CY-640 - Cyber Crime and Forensics Labs

Nikhil Patel

Spring Trimester 2022

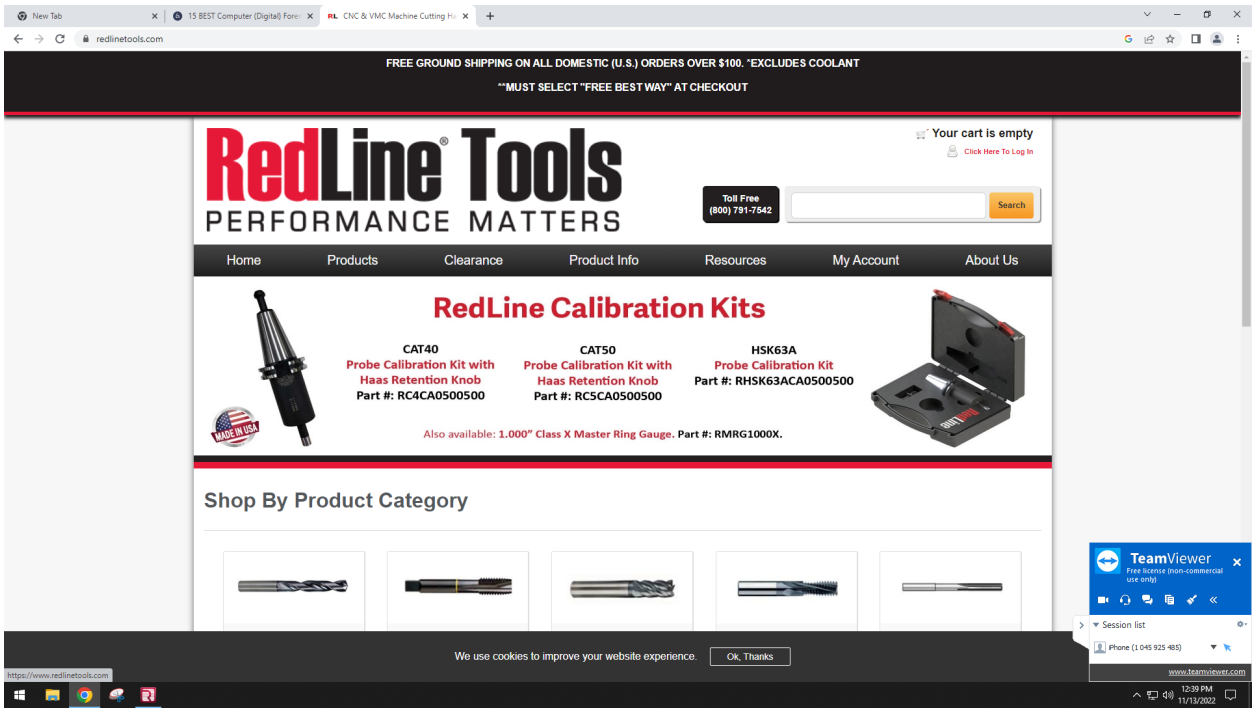
11/15/2022

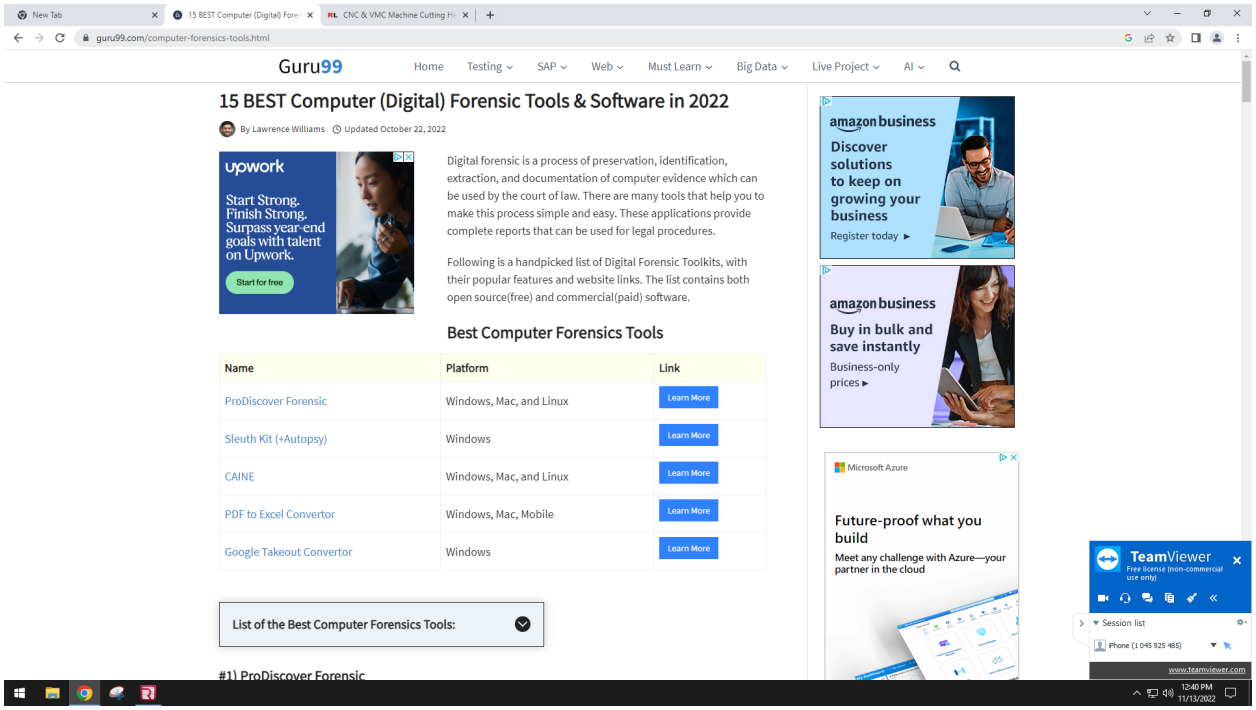
Project: INTERNET BROWSER MEMORY FORENSICS

OBJECTIVE: The primary objective of this research is to elucidate the concept of internet browser memory forensics and underscore its growing significance in the field of digital investigations. This paper aims to provide users with a comprehensive understanding of the intricate ways in which internet browsers store data within memory, along with the potential exploitable aspects for forensic purposes. Furthermore, it seeks to offer a practical guide on conducting an effective internet browser memory forensics study, coupled with a compelling exploration of captivating use cases unveiled by pioneering researchers in the field. Through this research, we aspire to contribute to the broader comprehension of memory forensics and its application in modern cybersecurity and digital forensics practices.

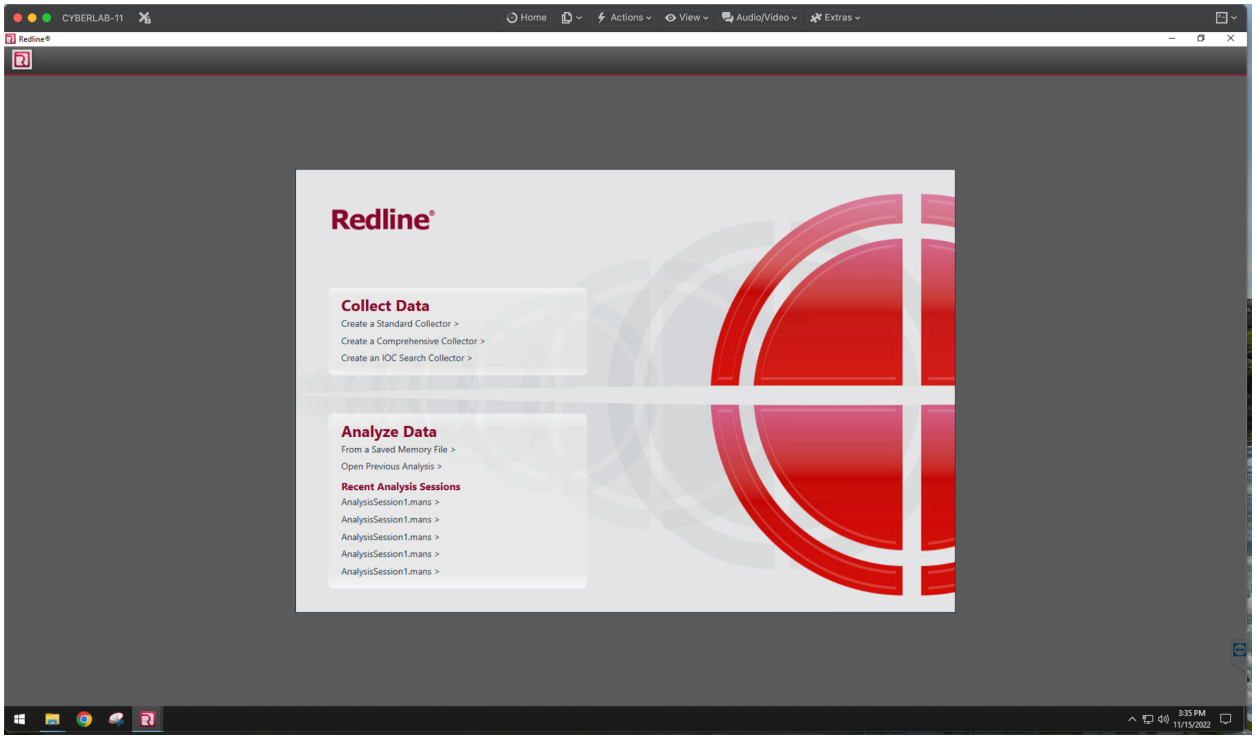
PROCEDURE:

1. In the first step, we will open an internet browser and search the internet for redline tools.

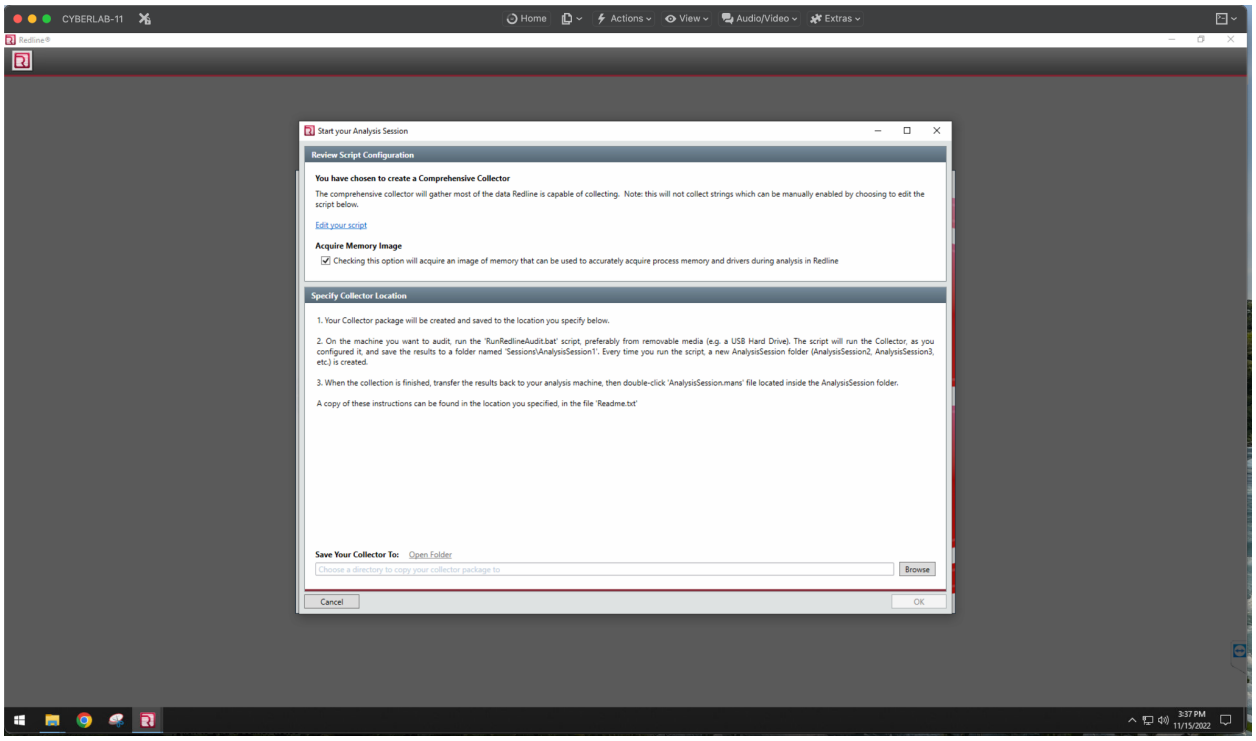


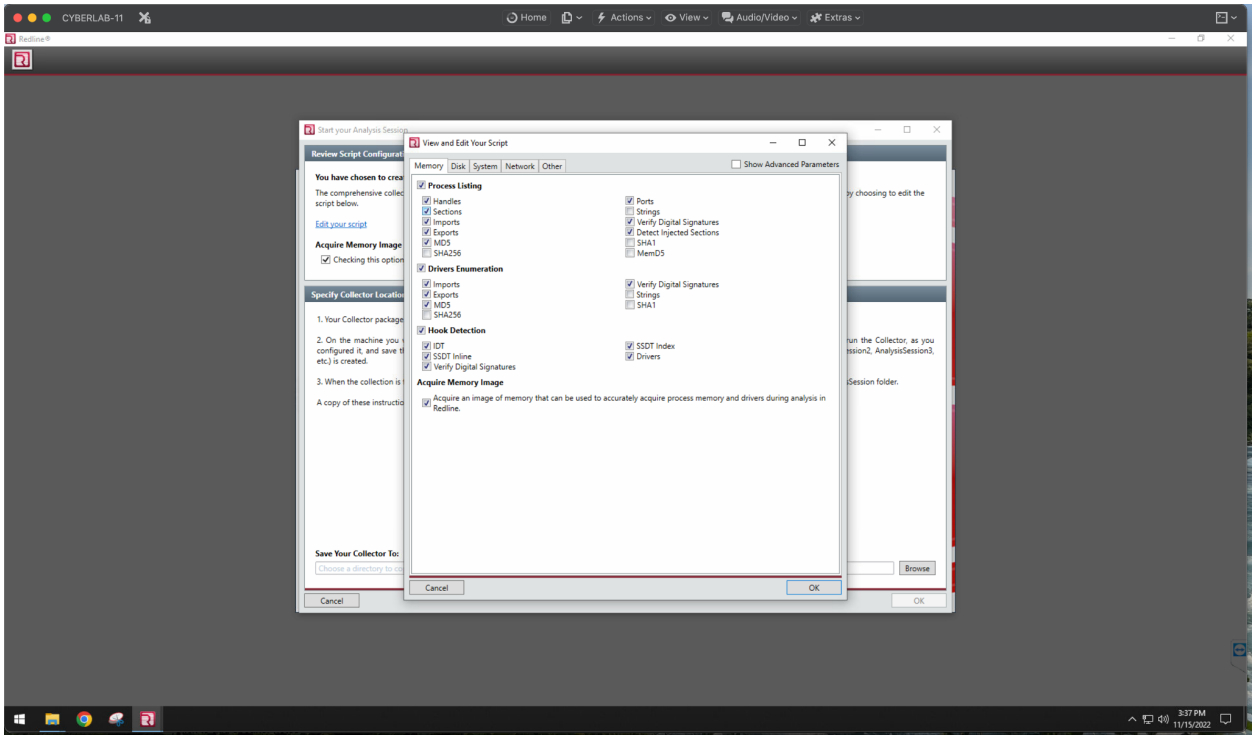


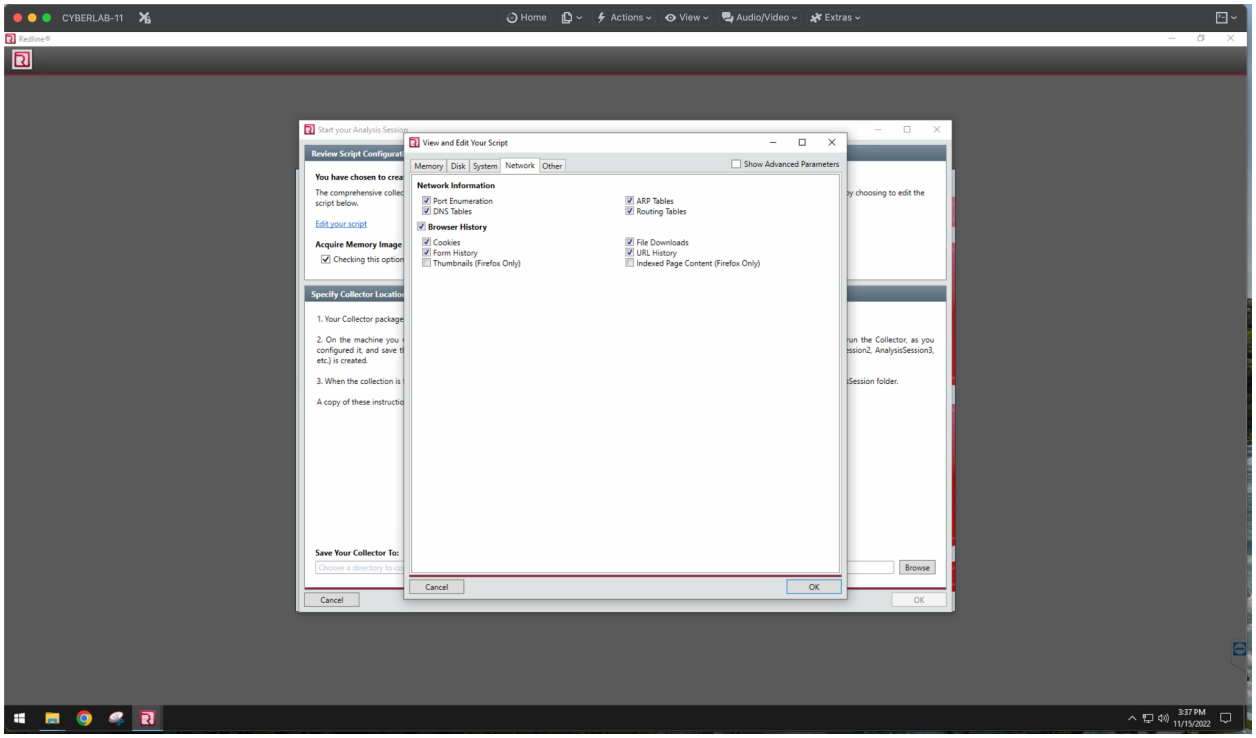
2. Click on the Start button and type redline, if the tool has not been downloaded yet, please download it from the link provided by a professor to the Forensics tool.
3. Open the Redline tool and select Create a Comprehensive Collector for the memory forensic so that we may get data from volatile memory since volatile data can only be obtained if the device is in a functional condition.



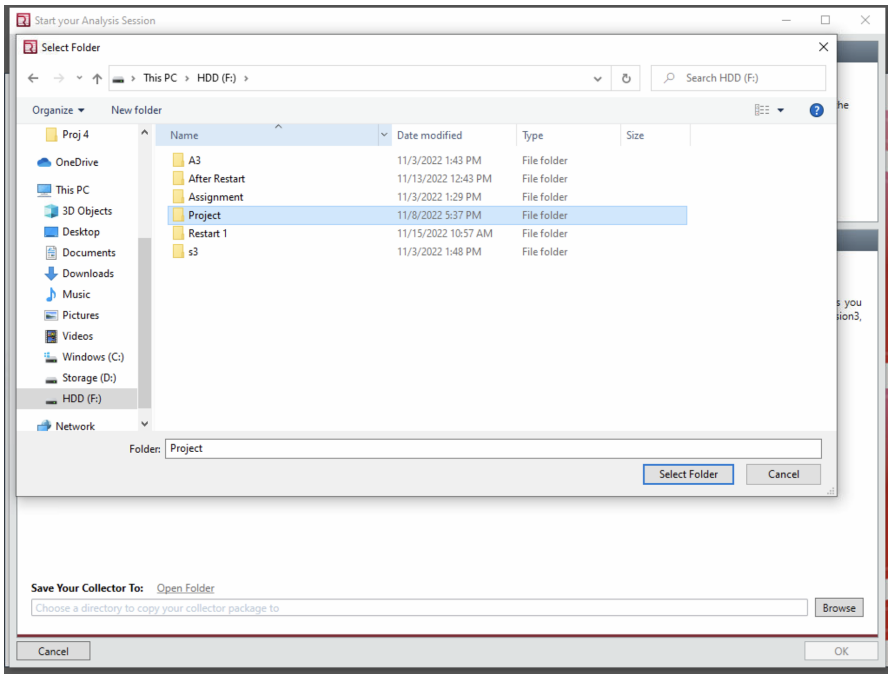
4. To obtain data from RAM, click Acquire Memory Image.
5. Now, return to the script and ensure that all of the RAM data is checked. Remember that we only want data from RAM; we don't want data from the network or disk, so uncheck them.



