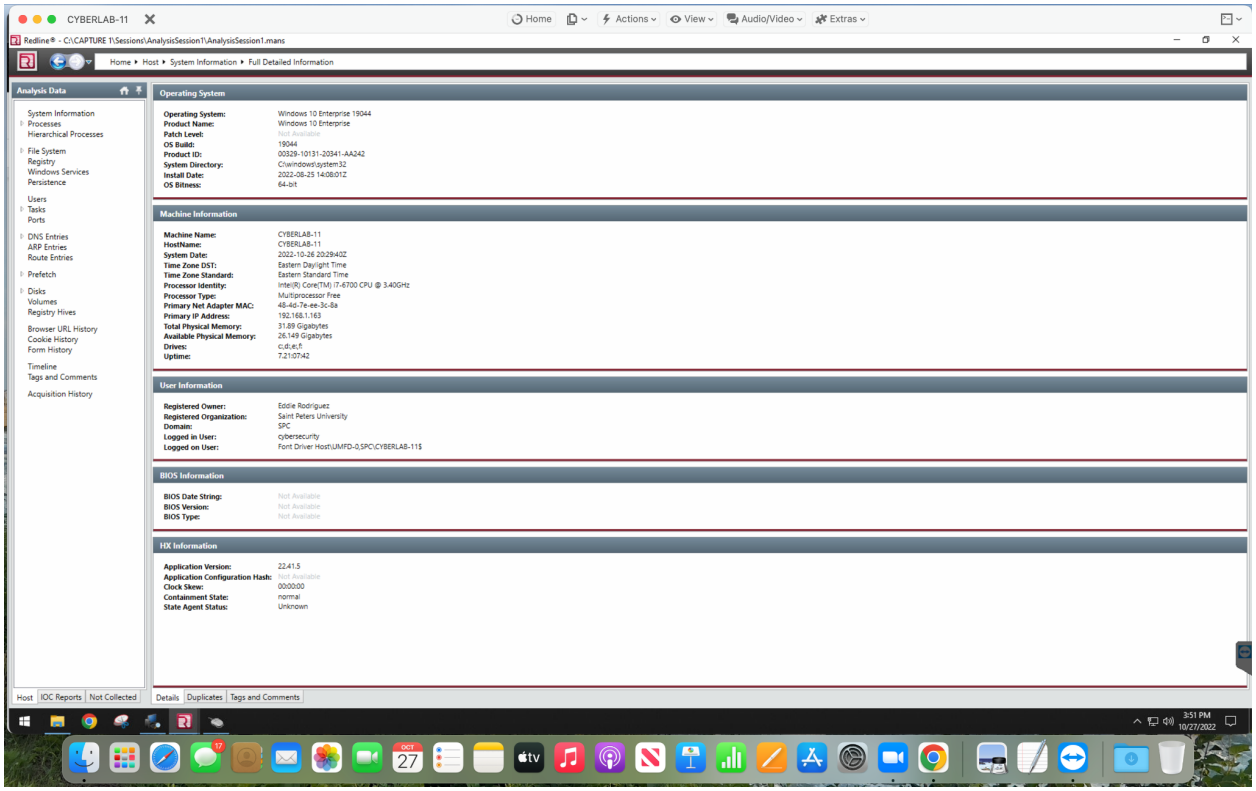
- It collects the most data that redline analyzes; it is typically utilized for a comprehensive analysis or when an expert only has one opportunity to get data from the system.
- Repeat the regular collection process with the exception of selecting the thorough collection option on the redline.
- It 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.

