

CY-640 - Cyber Crime and Forensics Labs

Nikhil Patel

Spring Trimester 2022

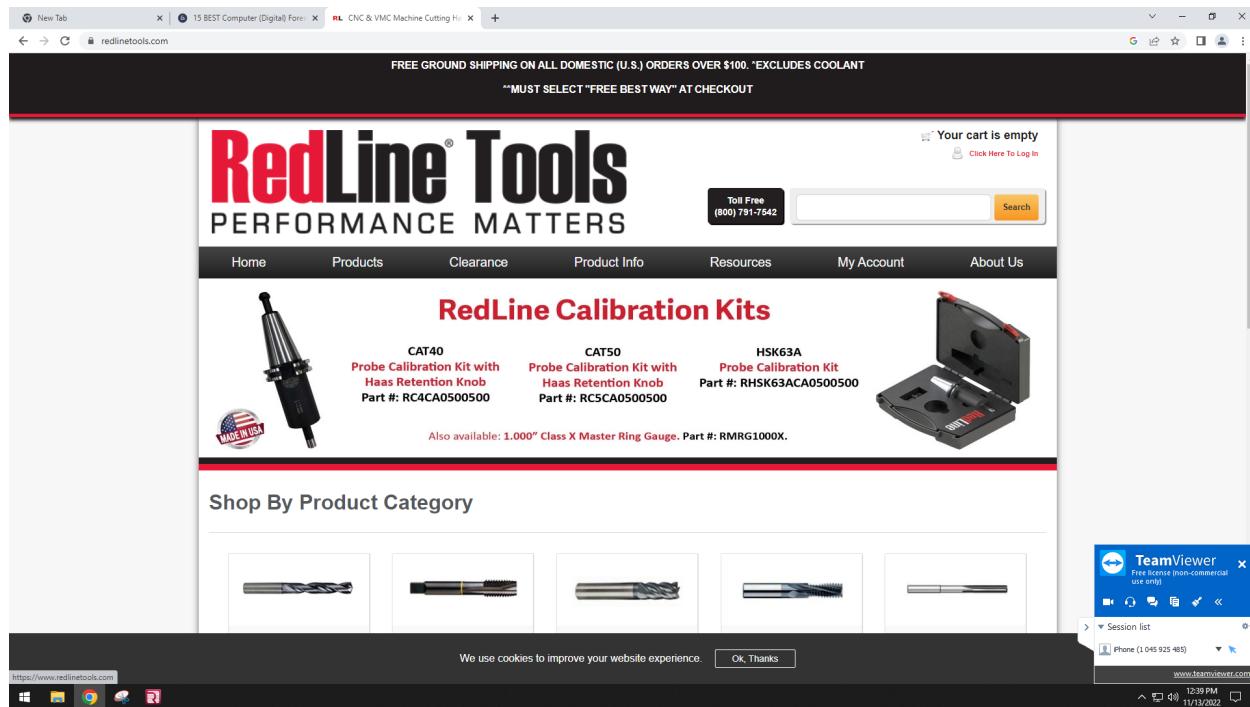
11/15/2022

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.