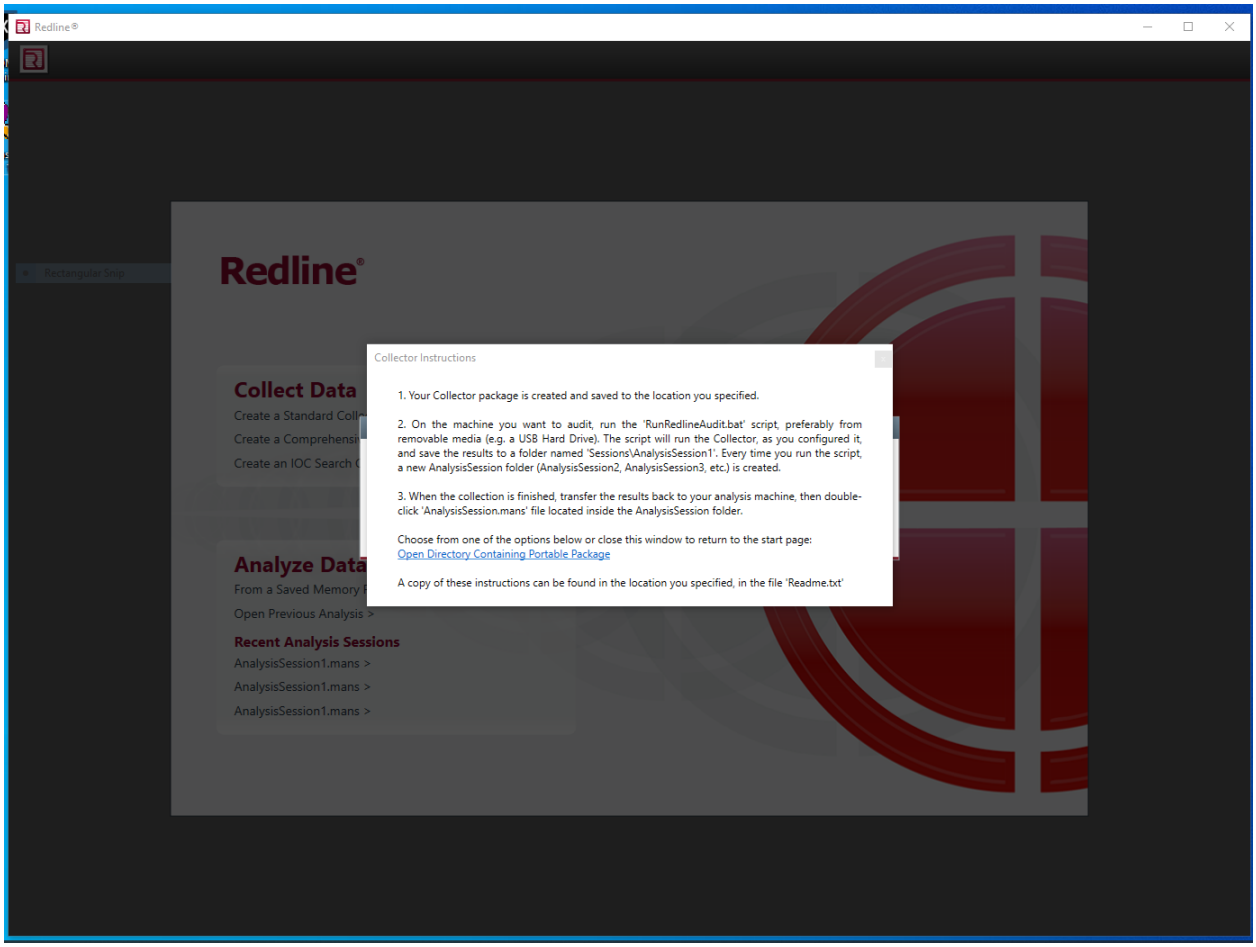




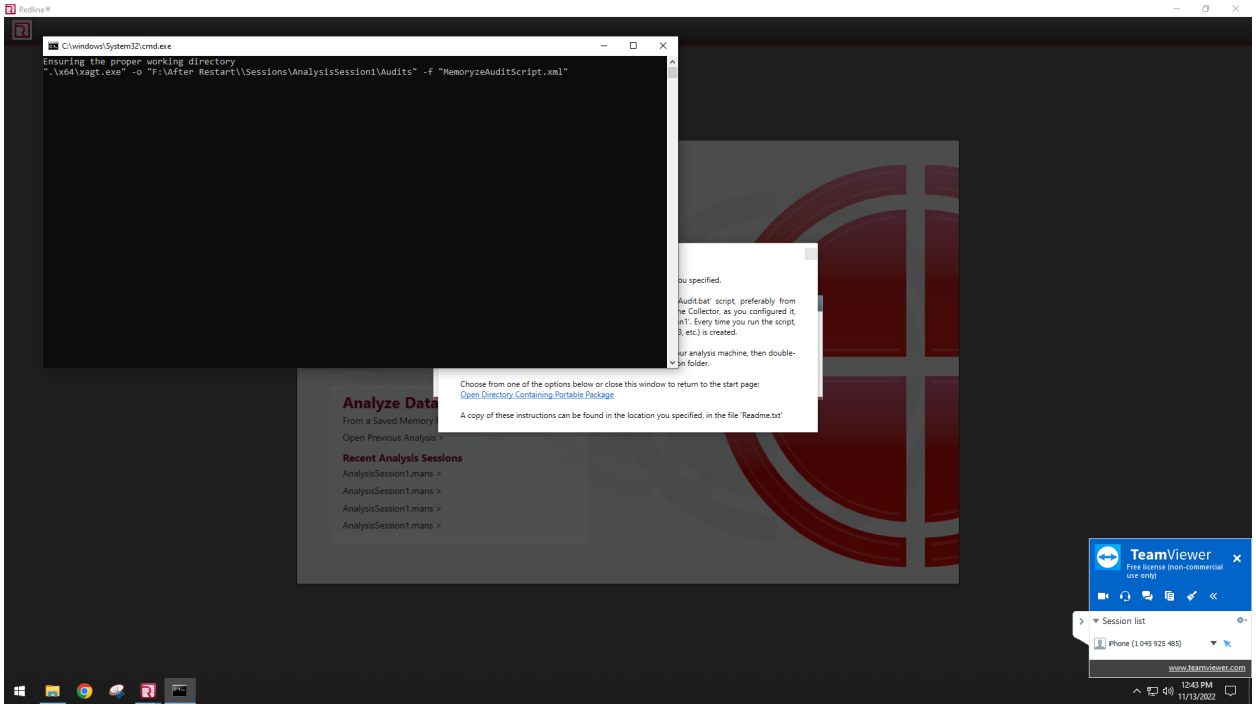
6. After you've finished changing the script, dismiss the box and navigate to the folder where you want to save the data. In this scenario, we saved the data to an external disk and separated it into two folders: Before and After Restart. This allows us to examine both files.