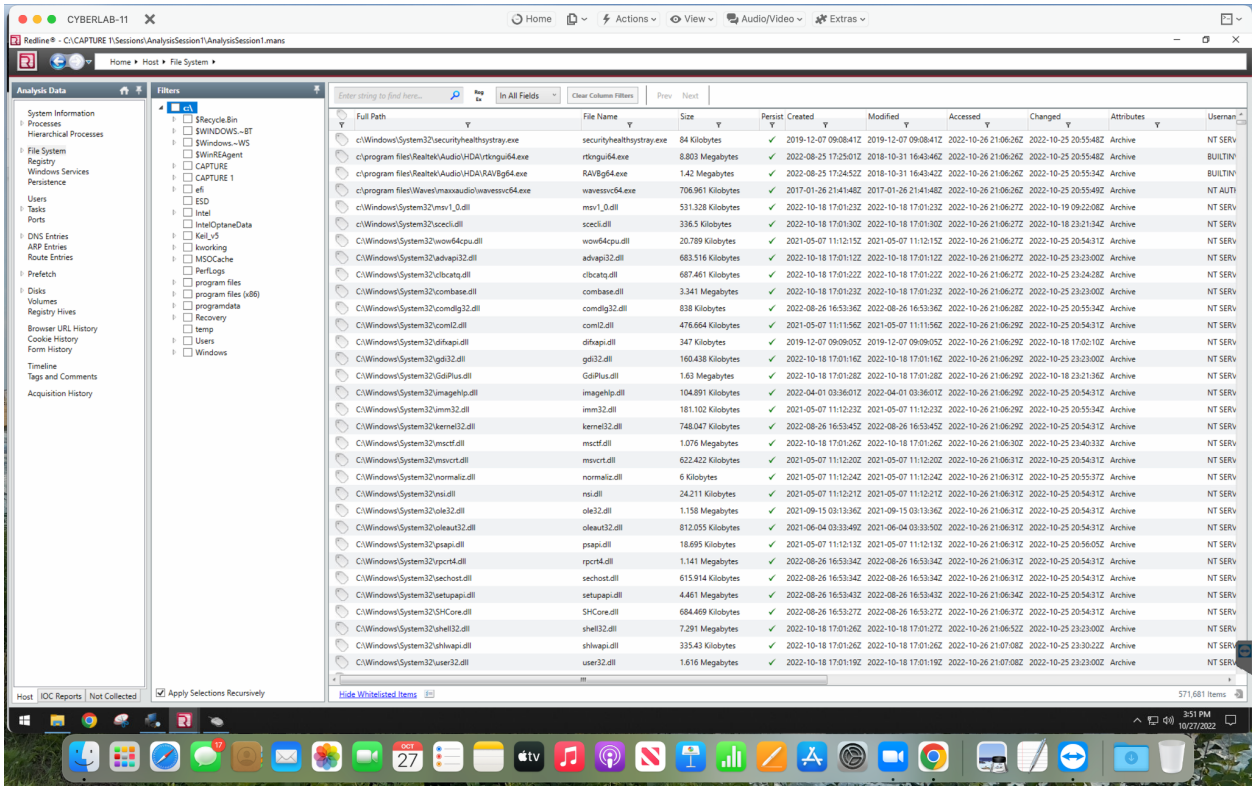


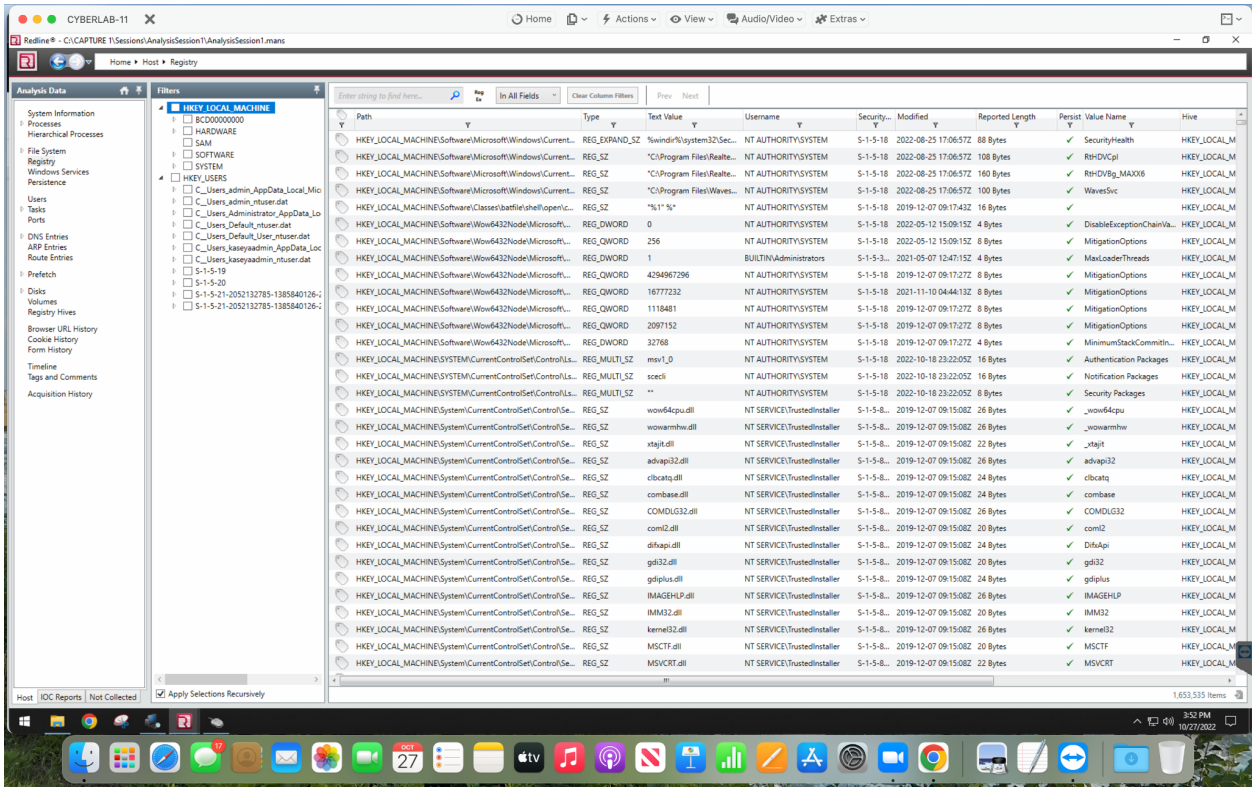

CYBERLAB-11
Home
Actions
View
Audio/Video
Extras
Redline®
Redline
Collect Data
Create a Standard Coll
Create a Comprehens
Create an IOC Search
Create New Analysis Session
Loading Audit Data from C:\CAPTURE 1\Sessions\AnalysisSession1\Audits\w32scripting-persistence.urn_uuid_67ab43ac-247d-4400-b82c-25f4666e84d0.xml
2/56
Cancel
Analyze Data
From a Saved Memory File >
Open Previous Analysis >
Recent Analysis Sessions
AnalysisSession1.mans >
3:32 PM
10/27/2022

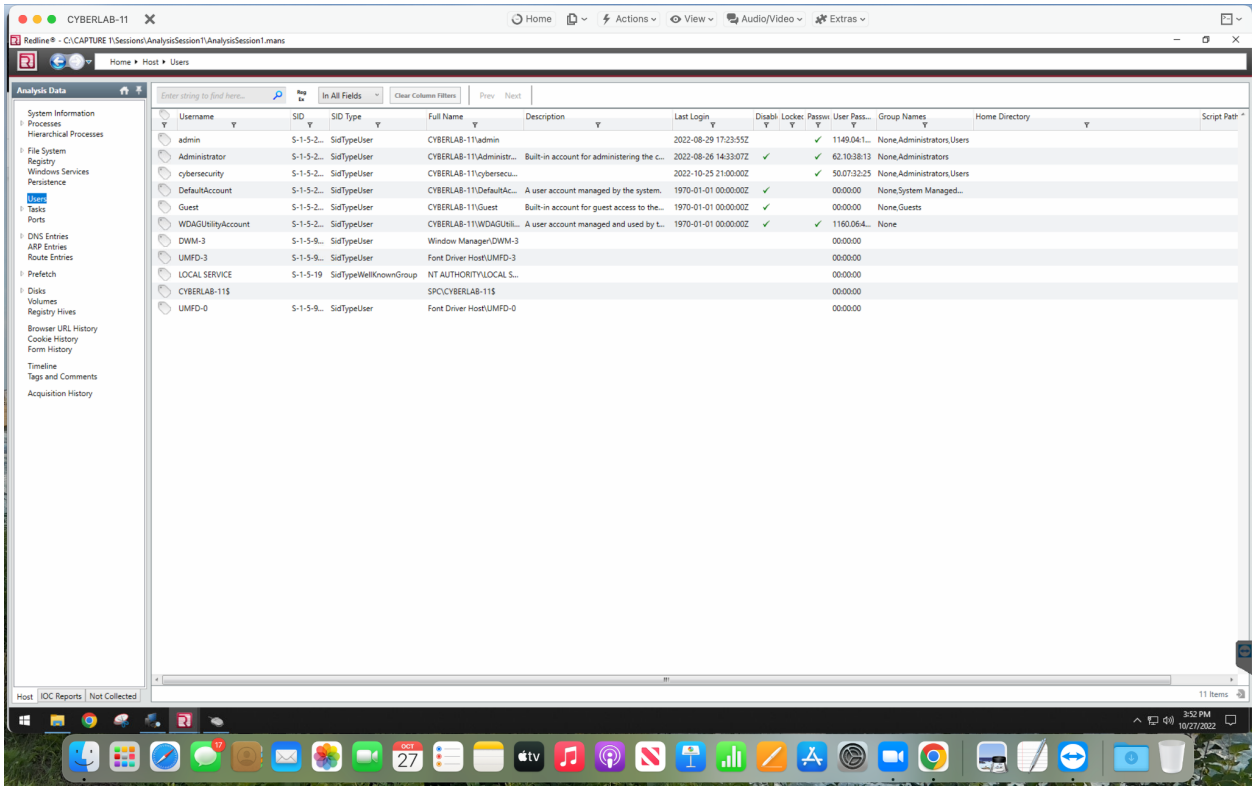

CYBERLAB-11
Home
Actions
View
Audio/Video
Extras
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Close
Home
Analysis Data
System Information
Processes
Hierarchical Processes
File System
Registry
Windows Services
Persistence
Users
Tasks
Ports
DNS Entries
ARP Entries
Route Entries
Prefetch
Disks
Volumes
Registry Hives
Browser URL History
Cookie History
Form History
Timeline
Tags and Comments
Acquisition History
Host
IOC Reports
Not Collected
Start Your Investigation
Show Home Page on Startup
I am Reviewing a Triage Collection from HX
Redline® works with FireEye Endpoint Threat Prevention Platform (HX)™ to help security analysts triage events they are reviewing in their SIEM / Log Management solution. HX integrates with these tools and automatically performs a "Triage Collection" on any endpoint involved in an alert.
You can open these Triage Collections in Redline and use the Timeline view to search for the network activity (by IP or DNS name) or host activity (such as malicious file name) and discover what process caused the activity. Using Redline features like TimeWrinkles™ and Timeline filtering (by process, for example) you can see what the process actually did: what files it created, what network connections it generated, and what registry keys it changed. This makes it easy to quickly assess whether the alert is a true compromise or not.
Investigate >
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 examinining, 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 occured 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.
Investigate >
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 includes sites with malicious code, and sites visited only once.
If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.
Investigate >
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.openioc.org
Investigate >
3:50 PM
10/27/2022