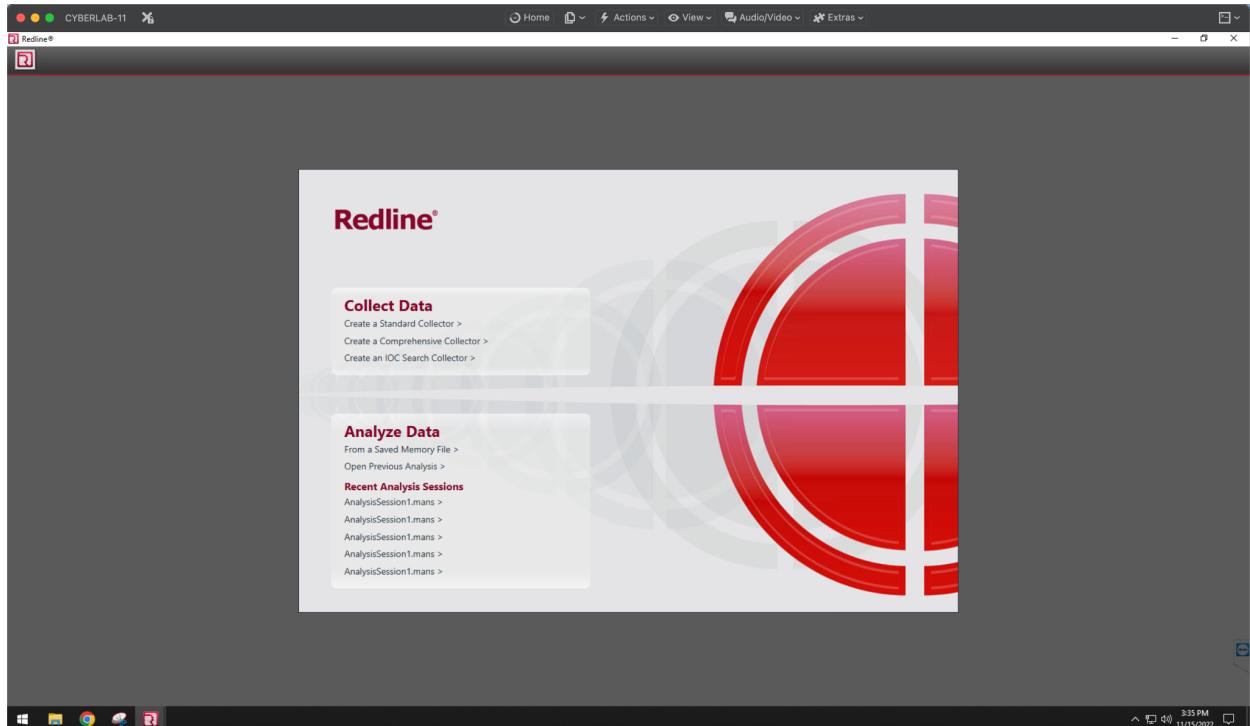


The screenshot shows a web browser window with multiple tabs open. The active tab is titled "15 BEST Computer (Digital) Forensic Tools & Software in 2022" from Guru99. The page content includes a sidebar for Upwork, an advertisement for Amazon Business, and another for Microsoft Azure. A sidebar also promotes TeamViewer. The main content area lists 15 forensic tools with their names, platforms, and links. Below this is a section titled "Best Computer Forensics Tools" with a table:

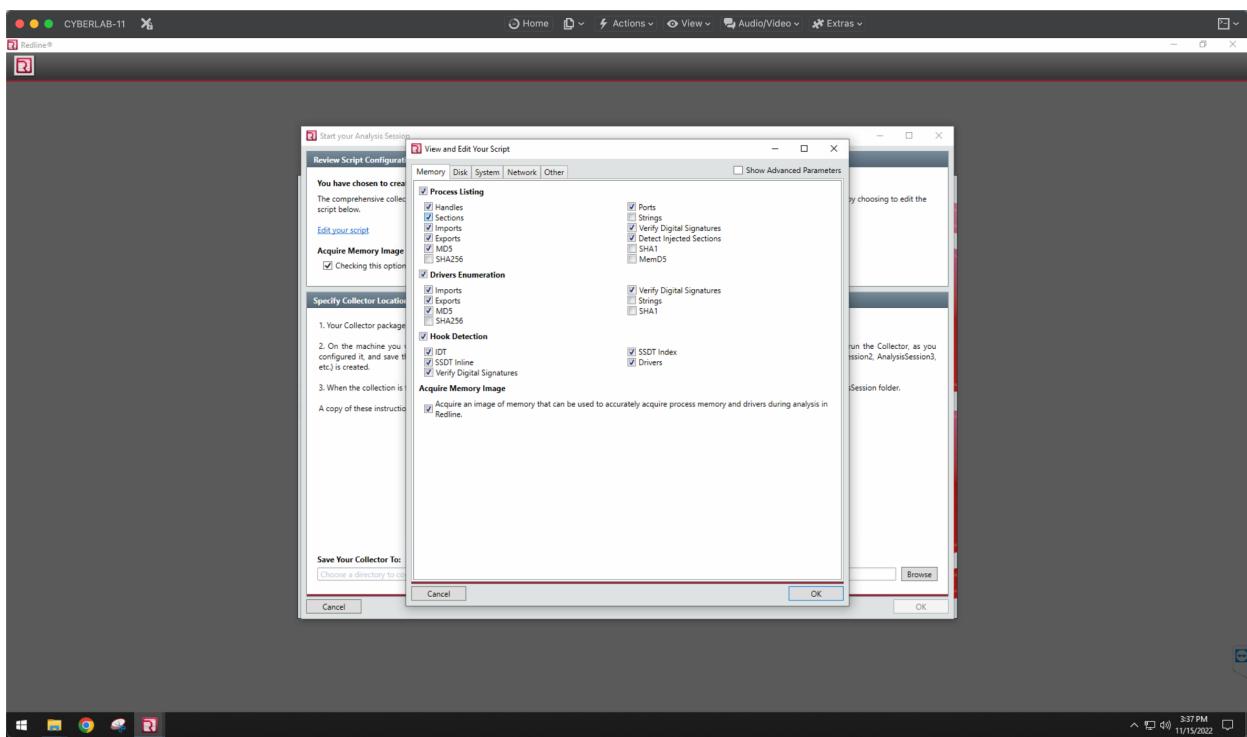
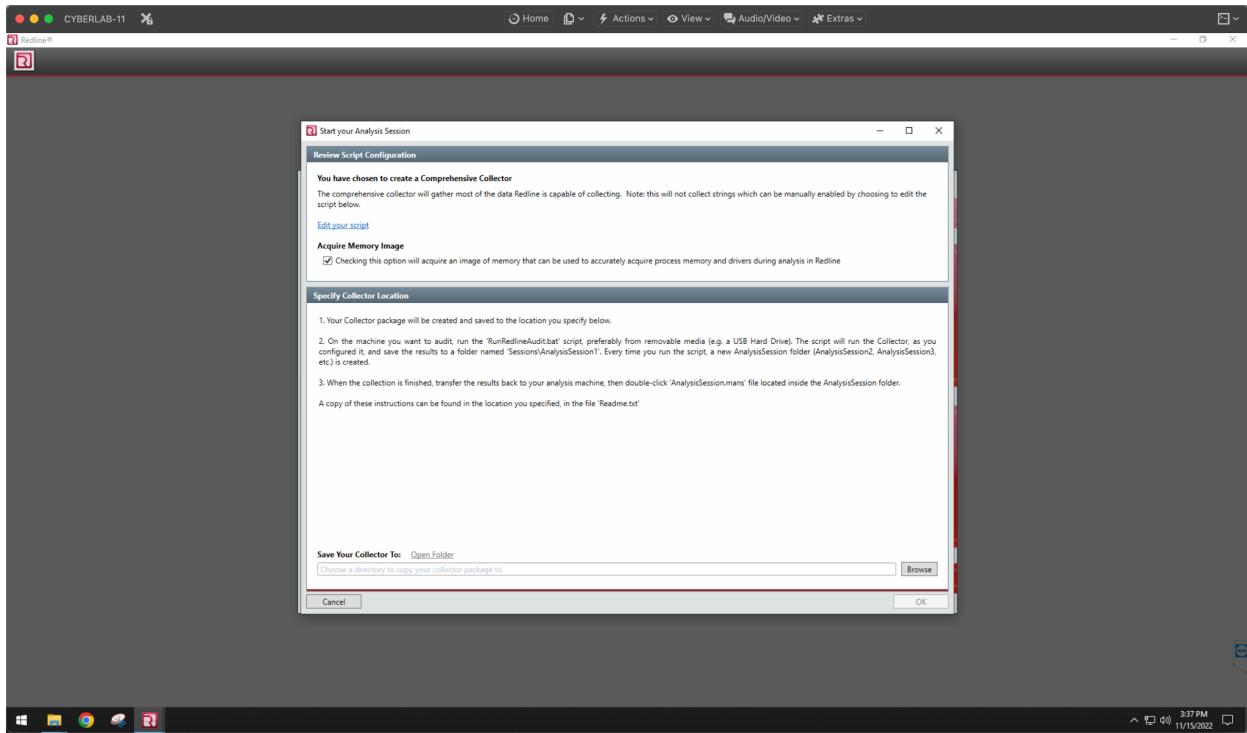
Name	Platform	Link
ProDiscover Forensic	Windows, Mac, and Linux	Learn More
Sleuth Kit (+Autopsy)	Windows	Learn More
CAINE	Windows, Mac, and Linux	Learn More
PDF to Excel Convertor	Windows, Mac, Mobile	Learn More
Google Takeout Convertor	Windows	Learn More

