

# **MAGNET VIRTUAL SUMMIT 2023**

## **CAPTURE THE FLAG (CTF)**

### **WINDOWS 11**

About This CTF Challenge .....	2
CTF Questions Only .....	3
<b>PREPARING THE CASE IN FORENSIC EXPLORER .....</b>	<b>5</b>
Question 1 - Gmail? Outlook? Yeah, right.. (5 points) .....	10
Question 2 - Two different versions, twice the emulation power! Makes sense to me! .....	11
Question 3 - LITEning fast write speeds! (5 points) .....	13
Question 4 - Really...? Plaintext...? (10 points) .....	15
Question 5 - Why was 6 afraid of 7? Because 7 can unarchive virtual drives! (10 points).....	17
Question 6 - We're not in Kansas anymore... (25 points) .....	18
Question 7 - Make sure to keep some tabs on that SysAdmin from Southern California (25 points) .	20
Question 8 - We have a History of attracting some sizeable donors with our projects (25 points)....	21
Question 9 - Scratch that Itch.io (25 points) .....	22
Question 10 - The breakfast bell is ringing (50 points) .....	23
Question 11 - Oh Deer...I think we're lost (50 points) .....	24
Question 12 - Gotta Git going fast with some Accelerated emulation! (50 points) .....	25
Question 13 - PCA - Program Clang Assistant? (100 points).....	27

## ABOUT THIS CTF CHALLENGE

This challenge was created by Magnet Forensics as part of their 2023 Virtual Summit.

Information about the next summit is available at:

- <https://magnetvirtualsummit.com/>
- <https://magnetvirtualsummit.com/capture-the-flag/>

## FORENSIC IMAGE SOURCE

Download: [PC-MUS-001.E01](#) (49.0 GB)

## OTHER ONLINE SOLUTIONS

The following solutions can be found on the web:

- [https://forensafe.com/blogs/challenges/mvs\\_windows11\\_ctf.html](https://forensafe.com/blogs/challenges/mvs_windows11_ctf.html)
- <https://www.stark4n6.com/2023/03/magnet-virtual-summit-2023-ctf-windows.html>
- <https://www.forgottennook.com/blog/magnet-windows11-2023>

## CTF QUESTIONS ONLY

The following questions were provided:

1	Gmail? Outlook? Yeah, right..  <b><i>What non-standard email service has the user used previously?</i></b>	5
2	Two different versions, twice the emulation power! Makes sense to me!  <b><i>The user installed and ran a mobile device emulation program on their system. Which 2 versions of this software did the user install? (Format: SoftwareName V1/V2)?</i></b>	5
3	LITEning fast write speeds!  <b><i>The user's system is equipped with a 256GB NVMe SSD. What is the make and model of this drive?</i></b>	5
4	Really...? Plaintext...?  <b><i>The user frequently accesses a Chrome Remote Desktop virtual machine. What password is used to log into this VM?</i></b>	10
5	Why was 6 afraid of 7? Because 7 can unarchive virtual drives!  <b><i>Within the past 2 years, a popular unarchiving program gained the ability to unarchive VHDX virtual disk images. What version of the program was this upgrade implemented?</i></b>	10
6	We're not in Kansas anymore...  <b><i>The user has established an RDP connection to one destination more than any other. What is the Geolocation of this destination? (Format: City, ST)?</i></b>	25

7	Make sure to keep some tabs on that SysAdmin from Southern California  <i>The user visited the Mastodon page of one user more than any others on the platform. What is the full legal name of the user Michael visited?</i>	25
8	We have a History of attracting some sizeable donors with our projects  <i>Michael used PowerShell to clone a particular GitHub utility. What is the account name of one of this repo's most prominent sponsors?</i>	25
9	Scratch that Itch.io  <i>The user viewed a YouTube video by the creator BenBonk surrounding video game developers. Within this video, how many developers were involved with the project?</i>	25
10	The breakfast bell is ringing  <i>The user has been doing some research lately on fast food items. What is, according to some experts, the unhealthiest food item of the bunch?</i>	50
11	Oh Deer...I think we're lost  <i>Michael lives just a mile south of a beautiful body of water. What is the name of this body of water?</i>	50
12	Gotta Git going fast with some Accelerated emulation!  <i>In order to emulate an Android device, the user required some specialized management tools. What Android port is used by default with these services?</i>	50
13	PCA Program Clang Assistant?  <i>The user has installed Android Studio with a specialized plugin dedicating to diagnosing and fixing some programming errors. When this plugin runs, what exit code is used upon completion?</i>	100