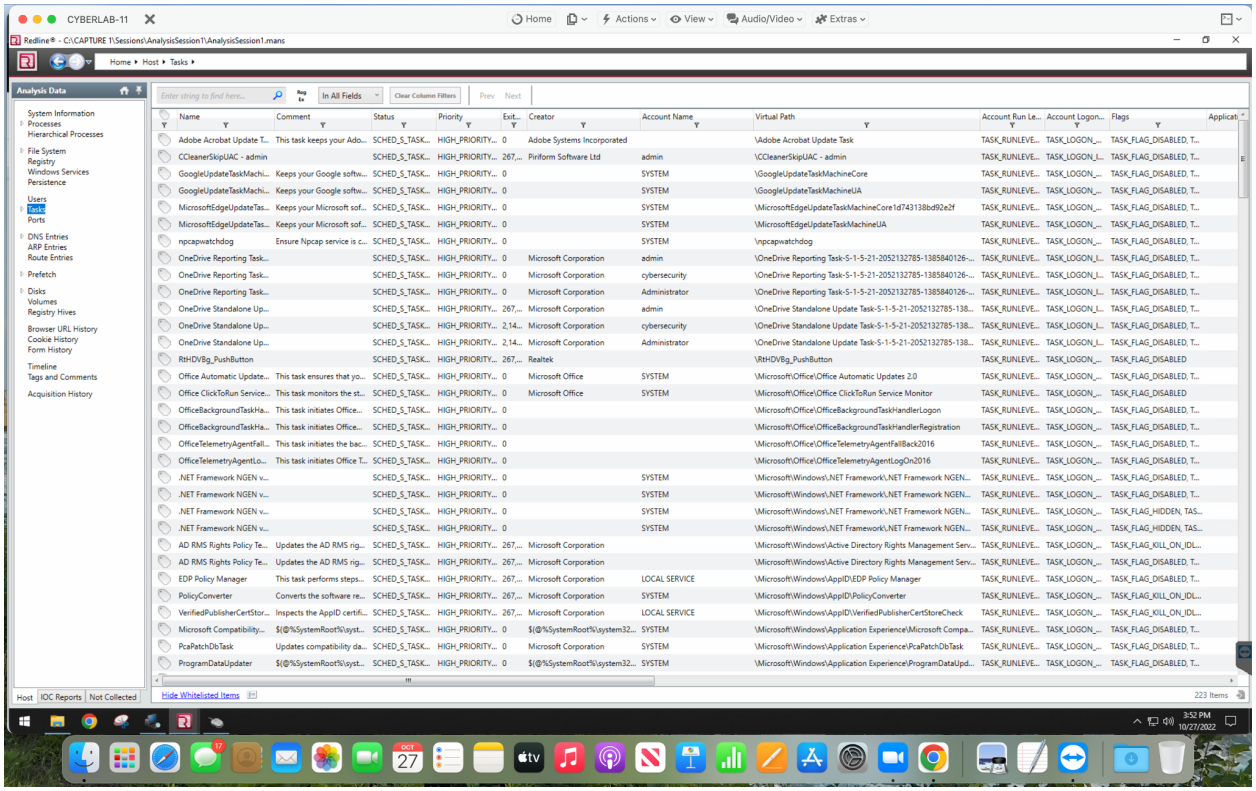

CYBERLAB-11
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Processes ▸
Analysis Data
System Information
Processes
Hierarchical Processes
File System
Registry
Windows Services
Persistence
Users
Tasks
Ports
DNS Entries
ARP Entries
Route Entries
Prefetch
Disks
Volumes
Registry Hives
Browser URL History
Cookie History
Form History
Timeline
Tags and Comments
Acquisition History
Host
IOC Reports
Not Collected
Hide Whitelisted Items
174 Items

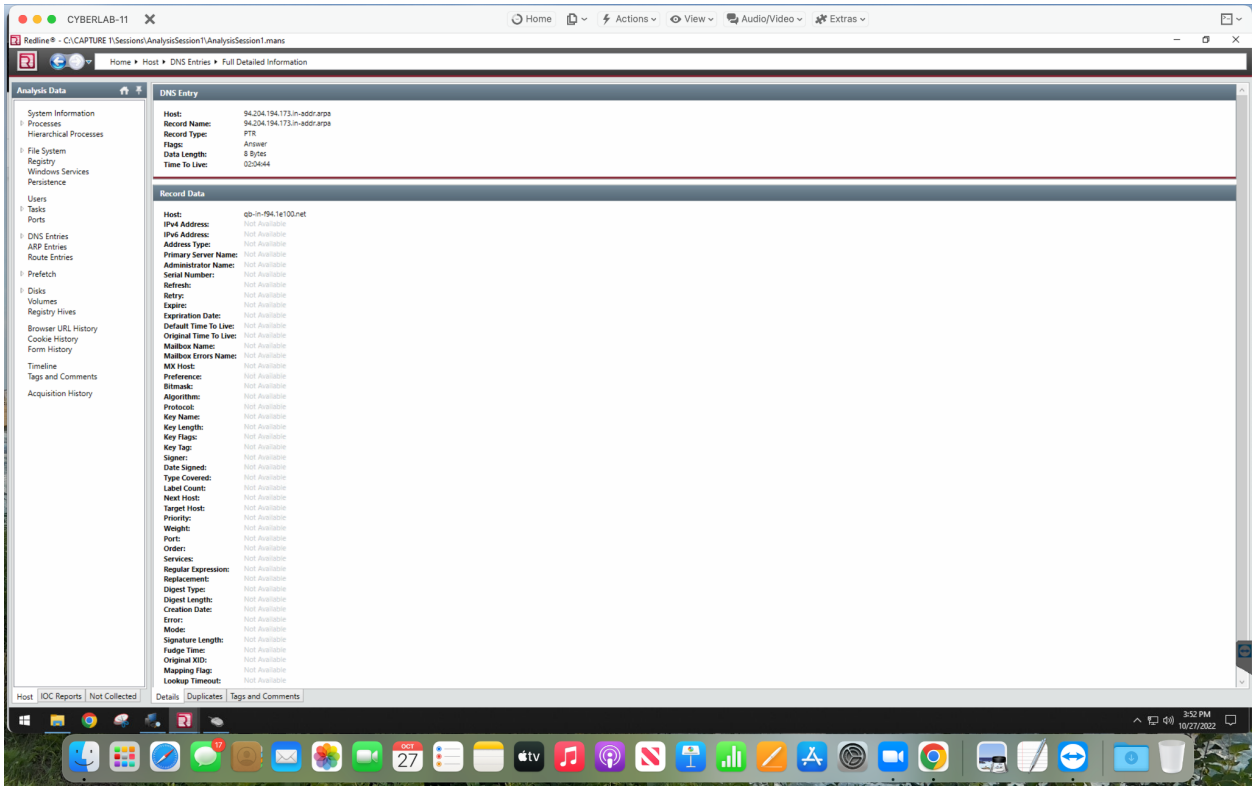

CYBERLAB-11
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ System Information ▸ Full Detailed Information
Analysis Data
Operating System
Operating System: Windows 10 Enterprise 19044
Product Name: Windows 10 Enterprise
Patch Level: Not Available
OS Build: 19044
Product ID: 00329-10131-20341-AA242
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 20:29:40Z
Time Zone DST: Eastern Daylight Time
Time Zone Standard: Eastern Standard Time
Processor Identity: Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz
Processor Type: Multiprocessor Free
Primary Net Adapter MAC: 48-4d-7e-ee-3c-8a
Primary IP Address: 192.168.1.163
Total Physical Memory: 31.89 Gigabytes
Available Physical Memory: 26.149 Gigabytes
Drives: c;d;e;f;
Uptime: 7.21:07:42
User Information
Registered Owner: Eddie Rodriguez
Registered Organization: Saint Peters University
Domain: SPC
Logged in User: cybersecurity
Logged on User: Font Driver Host\UMFD-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: Not Available
Clock Skew: 00:00:00
Containment State: normal
State Agent Status: Unknown
Details
Duplicates
Tags and Comments