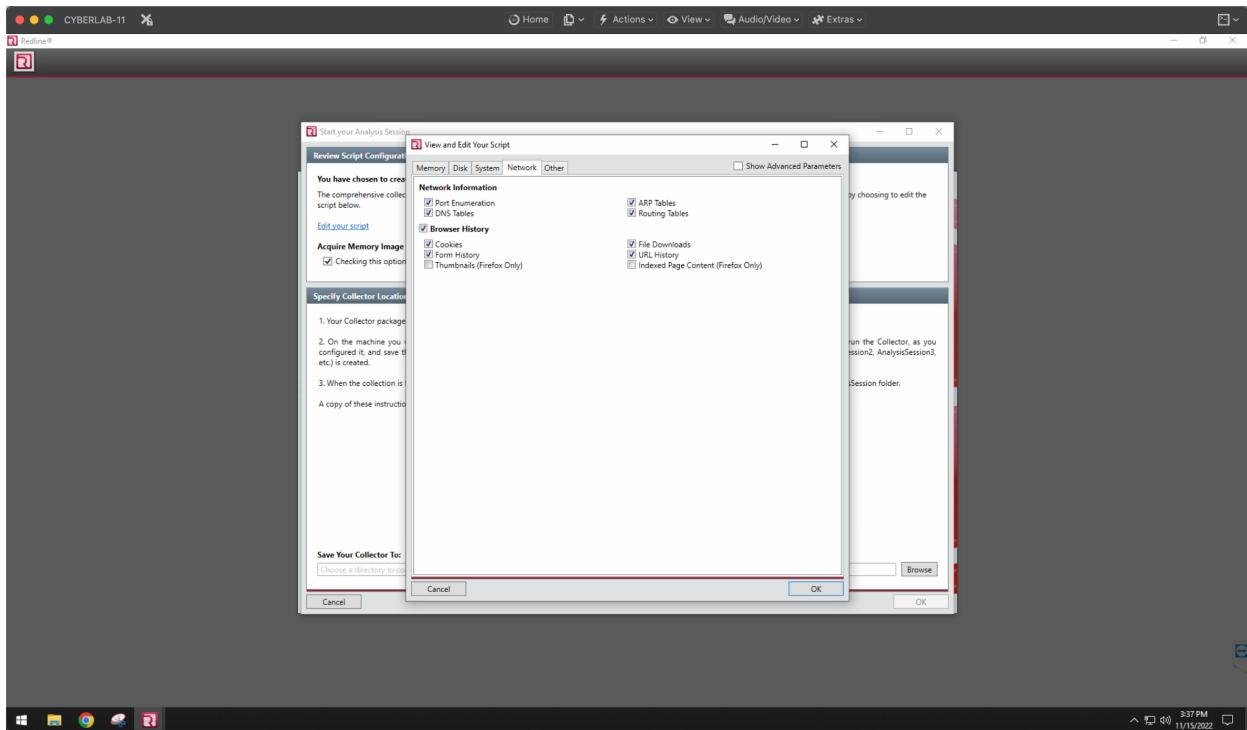
At the bottom of the page, there's a "List of the Best Computer Forensics Tools:" dropdown menu. The taskbar at the bottom shows icons for various applications, including a Redline icon.

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.