## PREPARING THE CASE IN FORENSIC EXPLORER

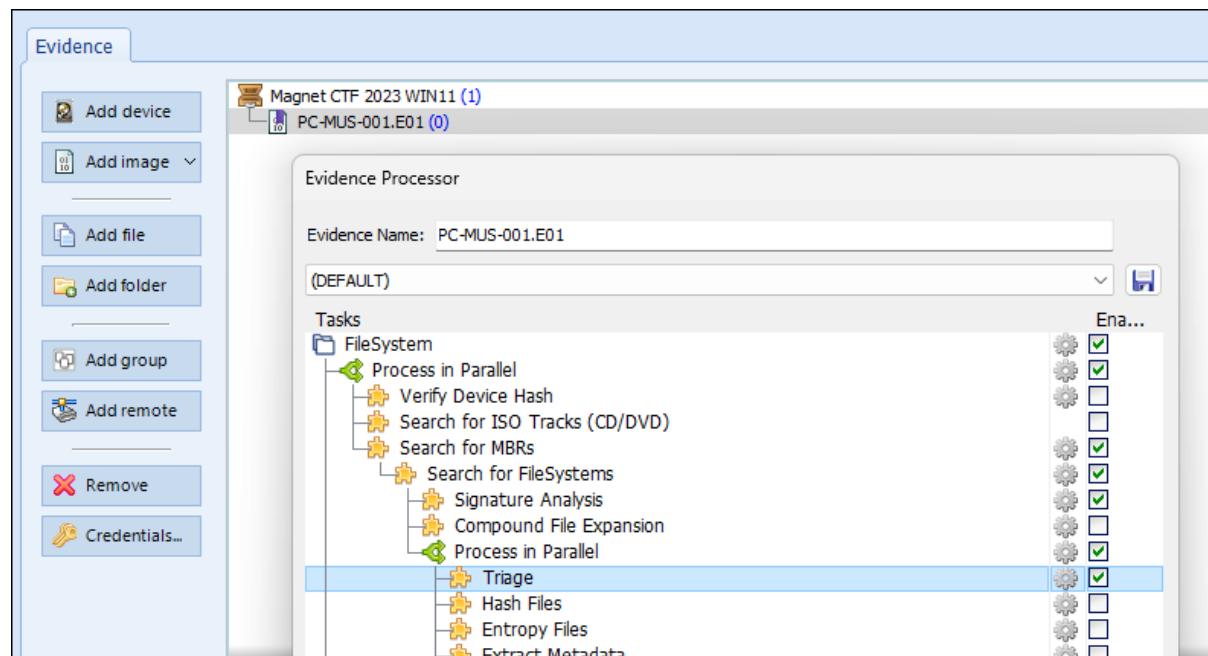
The following initial Forensic Explorer processing steps are recommended. These steps should take no longer than 15 minutes to complete.

### ADD EVIDENCE: PC-MUS-001.E01

In the Forensic Explorer **Evidence** module:

1. Select the **New Case**.
2. Enter **investigator details** (if required) and a **case name**.
3. Click **Add Image**.
4. Add the evidence file **PC-MUS-001.E01**.
5. In the **Evidence Processor** window, add **Triage** to processing options. [Optional].

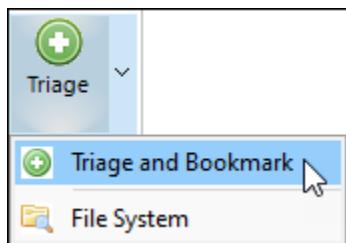
Figure 1: New Case > Add Image > Evidence Processor