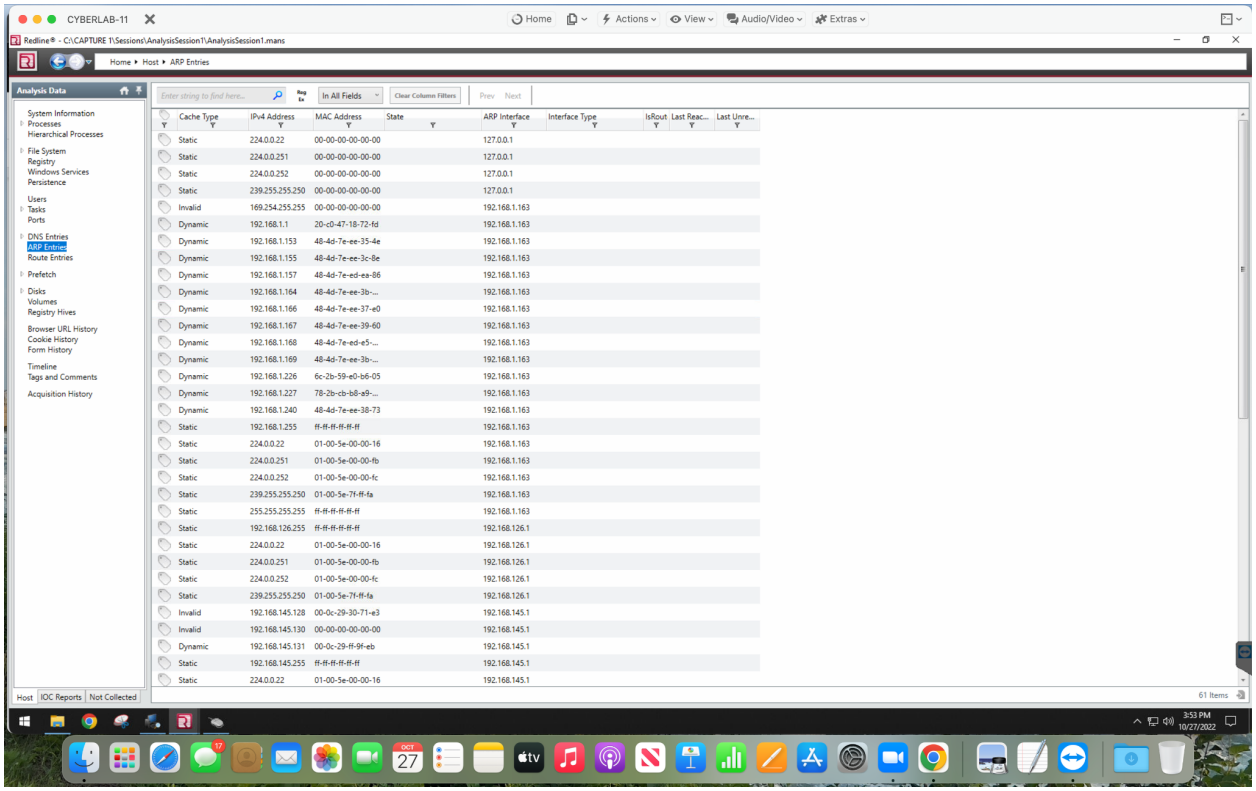

CYBERLAB-11
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ File System ▸
Analysis Data
Filters
Full Path
File Name
Size
Persist
Created
Modified
Accessed
Changed
Attributes
Username
Hide Whitelisted Items
571,681 Items

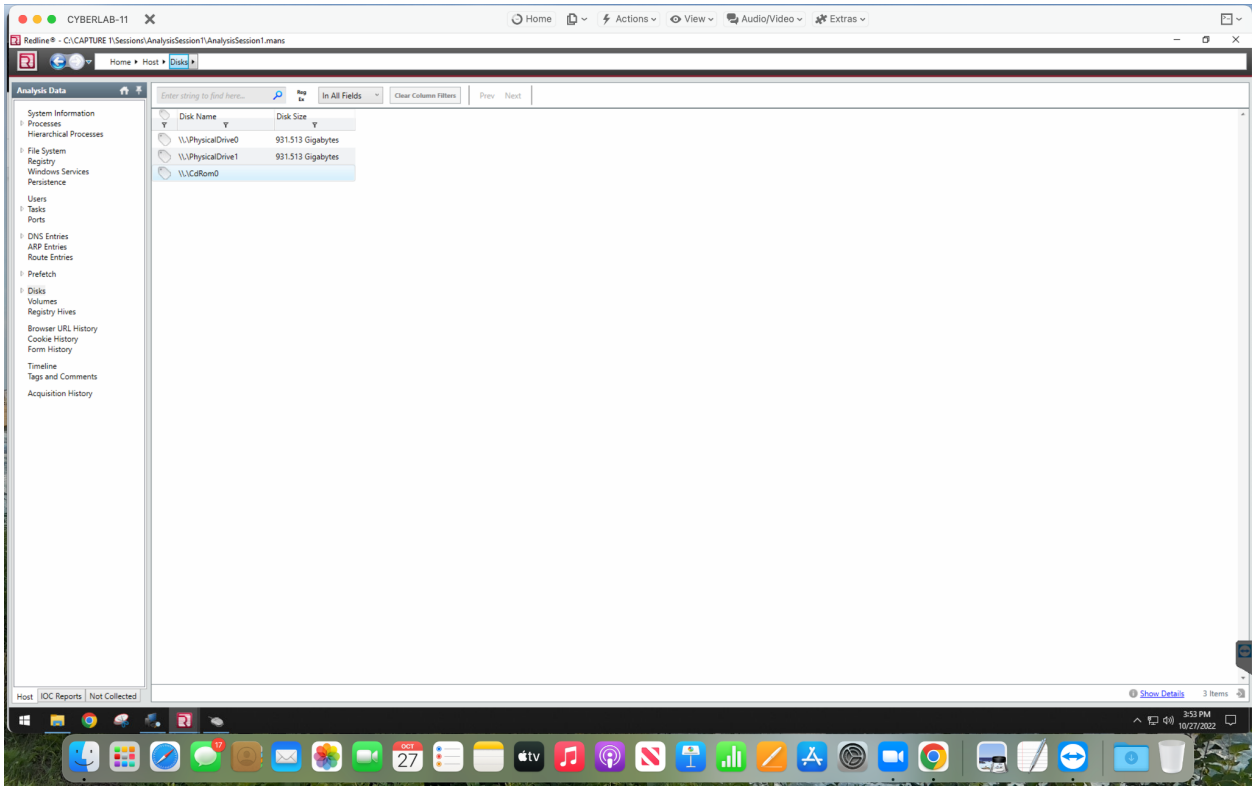

CYBERLAB-11
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Registry
Analysis Data
Filters
Path
Type
Text Value
Username
Modified
Reported Length
Persist
Value Name
Hive
1,653,535 Items