7. After selecting the folder, click OK to launch the program.



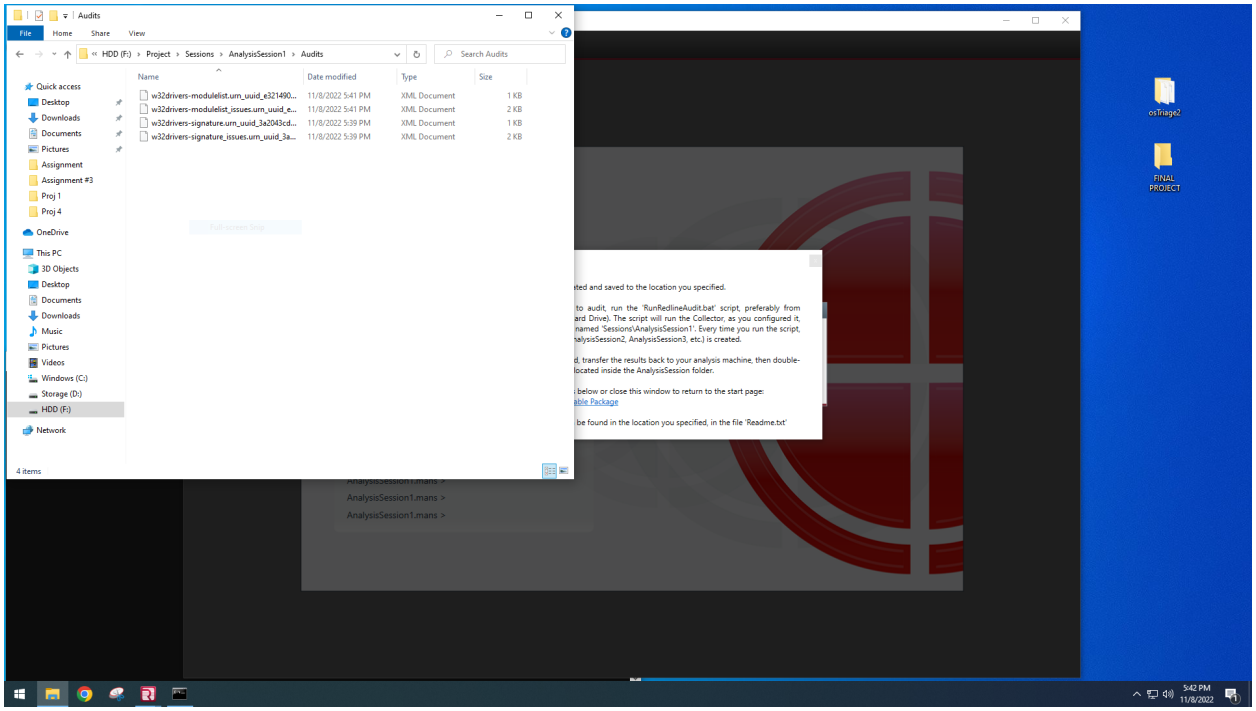
8. You will be prompted to execute the file from the folder. Navigate to folder



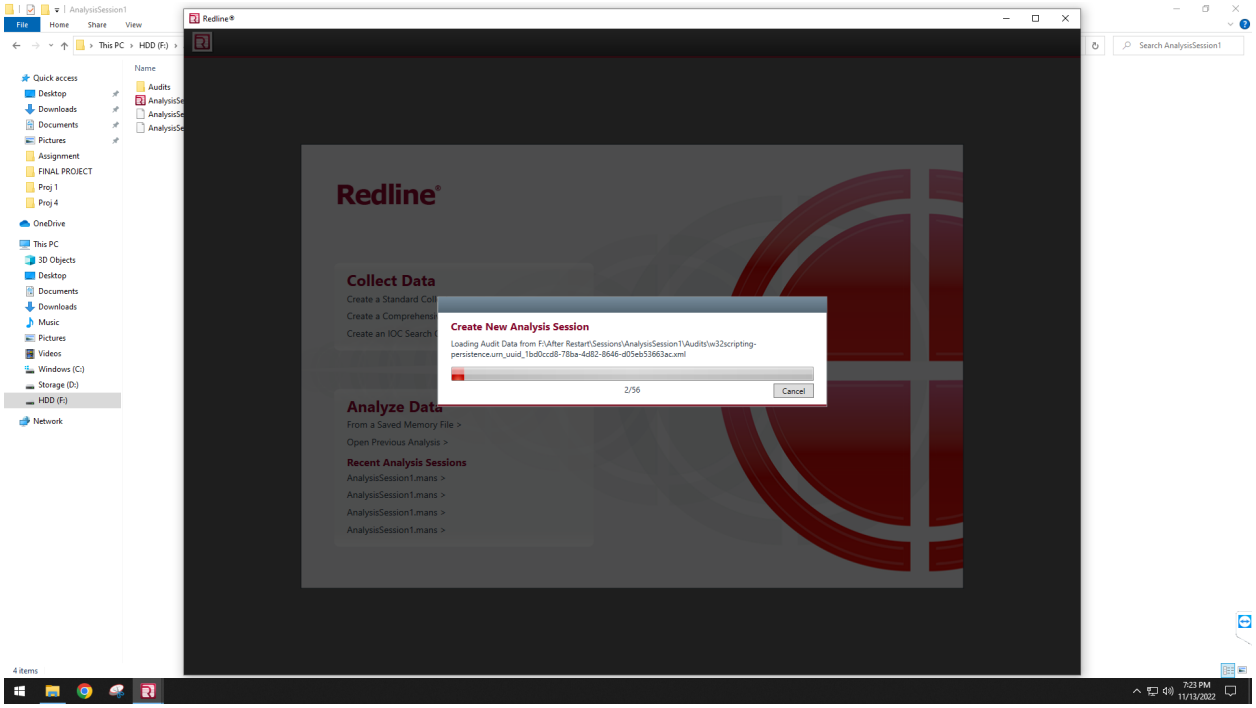
9. You will notice the command prompt performing a command; now, leave the lab alone till the CMD closes itself.