## TRIAGE

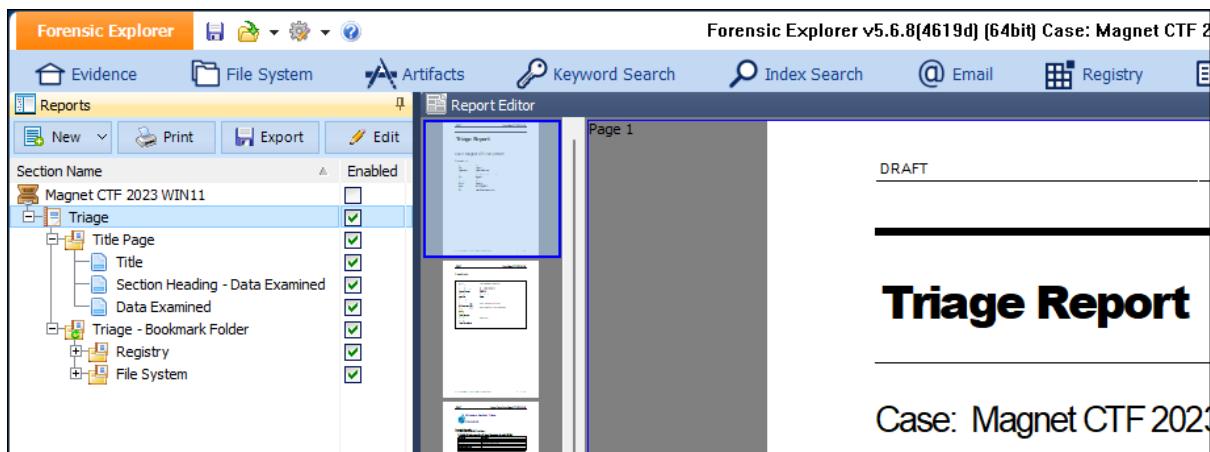
In Forensic Explorer, Triage is a fast process that extract and bookmark common artifacts and display this information in the **Reports** module as a **Triage Report**. If Triage was not run from the **Evidence Processor** it can be run at a later time from the **File System module > Triage button**.

Figure 2: Launch Triage from File System module



The Triage Report can often contain answers to CTF questions.

Figure 3: Triage Module > Triage Report

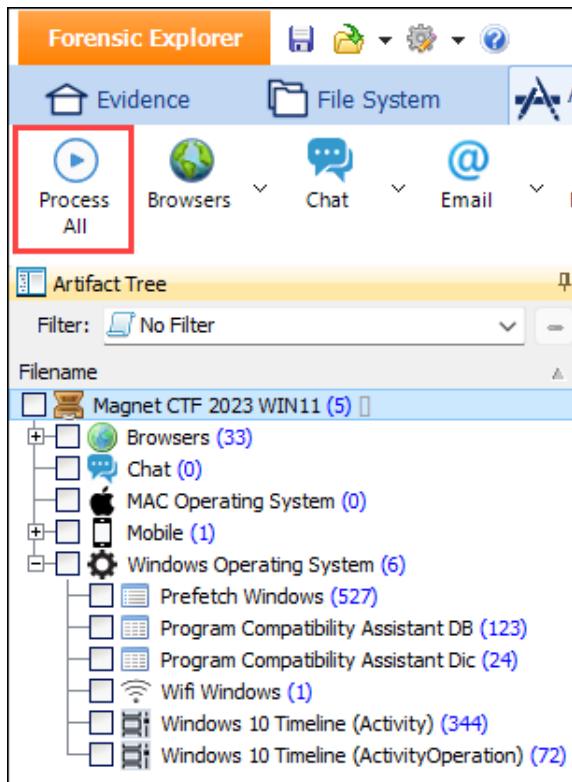


## ARTIFACTS > PROCESS ALL

The Forensic Explorer **Artifacts** module extracts common forensic artifacts from files, including SQLite, Plist, and XML. To populate artifacts:

1. Click the **Artifacts module > Process All** button.

Figure 4: Artifacts > Process All

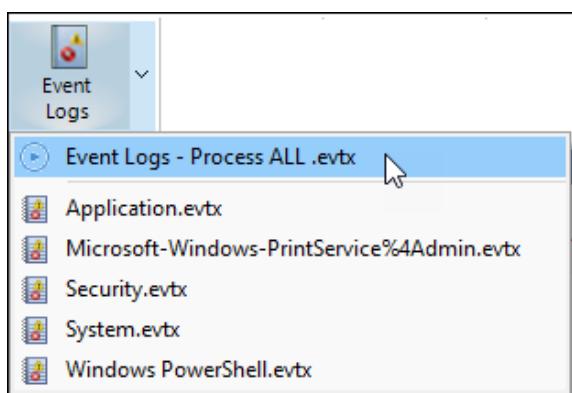


## ARTIFACTS > EVENT LOGS

It is evident that Question 6 will require analysis of Windows Event Logs (.evtx). To populate Event Logs in the Artifacts module:

1. Click the **Artifacts module > Event Logs – Process All .evtx** button.

Figure 5: Windows Event Logs



## REGISTRY

In the File System module:

1. Apply the Folder Filter: **Registry (All) - SAM, SECURITY, SOFTWARE, SYSTEM, NTUSER.DAT, USERCLASS.DAT**.
2. In the **File List**, click **Ctrl A** to highlight all of the filtered registry files.
3. Right-click and **Send to module > Registry**.