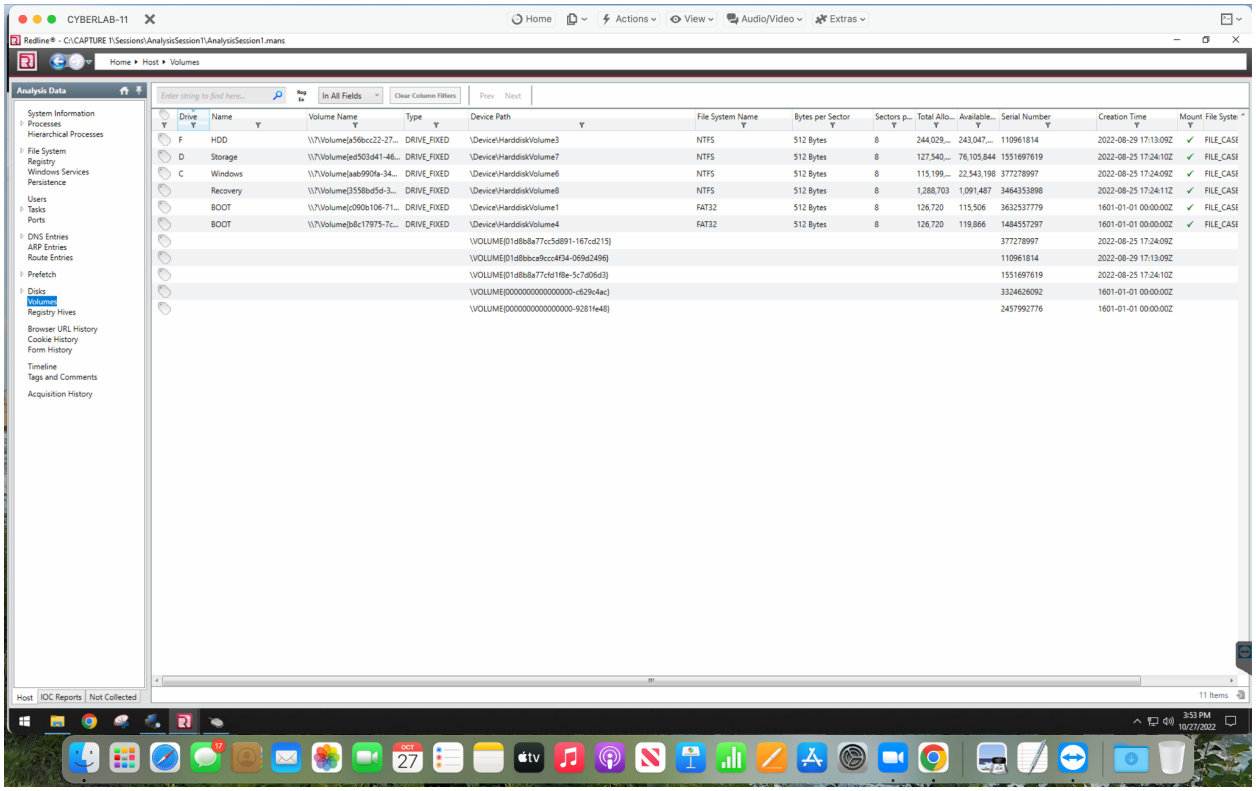

CYBERLAB-11
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Users
Analysis Data
System Information
Processes
Hierarchical Processes
File System
Registry
Windows Services
Persistence
Users
Tasks
Ports
DNS Entries
ARP Entries
Route Entries
Prefetch
Disks
Volumes
Registry Hives
Browser URL History
Cookie History
Form History
Timeline
Tags and Comments
Acquisition History
Host
IOC Reports
Not Collected
Username
SID
SID Type
Full Name
Description
Last Login
Group Names
Home Directory
admin
Administrator
cybersecurity
DefaultAccount
Guest
WDAGUtilityAccount
DWM-3
UMFD-3
LOCAL SERVICE
CYBERLAB-11$
UMFD-0
11 Items

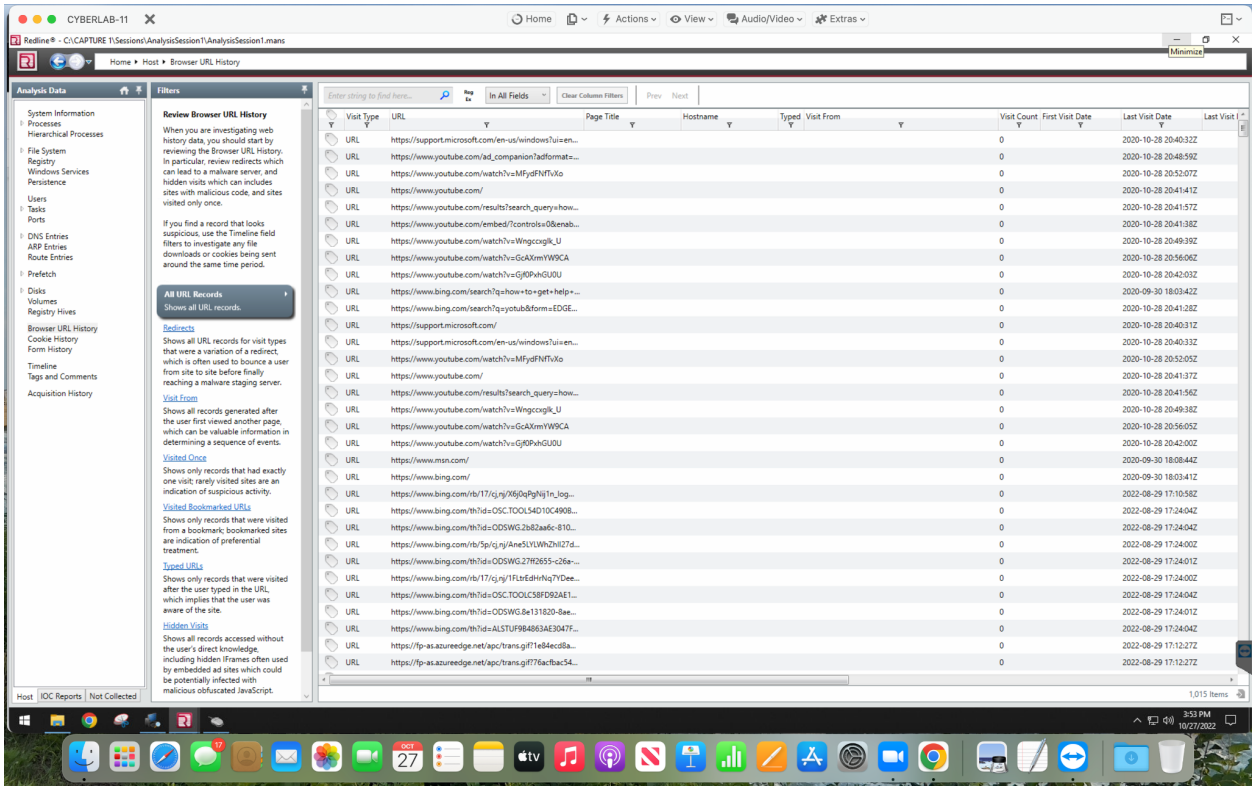

CYBERLAB-11
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Tasks ▸
Analysis Data
Tasks
Name
Comment
Status
Priority
Creator
Account Name
Virtual Path
Adobe Acrobat Update T...
CCleanerSkipUAC - admin
GoogleUpdateTaskMachi...
MicrosoftEdgeUpdateTas...
npcapwatchdog
OneDrive Reporting Task...
OneDrive Standalone Up...
RtHDVBg_PushButton
Office Automatic Update...
Office ClickToRun Service...
OfficeBackgroundTaskHa...
OfficeTelemetryAgentFall...
OfficeTelemetryAgentLo...
.NET Framework NGEN v...
AD RMS Rights Policy Te...
EDP Policy Manager
PolicyConverter
VerifiedPublisherCertStor...
Microsoft Compatibility...
PcaPatchDbTask
ProgramDataUpdater
Hide Whitelisted Items
223 Items