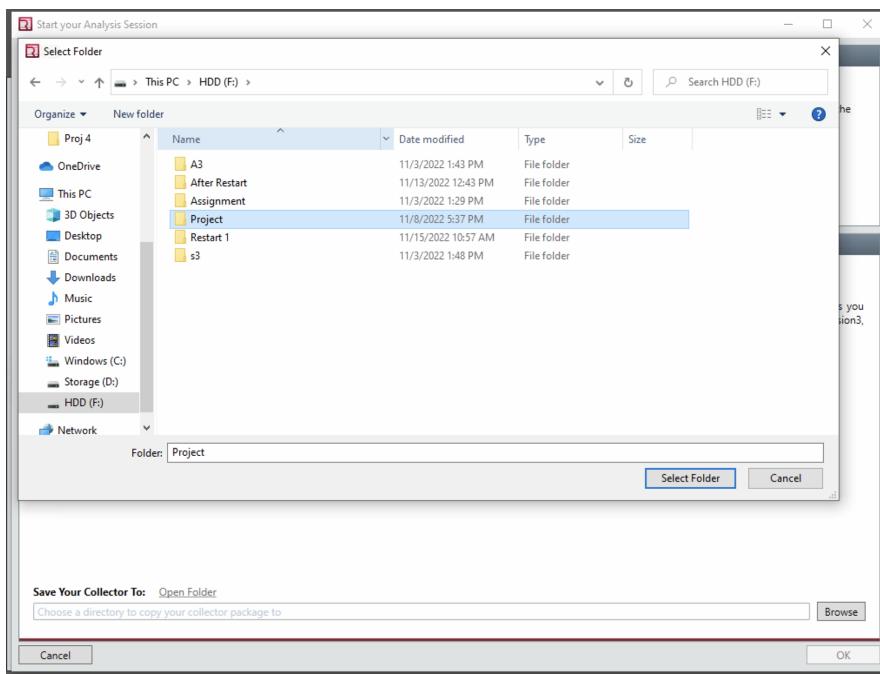


4. To obtain data from RAM, click Acquire Memory Image.
5. Now, return to the script and ensure that all of the RAM data is checked. Remember that we only want data from RAM; we don't want data from the network or disk, so uncheck them.