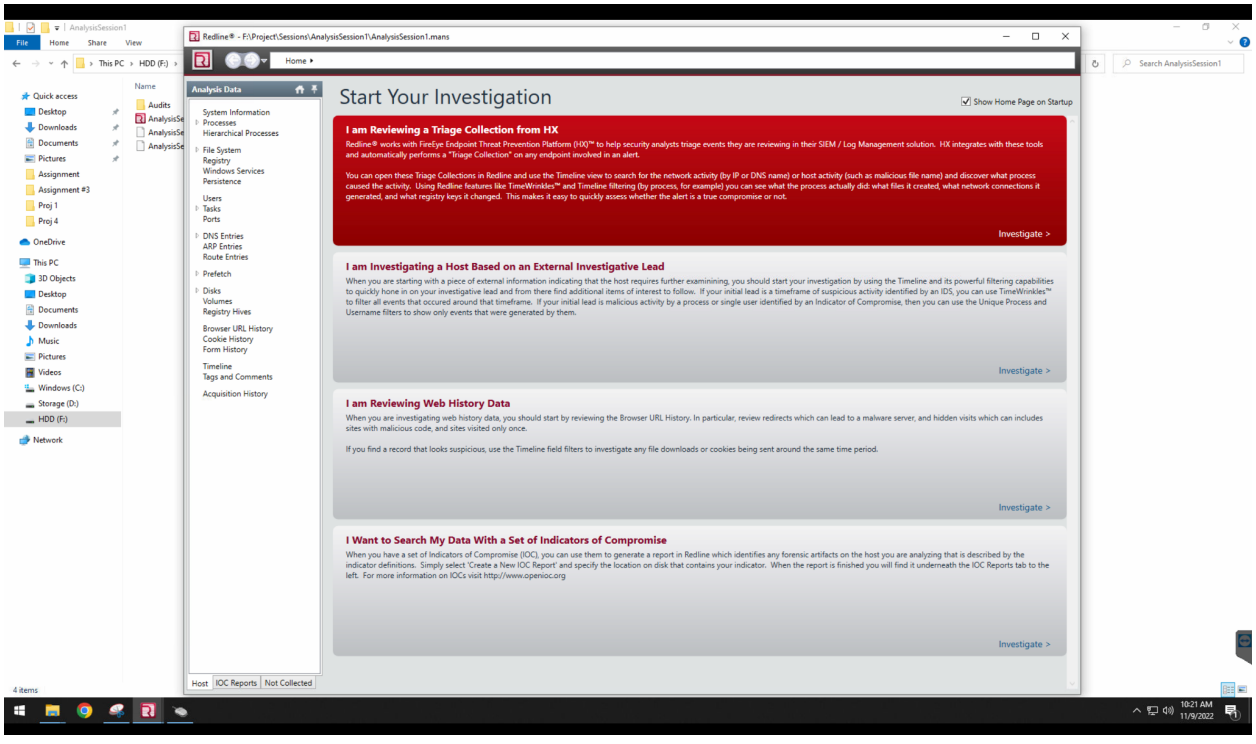
10. The first half took us about 4.5 hours.
11. When you execute the program, you will see that a new session is generated; navigate to folder and sessions > AnalysisSession1 > Audits. Wait until cmd automatically closes after one or two files are produced.



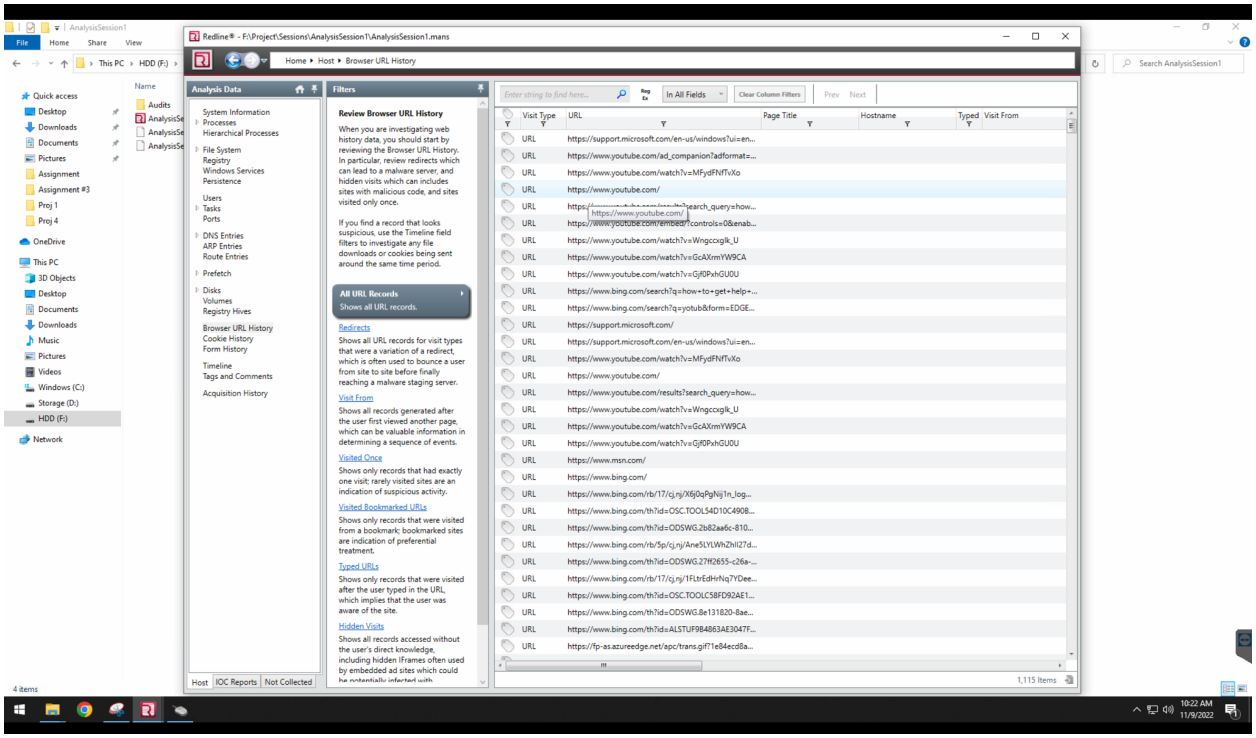
12. After you have closed cmd, you may access a file produced in Sessions > AnalysisSession.