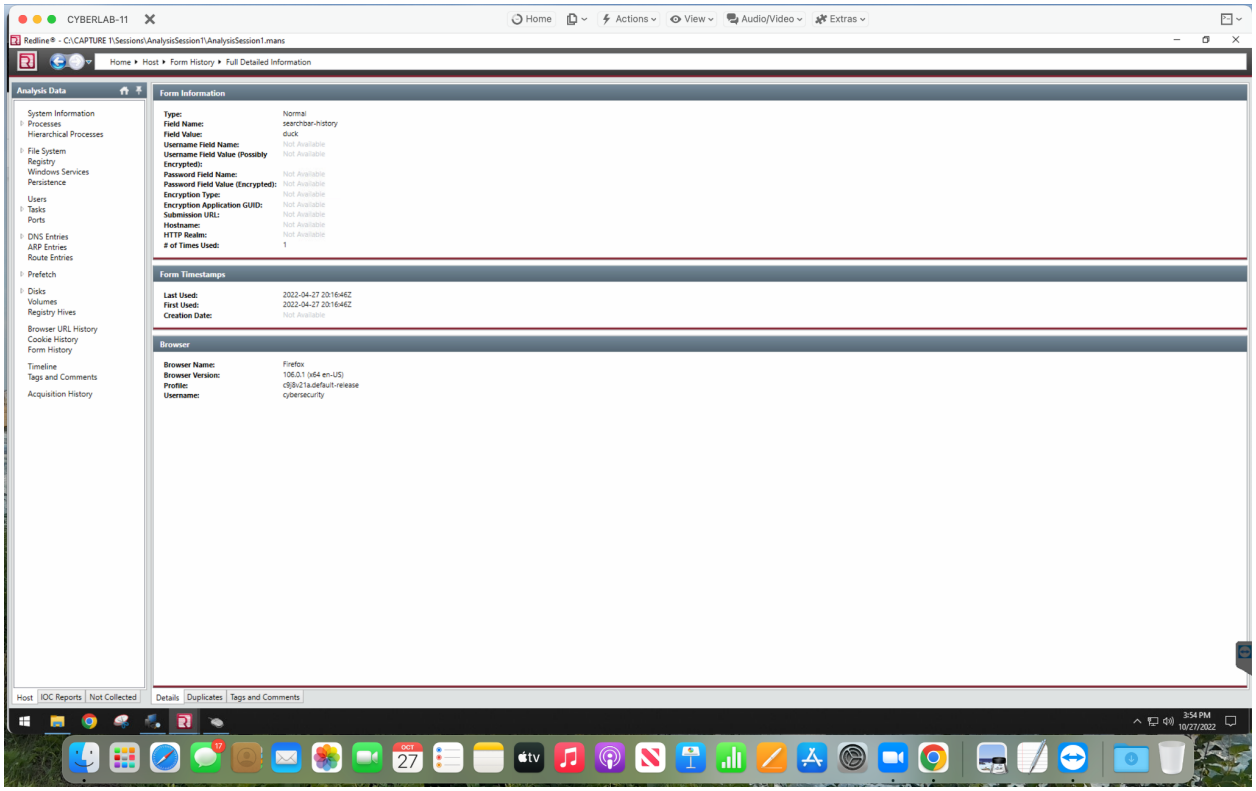

CYBERLAB-11
Home
Actions
View
Audio/Video
Extras
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ DNS Entries ▸ Full Detailed Information
Analysis Data
System Information
Processes
Hierarchical Processes
File System
Registry
Windows Services
Persistence
Users
Tasks
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: Answer
Data Length: 8 Bytes
Time To Live: 02:04:44
Record Data
Host: qb-in-f94.1e100.net
IPv4 Address:
IPv6 Address:
Address Type:
Primary Server Name:
Administrator Name:
Serial Number:
Refresh:
Retry:
Expire:
Expiration Date:
Default Time To Live:
Original Time To Live:
Mailbox Name:
Mailbox Errors Name:
MX Host:
Preference:
Bitmask:
Algorithm:
Protocol:
Key Name:
Key Length:
Key Flags:
Key Tag:
Signer:
Date Signed:
Type Covered:
Label Count:
Next Host:
Target Host:
Priority:
Weight:
Port:
Order:
Services:
Regular Expression:
Replacement:
Digest Type:
Digest Length:
Creation Date:
Error:
Mode:
Signature Length:
Fudge Time:
Original XID:
Mapping Flag:
Lookup Timeout:
Not Available
Host
IOC Reports
Not Collected
Details
Duplicates
Tags and Comments
3:52 PM
10/27/2022


CYBERLAB-11
Home
Actions
View
Audio/Video
Extras
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
Enter string to find here...
In All Fields
Clear Column Filters
Prev
Next
Cache Type
IPv4 Address
MAC Address
State
ARP Interface
Interface Type
IsRout
Last Reac...
Last Unre...
Static 224.0.0.22 00-00-00-00-00-00 127.0.0.1
Static 224.0.0.251 00-00-00-00-00-00 127.0.0.1
Static 224.0.0.252 00-00-00-00-00-00 127.0.0.1
Static 239.255.255.250 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 20-c0-47-18-72-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-8e 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-... 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-... 192.168.1.163
Dynamic 192.168.1.169 48-4d-7e-ee-3b-... 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-cb-b8-a9-... 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 224.0.0.22 01-00-5e-00-00-16 192.168.1.163
Static 224.0.0.251 01-00-5e-00-00-fb 192.168.1.163
Static 224.0.0.252 01-00-5e-00-00-fc 192.168.1.163
Static 239.255.255.250 01-00-5e-7f-ff-fa 192.168.1.163
Static 255.255.255.255 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 224.0.0.22 01-00-5e-00-00-16 192.168.126.1
Static 224.0.0.251 01-00-5e-00-00-fb 192.168.126.1
Static 224.0.0.252 01-00-5e-00-00-fc 192.168.126.1
Static 239.255.255.250 01-00-5e-7f-ff-fa 192.168.126.1
Invalid 192.168.145.128 00-0c-29-30-71-e3 192.168.145.1
Invalid 192.168.145.130 00-00-00-00-00-00 192.168.145.1
Dynamic 192.168.145.131 00-0c-29-ff-9f-eb 192.168.145.1
Static 192.168.145.255 ff-ff-ff-ff-ff-ff 192.168.145.1
Static 224.0.0.22 01-00-5e-00-00-16 192.168.145.1
61 Items
Host
IOC Reports
Not Collected
3:53 PM
10/27/2022


CYBERLAB-11
Home
Actions
View
Audio/Video
Extras
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Disks
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
Enter string to find here...
In All Fields
Clear Column Filters
Prev
Next
Disk Name
Disk Size
\\.\PhysicalDrive0
931.513 Gigabytes
\\.\PhysicalDrive1
931.513 Gigabytes
\\.\CdRom0
Host
IOC Reports
Not Collected
Show Details
3 Items
3:53 PM
10/27/2022