Figure 6: Send registry files to the Registry module

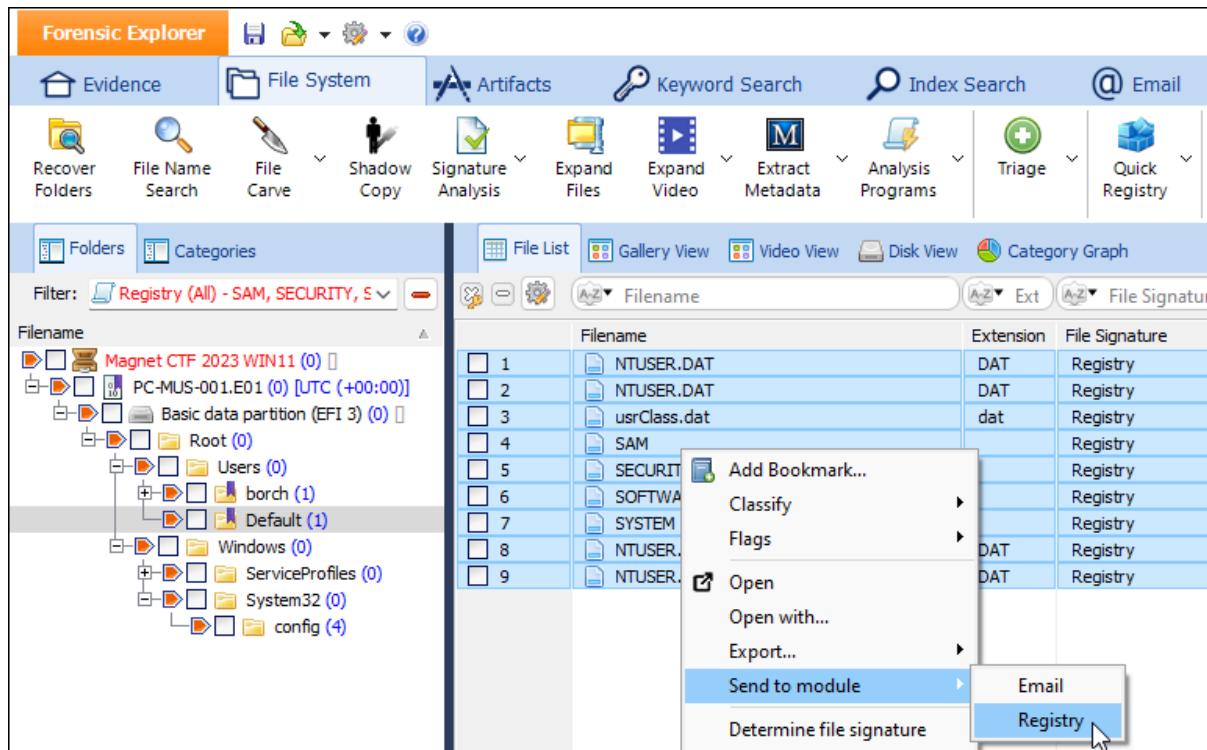
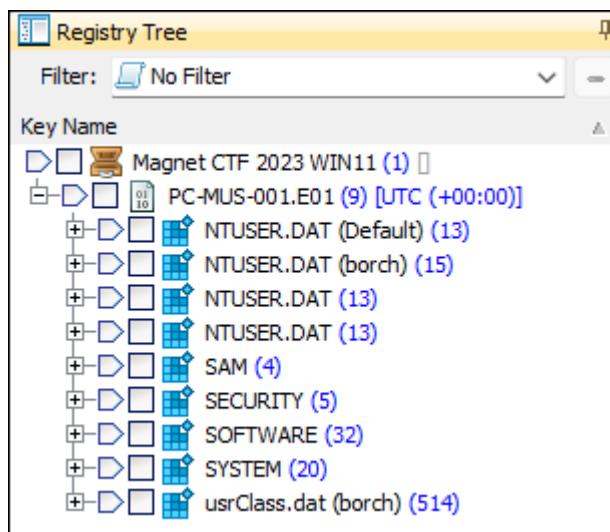


Figure 7: Registry module > Populated Registry Tree



## LIVE BOOT

Forensic Explorer Live Boot enables an investigator to virtualize a forensic evidence file and operate the target computer in a virtual environment. Live Boot uses a combination of Forensic Explorer, Mount Image Pro (provided with a Forensic Explorer license) and virtualization software (VirtualBox, or VMWare). Live Boot can provide insights into user activity that may not readily identifiable using standard forensic software methods.