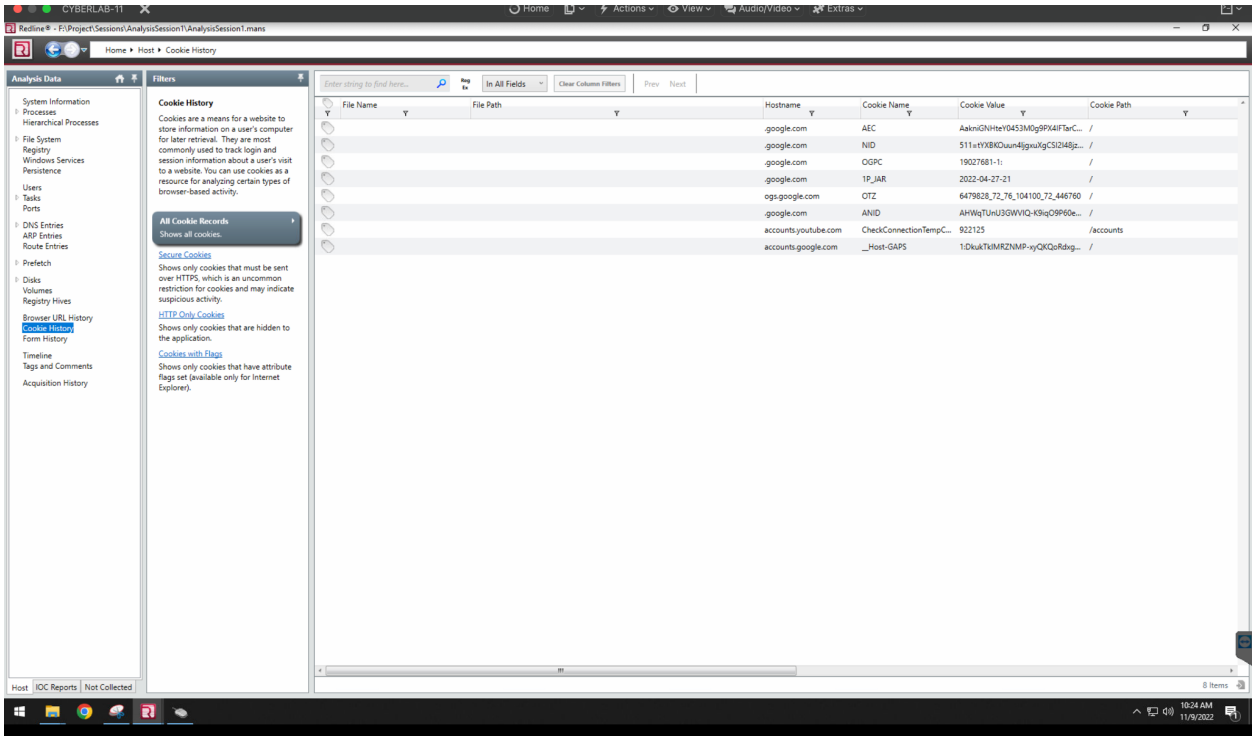


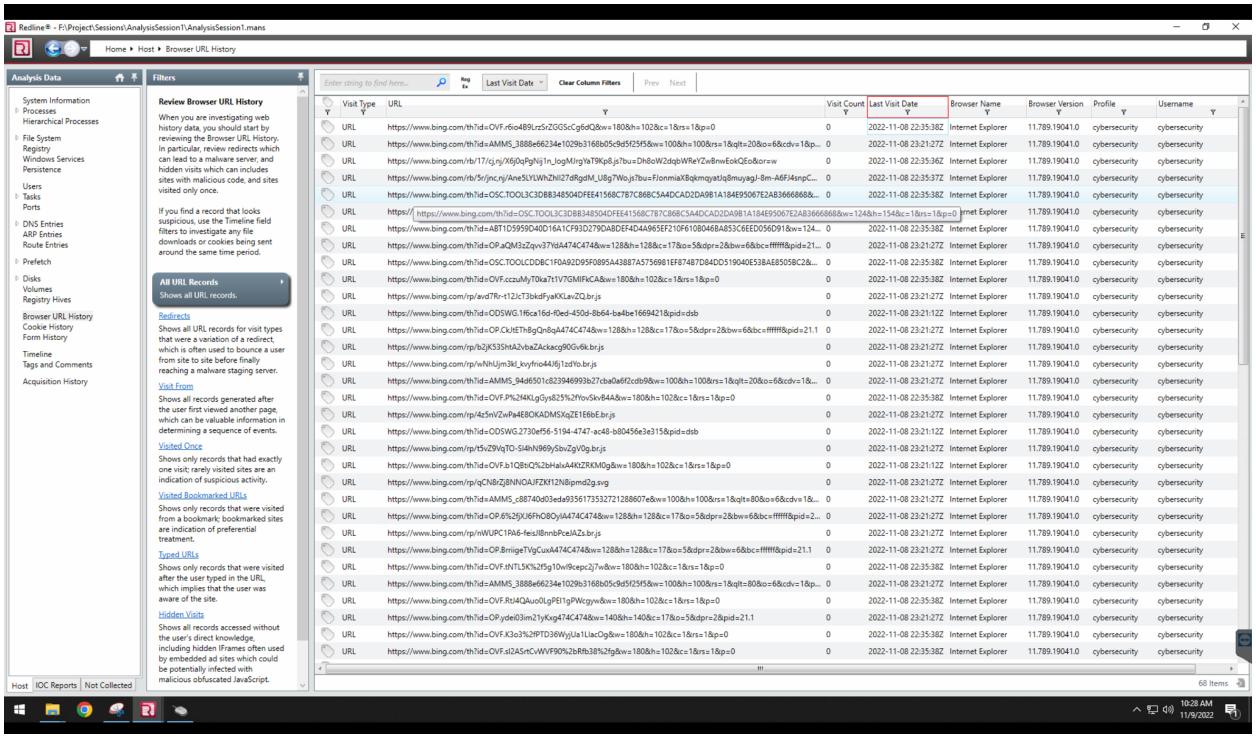
13. Select Brower URL History or I am Reviewing Web History Data now.

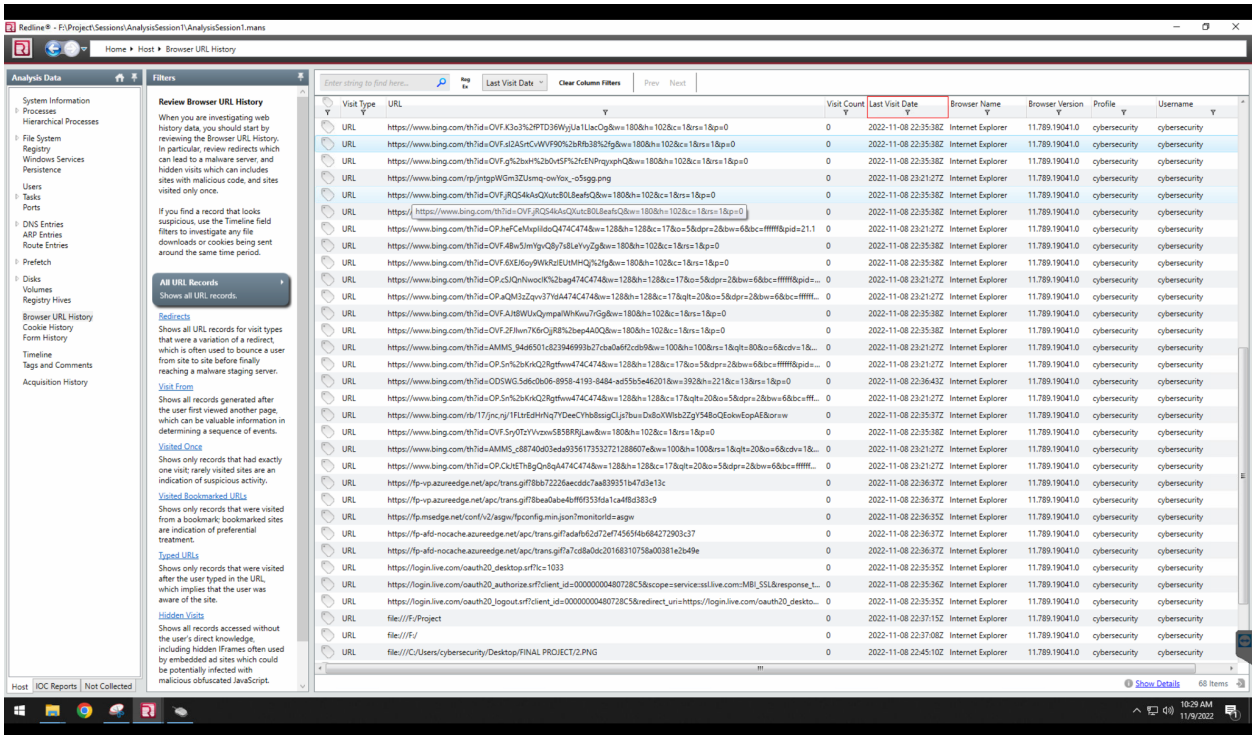


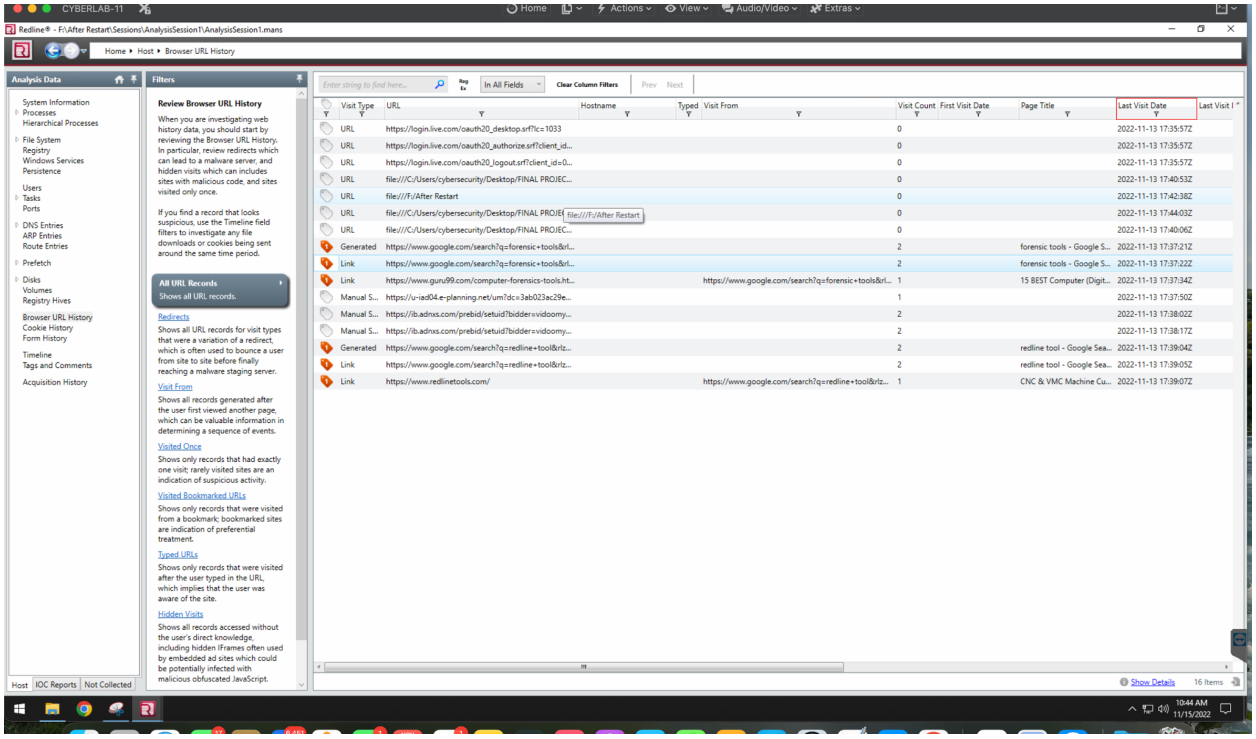
14. You will see URL records, which you can search for or filter based on.