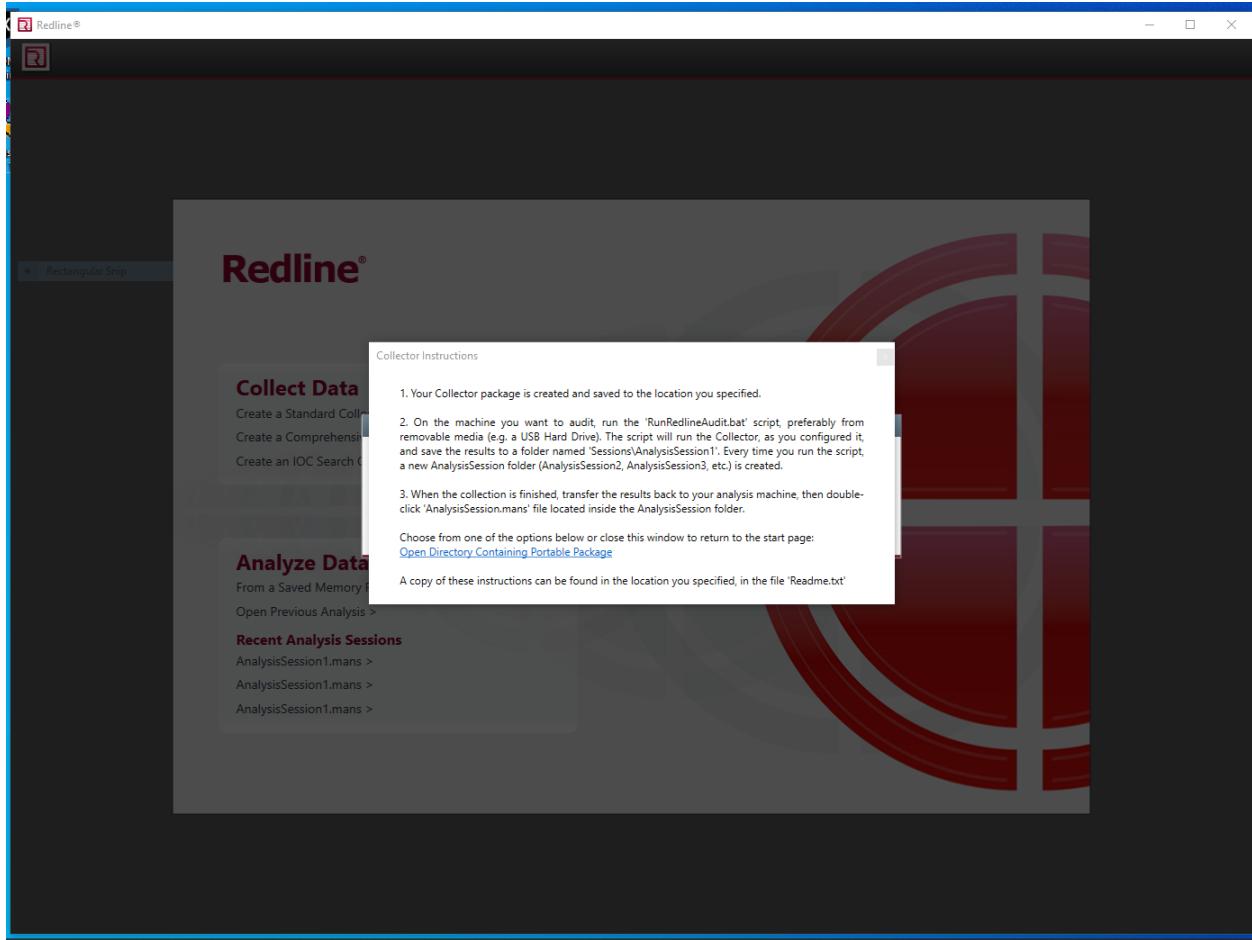




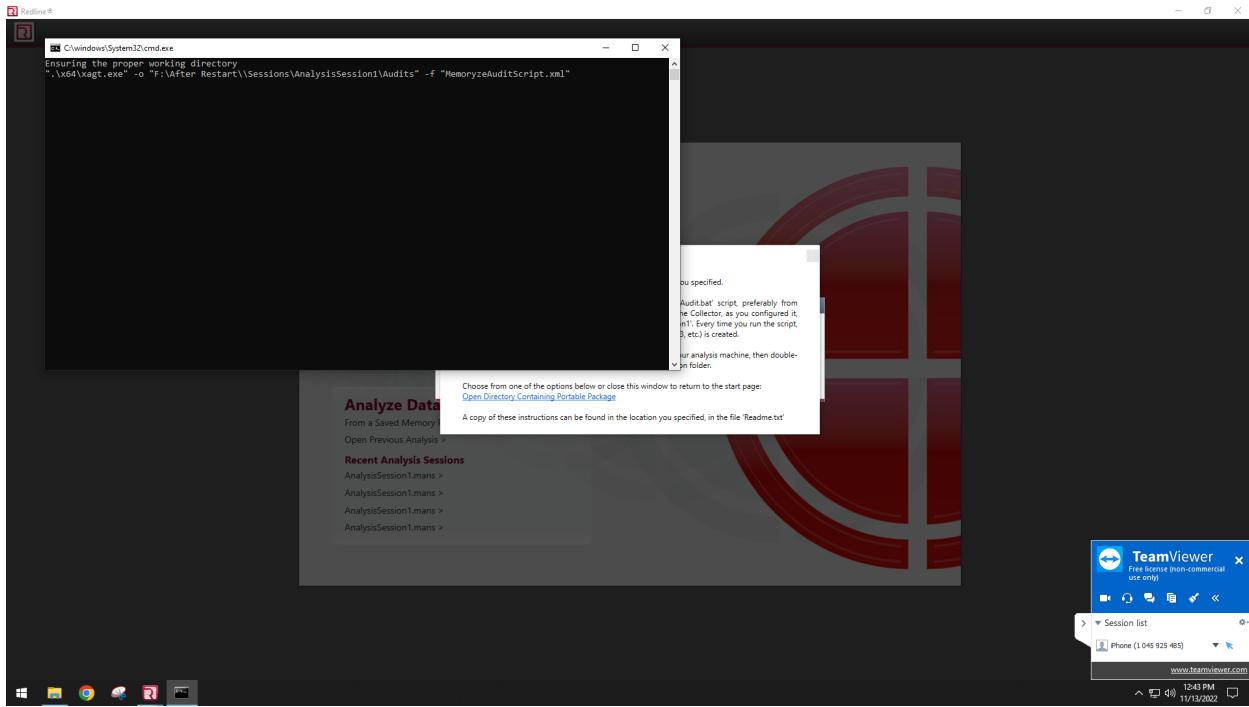
6. After you've finished changing the script, dismiss the box and navigate to the folder where you want to save the data. In this scenario, we saved the data to an external disk and separated it into two folders: Before and After Restart. This allows us to examine both files.
7. After selecting the folder,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



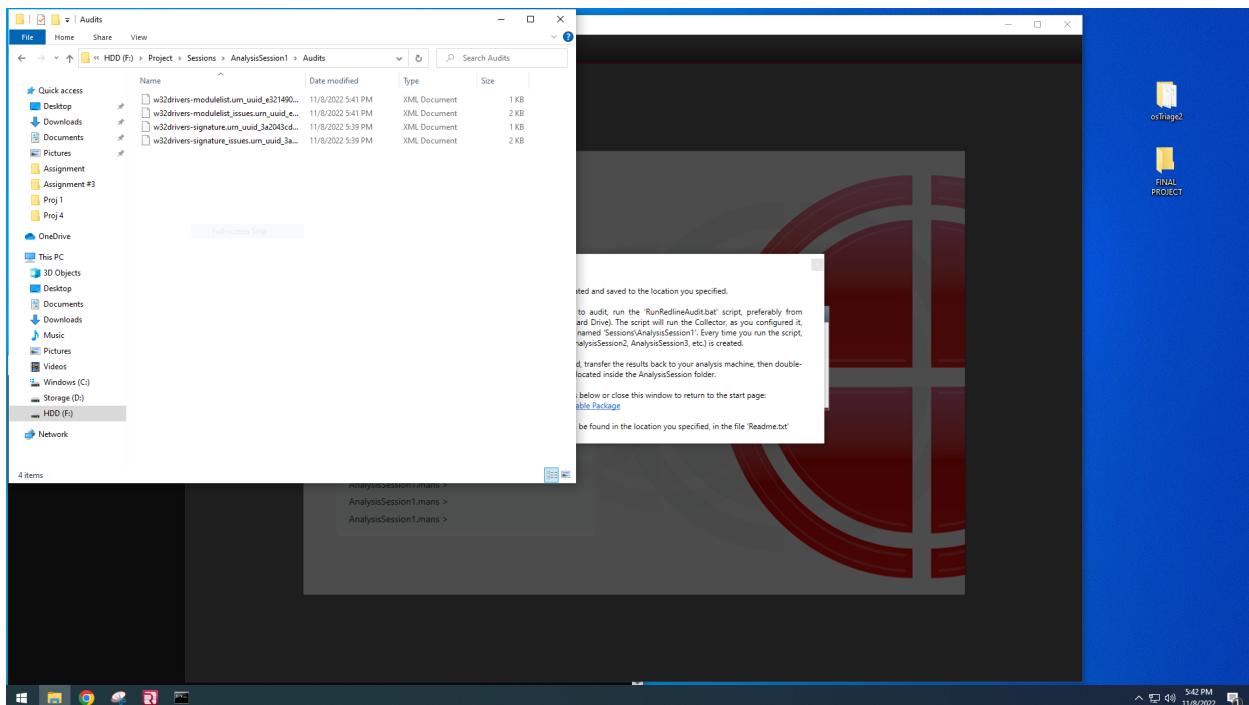
8. You will be prompted to execute the file from the folder. Navigate to folder