Note that the target system uses a **UEFI** boot process. See the Forensic Explorer manual for setup instructions and information to bypass the Win11 user password using **PCUnlocker**.

Figure 8: PC-MUS-001.E01 login screen

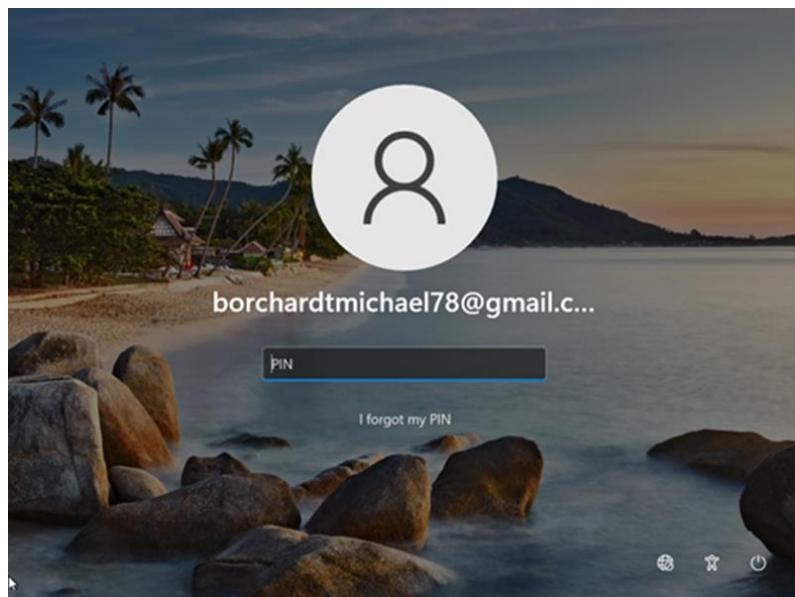
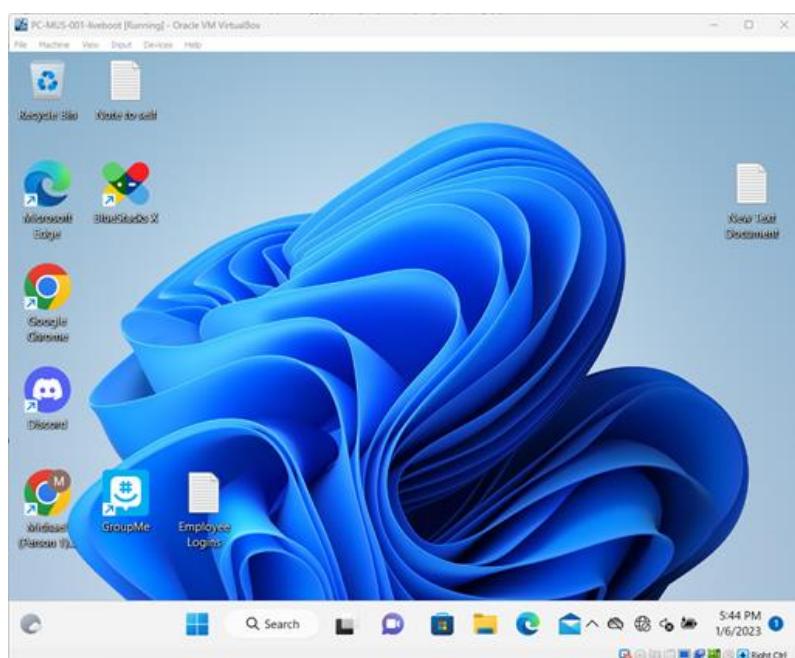