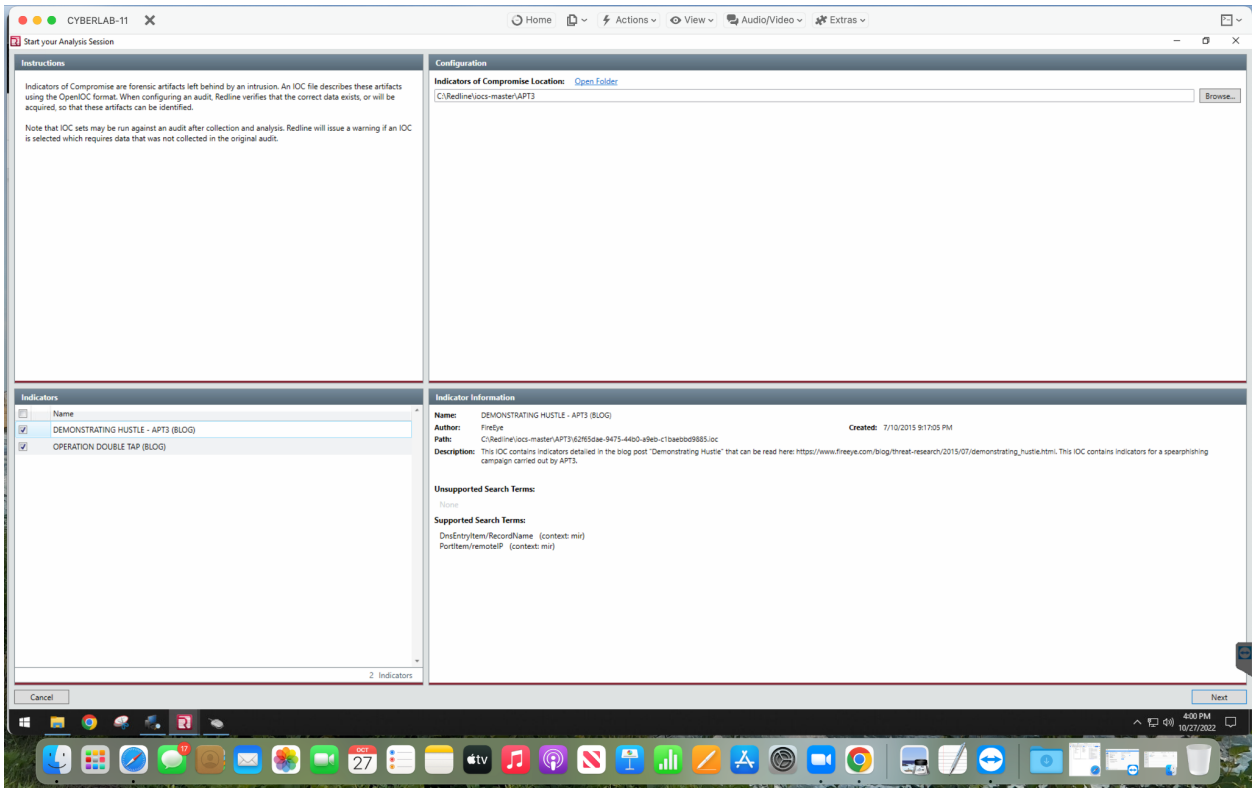

CYBERLAB-11
Home
Actions
View
Audio/Video
Extras
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Volumes
Analysis Data
Enter string to find here...
In All Fields
Clear Column Filters
Prev
Next
Drive
Name
Volume Name
Type
Device Path
File System Name
Bytes per Sector
Sectors p...
Total Allo...
Available...
Serial Number
Creation Time
Mount
File Syste
F HDD \\?\Volume{a56bcc22-27... DRIVE_FIXED \Device\HarddiskVolume3 NTFS 512 Bytes 8 244,029,... 243,047,... 110961814 2022-08-29 17:13:09Z FILE_CASE
D Storage \\?\Volume{ed503d41-46... DRIVE_FIXED \Device\HarddiskVolume7 NTFS 512 Bytes 8 127,540,... 76,105,844 1551697619 2022-08-25 17:24:10Z FILE_CASE
C Windows \\?\Volume{aab990fa-34... DRIVE_FIXED \Device\HarddiskVolume6 NTFS 512 Bytes 8 115,199,... 22,543,198 377278997 2022-08-25 17:24:09Z FILE_CASE
Recovery \\?\Volume{3558bd5d-3... DRIVE_FIXED \Device\HarddiskVolume8 NTFS 512 Bytes 8 1,288,703 1,091,487 3464353898 2022-08-25 17:24:11Z FILE_CASE
BOOT \\?\Volume{c090b106-71... DRIVE_FIXED \Device\HarddiskVolume1 FAT32 512 Bytes 8 126,720 115,506 3632537779 1601-01-01 00:00:00Z FILE_CASE
BOOT \\?\Volume{b8c17975-7c... DRIVE_FIXED \Device\HarddiskVolume4 FAT32 512 Bytes 8 126,720 119,866 1484557297 1601-01-01 00:00:00Z FILE_CASE
\VOLUME{01d8b8a77cc5d891-167cd215} 377278997 2022-08-25 17:24:09Z
\VOLUME{01d8bbca9ccc4f34-069d2496} 110961814 2022-08-29 17:13:09Z
\VOLUME{01d8b8a77cfd1f8e-5c7d06d3} 1551697619 2022-08-25 17:24:10Z
\VOLUME{00000000000000000-c629c4ac} 3324626092 1601-01-01 00:00:00Z
\VOLUME{00000000000000000-9281fe48} 2457992776 1601-01-01 00:00:00Z
Host
IOC Reports
Not Collected
11 Items
3:53 PM
10/27/2022

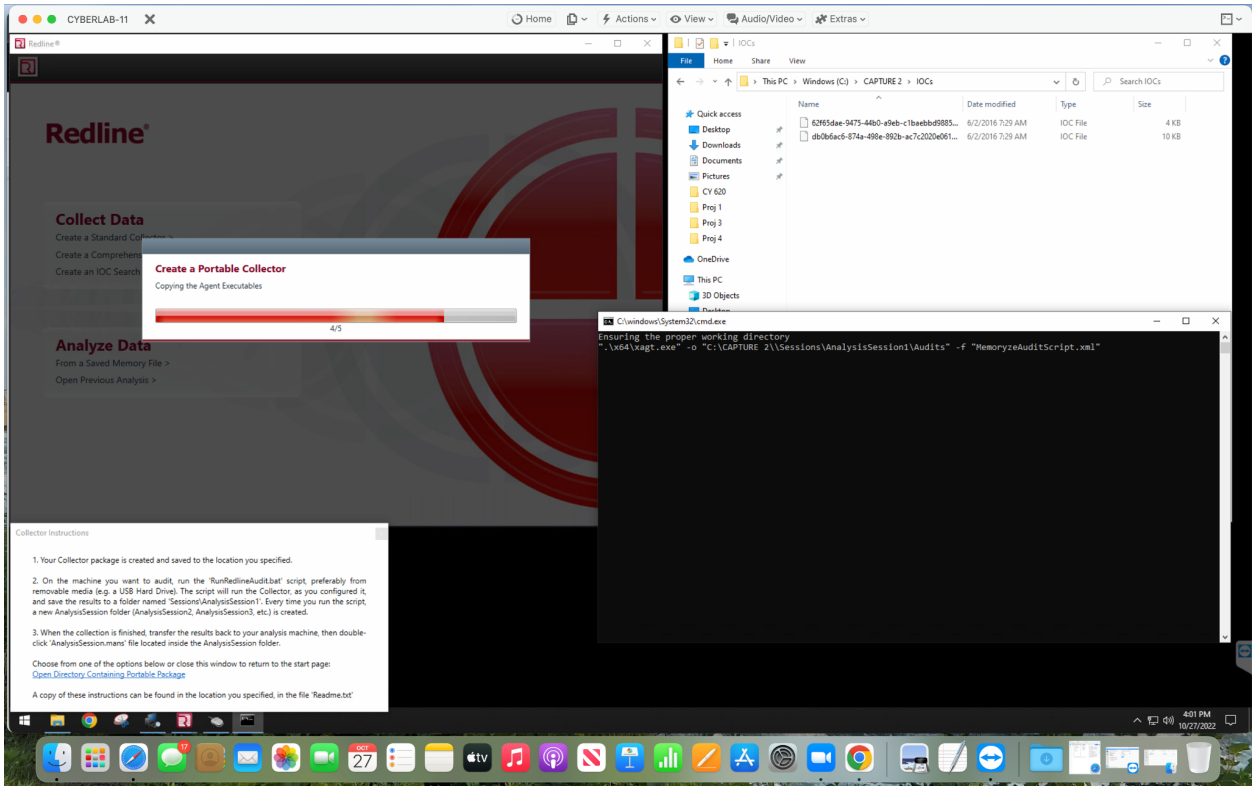

CYBERLAB-11
Home
Actions
View
Audio/Video
Extras
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Minimize
Home ▸ Host ▸ Browser URL History
Analysis Data
System Information
Processes
Hierarchical Processes
File System
Registry
Windows Services
Persistence
Users
Tasks
Ports
DNS Entries
ARP Entries
Route Entries
Prefetch
Disks
Volumes
Registry Hives
Browser URL History
Cookie History
Form History
Timeline
Tags and Comments
Acquisition History
Host
IOC Reports
Not Collected
Filters
Review Browser URL History
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 includes sites with malicious code, and sites visited only once.
If you find a record that looks suspicious, use the Timeline field filters 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 bounce a user from site to site before finally reaching 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 indication of preferential treatment.
Typed URLs
Shows only records that were visited after the user typed in the URL, which implies 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.
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
1,015 Items
3:53 PM
10/27/2022