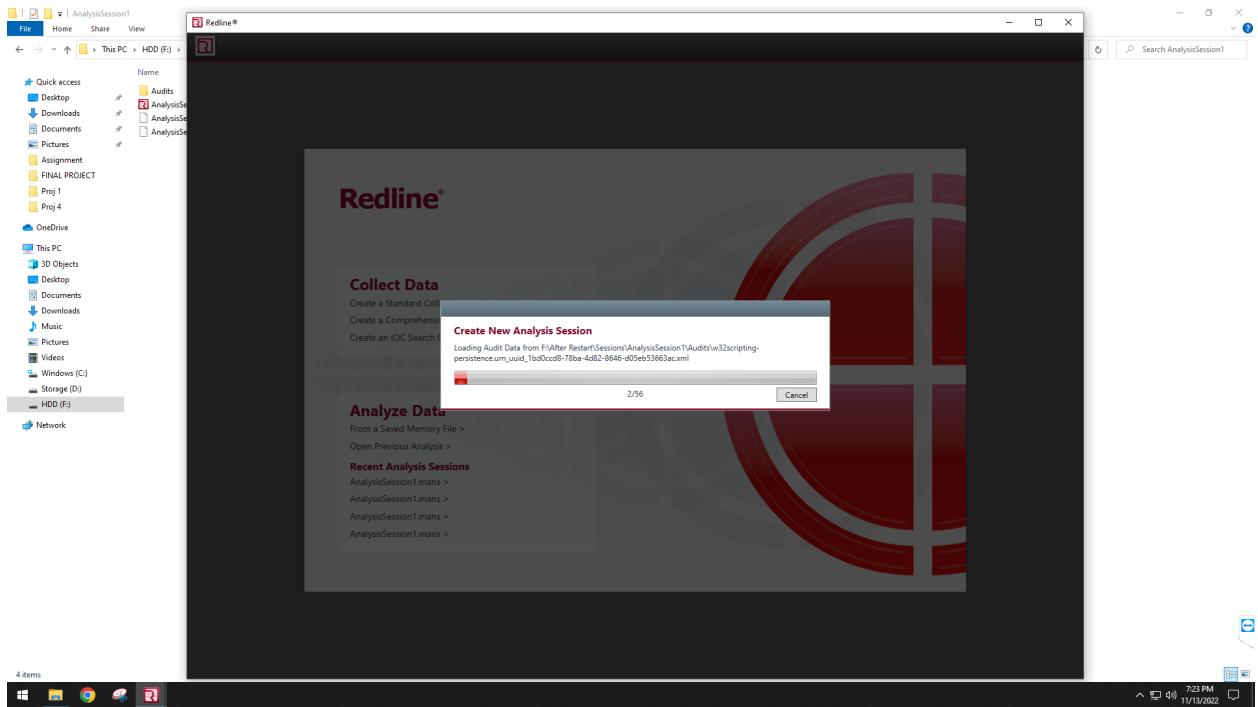
9. You will notice the command prompt performing a command; now, leave the lab alone till the CMD closes itself.



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:\ProjectSessions\AnalysisSession1\AnalysisSession1.mans

Analysis Data

Review Browser URL History

When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, 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 URLs 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 baffle a user from knowing exactly where they're reaching a malware hosting 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.

Visit Only

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 bookmarked bookmarked sites are an 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 frames often used by embedded ad sites which could be externally interacted with.

Enter string to find here...

Filters

In All Fields

Page Title

Hostname

Typed Visit From

URL

1,115 Items

10:22 AM 11/9/2022

Redline - F:\ProjectSessions\AnalysisSession1\AnalysisSession1.mans

Analysis Data

Cookie History

Cookies are a means for a website to leave data on a user's computer for later retrieval. They are most commonly used to track login and session data, and to tailor a user's visit to a website. You can use cookies as a resource for analyzing certain types of browser-based activity.

All Cookie Records

Shows all cookies.

Secure Cookies

Shows only cookies that must be sent over HTTPS, which is an uncommon restriction for cookies and may indicate suspicious activity.

Hidden Cookies

Shows only cookies that are hidden to the application.

Cookies-with-Flags

Shows only cookies that have attribute flags set (available only for Internet Explorer).

Enter string to find here...

Filters

In All Fields

File Name

File Path

Hostname

Cookie Name

Cookie Value

Cookie Path

google.com	AEC	AaknGhHtErY0453M0gPXR4fTc...	/
google.com	NID	511nXK0kounJigmuXgCS048j...	/
google.com	OGPC	19027681-1	/
google.com	1P_JAR	2022-04-27-21	/
ogs.google.com	OTZ	6479832_72_76_104100_72_446760	/
google.com	ANID	AHNqTUuJSGWVlQ-K9uO9P60e...	/
accounts.youtube.com	CheckConnectionTempC	922125	/accounts
accounts.google.com	_Host-GAPS	1:DkuTkIMRZNMP-yQKQoRdxg...	/

8 Items

10:24 AM 11/9/2022

Analysis Data																			
Analysis Data		Filters		Enter string to find here... <input type="text"/> <input type="button" value="Reg Ex"/>															
				Last Visit Date	Clear Column Filters	Prev	Next												
System Information	Process	File	Hierarchical Processes																
File System	Registry	Windows Service	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																			
Review Browser URL History																			
When you are investigating web history data, analysis should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden URLs which may include 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 typically occurs when a user from site to site before finally reaching a malware staging server.																			
Visit From																			
Shows all records generated after the user has 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 Recently																			
Shows only records that were visited from a bookmark or bookmarked sites are 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 frames often used by embedded ad sites which could be potentially infected with malicious obfuscated JavaScript.																			