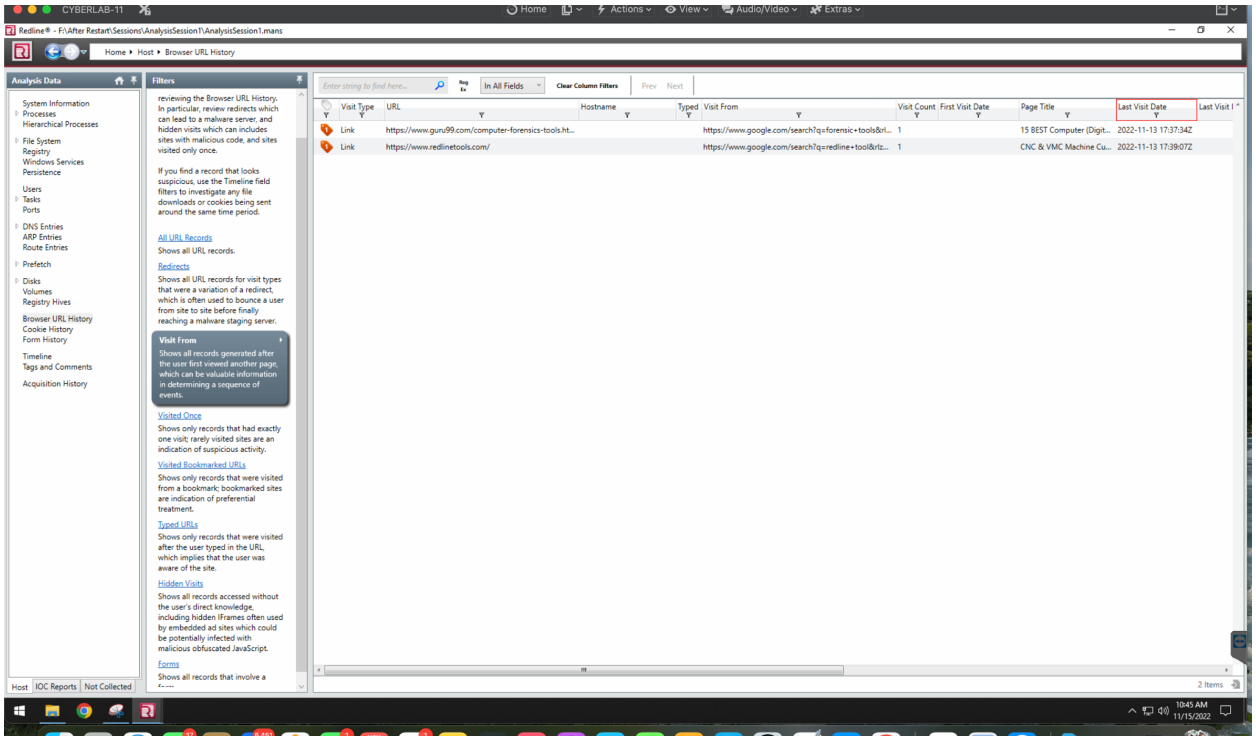

Redline® - F:\Project\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Browser URL History
Analysis Data
Filters
Review Browser URL History
All URL Records
Shows all URL records.
Redirects
Visit From
Visited Once
Visited Bookmarked URLs
Typed URLs
Hidden Visits
Visit Type
URL
Page Title
Hostname
Typed
Visit From
1,115 Items
Host
IOC Reports
Not Collected


Redline® - F:\Project\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Cookie History
Analysis Data
Filters
Cookie History
All Cookie Records
Shows all cookies.
Secure Cookies
HTTP Only Cookies
Cookies with Flags
File Name
File Path
Hostname
Cookie Name
Cookie Value
Cookie Path
8 Items
Host
IOC Reports
Not Collected

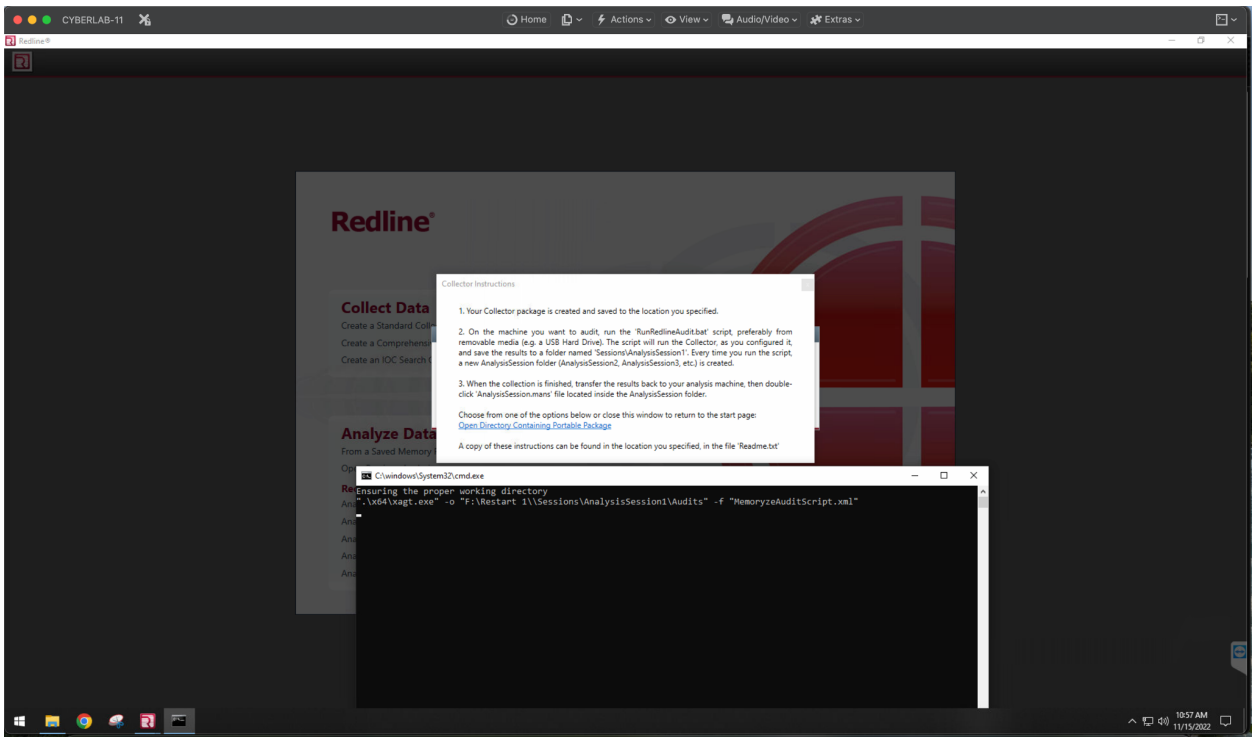

Redline® - F:\Project\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Browser URL History
Analysis Data
System Information
Processes
Hierarchical Processes
File System
Registry
Windows Services
Persistence
Users
Tasks
Ports
DNS Entries
ARP Entries
Route Entries
Prefetch
Disks
Volumes
Registry 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...
Reg Ex
Last Visit Date
Clear Column Filters
Prev
Next
Visit Type
URL
Visit Count
Last Visit Date
Browser Name
Browser Version
Profile
Username
68 Items
10:28 AM
11/9/2022