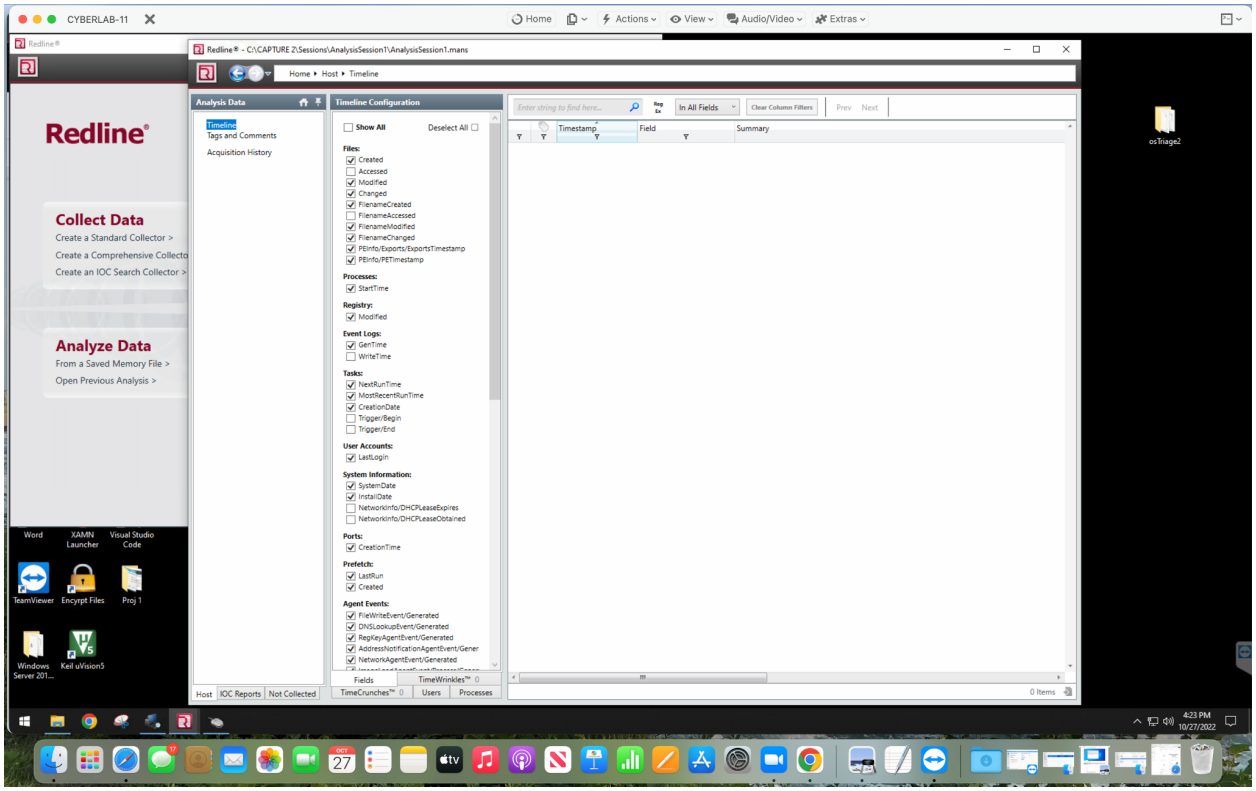

CYBERLAB-11
Home
Actions
View
Audio/Video
Extras
Redline® - C:\CAPTURE 1\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Form History ▸ Full Detailed Information
Analysis Data
Host
IOC Reports
Not Collected
Form Information
Type: Normal
Field Name: searchbar-history
Field Value: duck
Username Field Name: Not Available
Username Field Value (Possibly Encrypted): Not Available
Password Field Name: Not Available
Password Field Value (Encrypted): Not Available
Encryption Type: Not Available
Encryption Application GUID: Not Available
Submission URL: Not Available
Hostname: Not Available
HTTP Realm: Not Available
# of Times Used: 1
Form Timestamps
Last Used: 2022-04-27 20:16:46Z
First Used: 2022-04-27 20:16:46Z
Creation Date: Not Available
Browser
Browser Name: Firefox
Browser Version: 106.0.1 (x64 en-US)
Profile: cfj8vi21a.default-release
Username: cybersecurity
Details
Duplicates
Tags and Comments
3:54 PM
10/27/2022

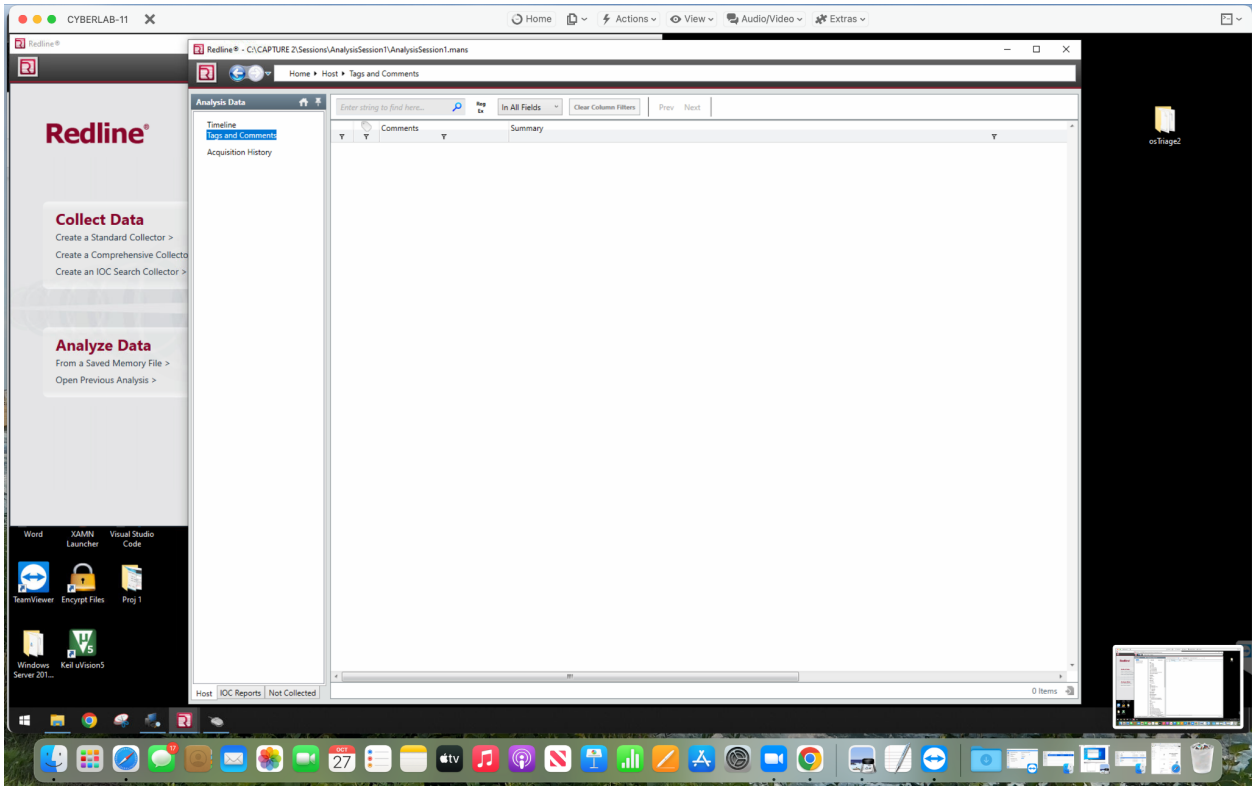
IOC (an indicator of compromise):

- 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.)




CYBERLAB-11
Redline
Collect Data
Create a Standard Collector >
Create a Comprehensive Collector >
Create an IOC Search Collector >
Analyze Data
From a Saved Memory File >
Open Previous Analysis >
Create a Portable Collector
Copying the Agent Executables
4/5
C:\windows\System32\cmd.exe
Ensuring the proper working directory
".\x64\xagt.exe" -o "C:\CAPTURE 2\\Sessions\AnalysisSession1\Audits" -f "MemoryzeAuditScript.xml"
Collector Instructions
1. Your Collector package is created and saved to the location you specified.
2. On the machine you want to audit, run the 'RunRedlineAudit.bat' script, preferably from removable media (e.g. a USB Hard Drive). The script will run the Collector, as you configured it, and save the results to a folder named 'Sessions\AnalysisSession1'. Every time you run the script, a new AnalysisSession folder (AnalysisSession2, AnalysisSession3, etc.) is created.
3. When the collection is finished, transfer the results back to your analysis machine, then double-click 'AnalysisSession.mans' file located inside the AnalysisSession folder.
Choose from one of the options below or close this window to return to the start page:
Open Directory Containing Portable Package
A copy of these instructions can be found in the location you specified, in the file 'Readme.txt'
4:01 PM
10/27/2022


CYBERLAB-11
Redline
Collect Data
Create a Standard Collector >
Create a Comprehensive Collecto
Create an IOC Search Collector >
Analyze Data
From a Saved Memory File >
Open Previous Analysis >
Redline® - C:\CAPTURE 2\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Timeline
Analysis Data
Timeline
Tags and Comments
Acquisition History
Timeline Configuration
Show All
Deselect All
Files:
Created
Accessed
Modified
Changed
FilenameCreated
FilenameAccessed
FilenameModified
FilenameChanged
PEInfo/Exports/ExportsTimestamp
PEInfo/PETimestamp
Processes:
StartTime
Registry:
Modified
Event Logs:
GenTime
WriteTime
Tasks:
NextRunTime
MostRecentRunTime
CreationDate
Trigger/Begin
Trigger/End
User Accounts:
LastLogin
System Information:
SystemDate
InstallDate
NetworkInfo/DHCPLeaseExpires
NetworkInfo/DHCPLeaseObtained
Ports:
CreationTime
Prefetch:
LastRun
Created
Agent Events:
FileWriteEvent/Generated
DNSLookupEvent/Generated
RegKeyAgentEvent/Generated
Timestamp
Field
Summary
Host
IOC Reports
Not Collected
Fields
TimeWrinkles™
TimeCrunches™
Users
Processes
0 Items
osTriage2
Word
XAMN Launcher
Visual Studio Code
TeamViewer
Encrypt Files
Proj 1
Windows Server 201...
Keil uVision5
4:23 PM
10/27/2022



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.