CYBERLAB-11 CYBERLAB-11

Redline® - F:\After Restart\Session\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 include sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field 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 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.

Type 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.

Forms

Shows all records that involve a form.

Host IOC Reports Not Collected

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

Visit Type	URL	Hostname	Typed	Visit From	Visit Count	First Visit Date	Page Title	Last Visit Date	Last Visit I
URL	https://login.live.com/oauth20_desktop.srf?lc=1033				0	2022-11-13 17:35:57Z			
URL	https://login.live.com/oauth20_authorize.srf?client_id=...				0	2022-11-13 17:35:57Z			
URL	https://login.live.com/oauth20_logout.srf?client_id=0...				0	2022-11-13 17:35:57Z			
URL	file:///C:/Users/cybersecurity/Desktop/FINAL PROJE...				0	2022-11-13 17:40:53Z			
URL	file:///F:/After Restart				0	2022-11-13 17:42:38Z			
URL	file:///C:/Users/cybersecurity/Desktop/FINAL PROJE...				0	2022-11-13 17:44:03Z			
URL	file:///C:/Users/cybersecurity/Desktop/FINAL PROJE...				0	2022-11-13 17:40:06Z			
Generated	https://www.google.com/search?q=forensic+tools&rl...				2	2022-11-13 17:37:21Z	forensic tools - Google S...	2022-11-13 17:37:22Z	
Link	https://www.google.com/search?q=forensic+tools&rl...				2	2022-11-13 17:37:22Z	forensic tools - Google S...	2022-11-13 17:37:22Z	
Link	https://www.guru99.com/computer-forensics-tools.ht...			https://www.google.com/search?q=forensic+tools&rl...	1	2022-11-13 17:37:34Z	15 BEST Computer (Digit...	2022-11-13 17:37:50Z	
Manual S...	https://ia004.e-planning.net/umidc>3ab023ac29e...				1	2022-11-13 17:37:50Z			
Manual S...	https://badrnx.com/prebid/setuid/bidder/vidomy...				2	2022-11-13 17:38:00Z			
Manual S...	https://badrnx.com/prebid/setuid/bidder/vidomy...				2	2022-11-13 17:38:17Z			
Generated	https://www.google.com/search?q=redline+tool&rl...				2	2022-11-13 17:39:04Z	redline tool - Google Se...	2022-11-13 17:39:05Z	
Link	https://www.google.com/search?q=redline+tool&rl...				2	2022-11-13 17:39:05Z	redline tool - Google Se...	2022-11-13 17:39:05Z	
Link	https://www.redlinetools.com/				1	2022-11-13 17:39:07Z	CNC & VMC Machine Cu...	2022-11-13 17:39:07Z	

Show Details 16 Items 10:44 AM 11/15/2022

CYBERLAB-11 CYBERLAB-11

Redline® - F:\After Restart\Session\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 include sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field 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 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.

Type 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.

Forms

Shows all records that involve a form.