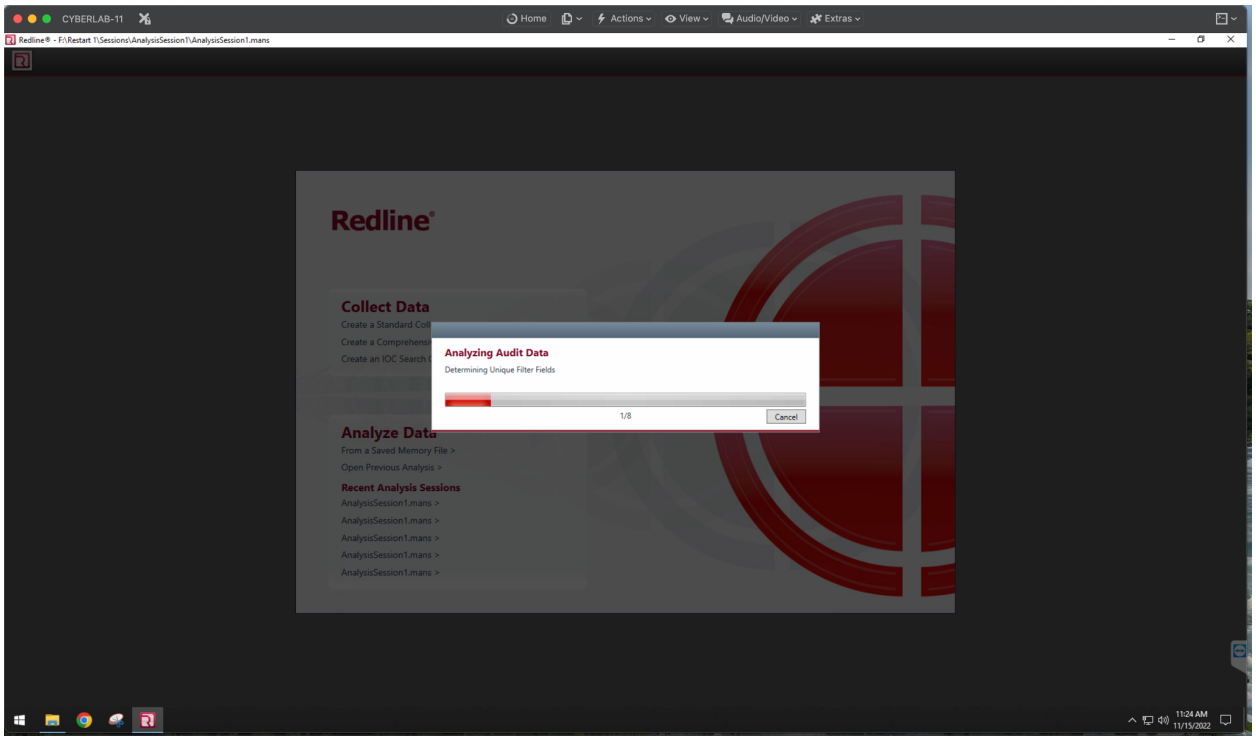

Redline® - F:\Project\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Browser URL History
Analysis Data
Filters
Review Browser URL History
All URL Records
Shows all URL records.
Redirects
Visit From
Visited Once
Visited Bookmarked URLs
Typed URLs
Hidden Visits
Host
IOC Reports
Not Collected
Enter string to find here...
Last Visit Date
Clear Column Filters
Prev
Next
Visit Type
URL
Visit Count
Last Visit Date
Browser Name
Browser Version
Profile
Username
Show Details
68 Items
10:29 AM
11/9/2022


CYBERLAB-11
Redline® - F:\After Restart\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Browser URL History
Analysis Data
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.
Visit Type
URL
Hostname
Typed
Visit From
Visit Count
First Visit Date
Page Title
Last Visit Date
Show Details
16 Items
10:44 AM
11/15/2022

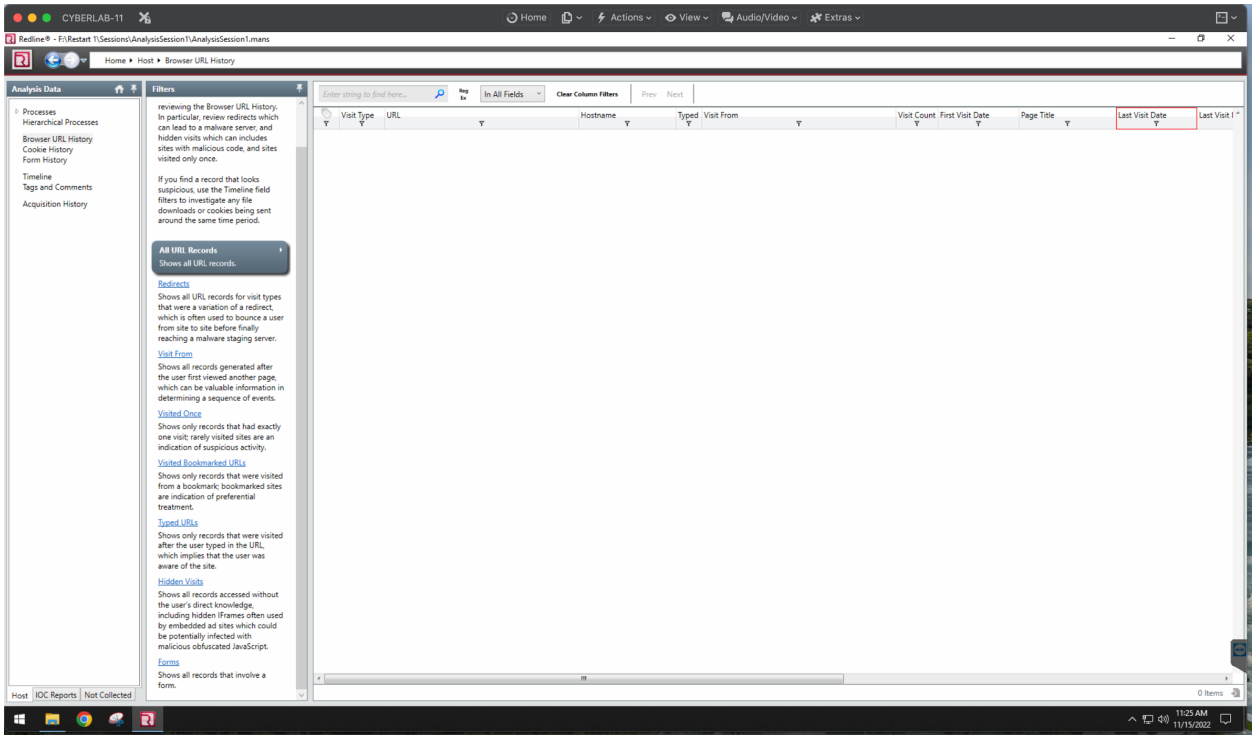

CYBERLAB-11
Redline® - F:\After Restart\Sessions\AnalysisSession1\AnalysisSession1.mans
Home ▸ Host ▸ Browser URL History
Analysis Data
Filters
Visit From
Shows all records generated after the user first viewed another page, which can be valuable information in determining a sequence of events.
Visit Type
URL
Hostname
Typed
Visit From
Visit Count
First Visit Date
Page Title
Last Visit Date
2 Items
10:45 AM
11/15/2022

AFTER RESTART





CONCLUSION



To sum it up, this project has taken us on a journey through the complex realm of internet browser memory forensics, revealing its crucial role in modern digital investigations. As we delved into this field, we came to realize that accessing data such as visited URLs, clicked links, browser cookies, and more relies heavily on the condition of the device. This determination is expertly aided by the Redline tool.

One key insight emerged from the successful collection of volatile data: it hinges on the operational state of the device. An interesting finding came to light as we progressed: restarting the device can compromise the retrieval of volatile data, leading to only partial insights from non-volatile data.

In essence, our exploration underscores the critical importance of thorough and timely memory analysis, especially in situations where immediate access to volatile data plays a vital role. As we navigate the ever-evolving landscape of cybersecurity and digital forensics, grasping these nuances becomes paramount.

This project not only deepened our understanding of memory forensics but also fostered a greater appreciation for the intricacies governing the recovery of crucial digital evidence. Armed with this newfound knowledge, we move forward, contributing to the broader mission of enhancing digital landscape security through advanced forensic practices.