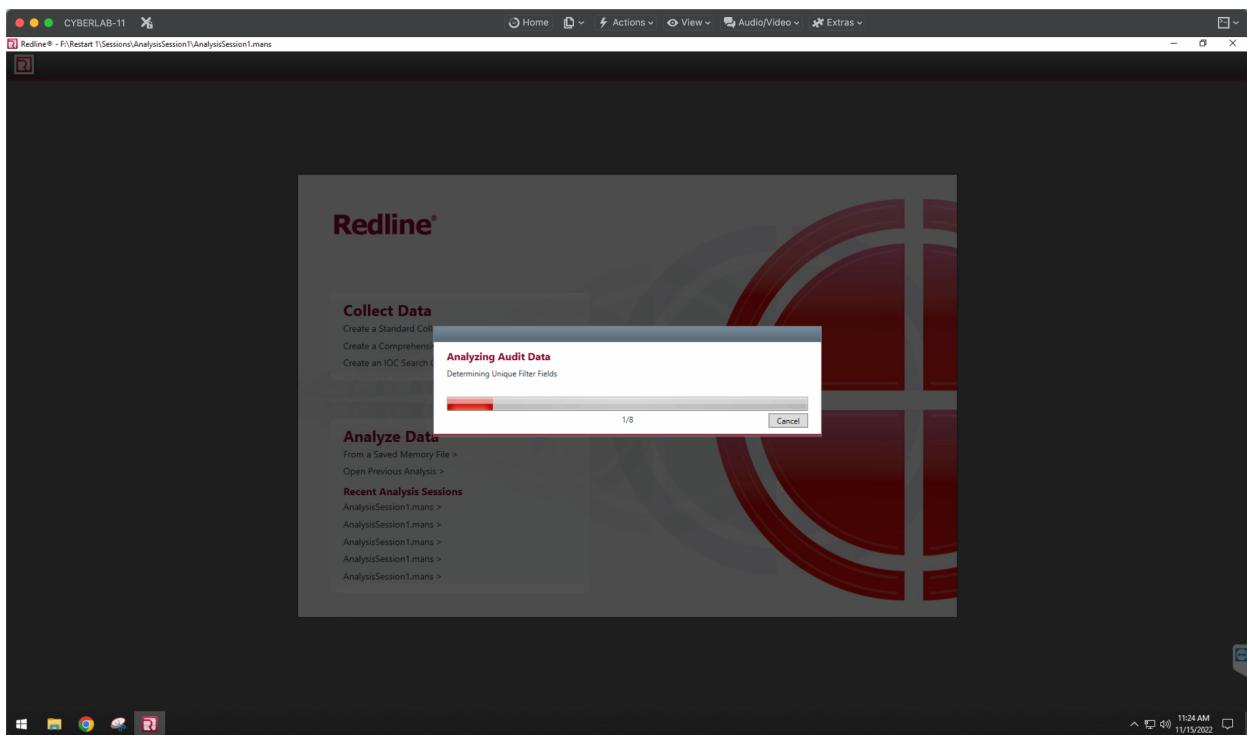
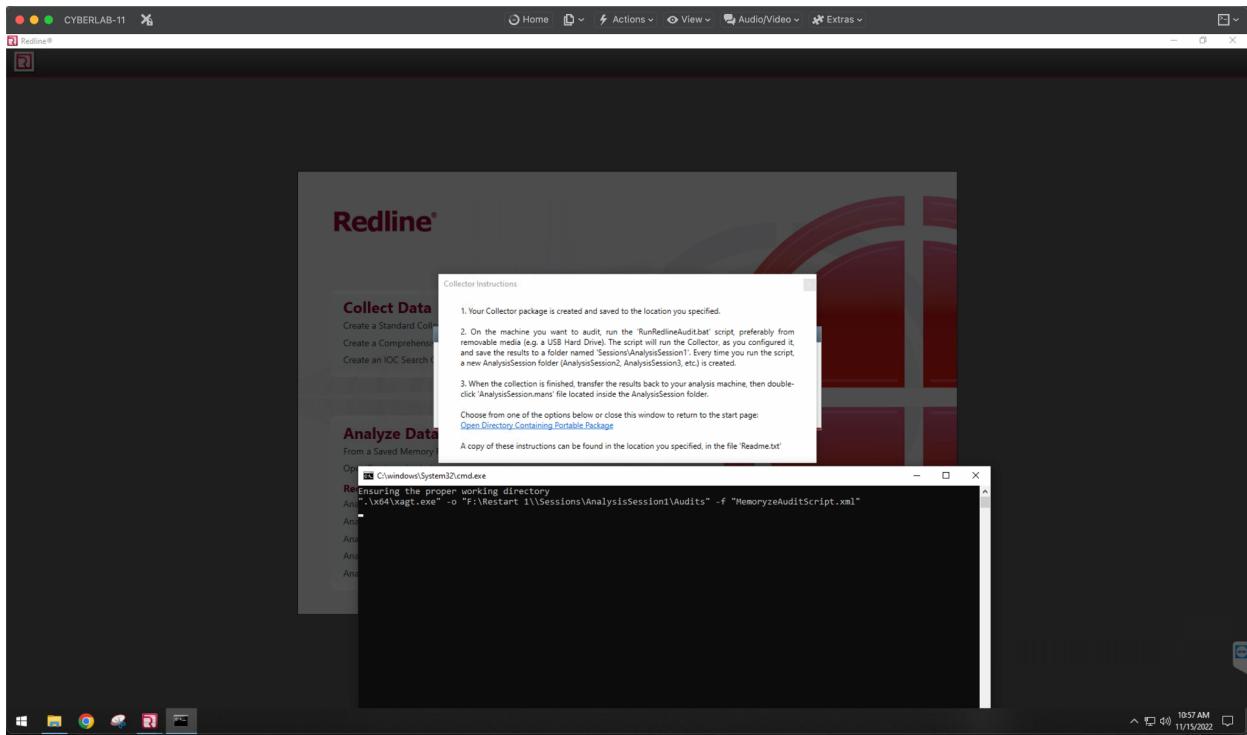
Host IOC Reports Not Collected

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

Visit Type	URL	Hostname	Typed	Visit From	Visit Count	First Visit Date	Page Title	Last Visit Date	Last Visit I
Link	https://www.guru99.com/computer-forensics-tools.ht...			https://www.google.com/search?q=forensic+tools&rl...	1	2022-11-13 17:37:34Z	15 BEST Computer (Digit...	2022-11-13 17:37:34Z	
Link	https://www.redlinetools.com/			https://www.google.com/search?q=redline+tool&rl...	1	2022-11-13 17:39:07Z	CNC & VMC Machine Cu...	2022-11-13 17:39:07Z	

2 Items 10:45 AM 11/15/2022

AFTER RESTART



CONCLUSION

The screenshot shows the Redline tool's interface with the title bar "CYBERLAB-11" and the path "Redline 4 - F:\Restart\1\Sessions\AnalysisSession1\AnalysisSession1.mans". The main window is titled "Analysis Data" and displays "Browser URL History". On the left, a sidebar lists "Processes", "Hierarchical Processes", "Browser URL History", "Cookie History", "Form History", "Timeline", "Tags and Comments", and "Acquisition History". A detailed description of "Browser URL History" is provided, mentioning redirects, malware servers, and malicious sites. Below this are several filtering options: "All URL Records" (selected), "Redirects", "Visit From", "Visited Once", "Visited Bookmarked URLs", "Visited URLs", "Hidden Visits", and "Forms". The main pane shows a table with columns: Visit Type, URL, Hostname, Typed, Visit From, Visit Count, First Visit Date, Page Title, Last Visit Date, and Last Visit. A search bar at the top allows filtering by "Enter string to find here". Navigation buttons "Prev" and "Next" are also present.

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.