Figure 9: PC-MUS-001.E01 virtualized desktop



## QUESTION 1 - GMAIL? OUTLOOK? YEAH, RIGHT.. (5 POINTS)

**What non-standard email service has the user used previously?**

### Q1. ANSWER

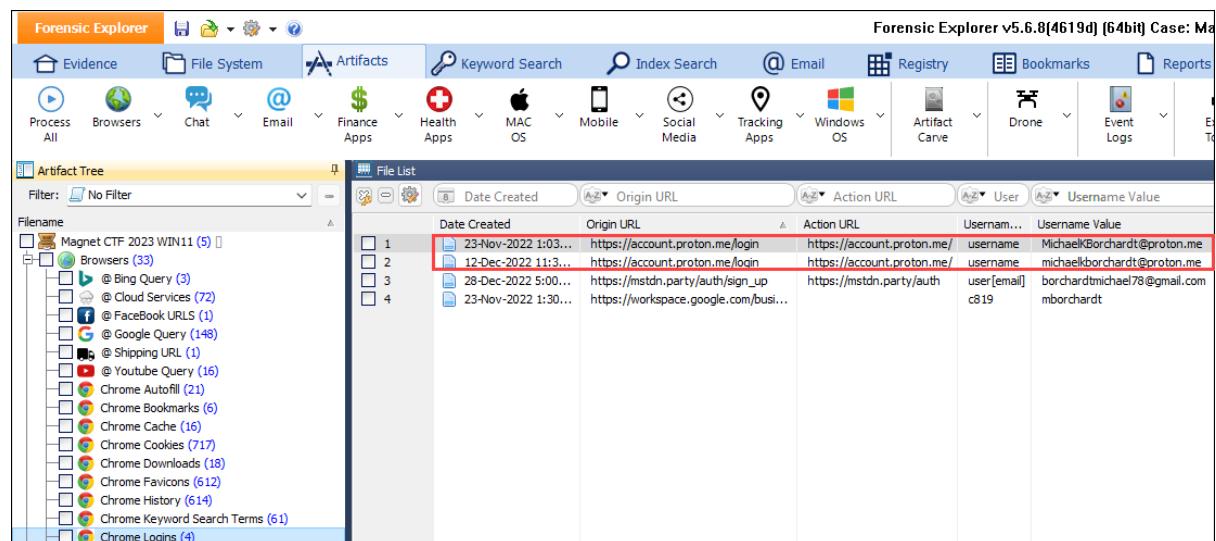
Proton.

### Q1. FORENSIC EXPLORER METHODOLOGY

This question suggests that a lesser known email program is in use. Artifacts web history is a useful place to start to check for web-based activity.

Chrome Logins identifies that the user has visited the login screen for Proton mail, <https://account.proton.me/login>.

Figure 10: Artifacts > Browsers > Chrome Logins



The screenshot shows the Forensic Explorer interface with the 'Artifacts' tab selected. The 'File List' pane displays a table of Chrome Logins artifacts. The table has columns for Date Created, Origin URL, Action URL, Username, and Username Value. The first two rows are highlighted with red boxes. The first row shows a Date Created of 23-Nov-2022 1:03, an Origin URL of https://account.proton.me/login, an Action URL of https://account.proton.me/, and a Username of MichaelkBorchardt@proton.me. The second row shows a Date Created of 12-Dec-2022 11:3, an Origin URL of https://account.proton.me/login, an Action URL of https://account.proton.me/, and a Username of michaelkBorchardt@proton.me. The 'Artifact Tree' pane on the left shows a tree structure with 'Browsers' expanded, showing sub-items like 'Bing Query', 'Cloud Services', 'Facebook URLs', 'Google Query', 'Shipping URL', 'Youtube Query', 'Chrome Autofill', 'Bookmarks', 'Cache', 'Cookies', 'Downloads', 'Favicons', 'History', 'Keyword Search Terms', and 'Logins' (4).

Date Created	Origin URL	Action URL	Username	Username Value
23-Nov-2022 1:03...	https://account.proton.me/login	https://account.proton.me/	username	MichaelkBorchardt@proton.me
12-Dec-2022 11:3...	https://account.proton.me/login	https://account.proton.me/	username	michaelkBorchardt@proton.me
28-Dec-2022 5:00...	https://mstdn.party/auth/sign_up	https://mstdn.party/auth	user [email]	borchardtmichael78@gmail.com
23-Nov-2022 1:30...	https://workspace.google.com/busi...		c819	mborchardt

## QUESTION 2 - TWO DIFFERENT VERSIONS, TWICE THE EMULATION POWER! MAKES SENSE TO ME!

***The user installed and ran a mobile device emulation program on their system. Which 2 versions of this software did the user install? (Format: SoftwareName V1/V2)?***

### Q2. ANSWER

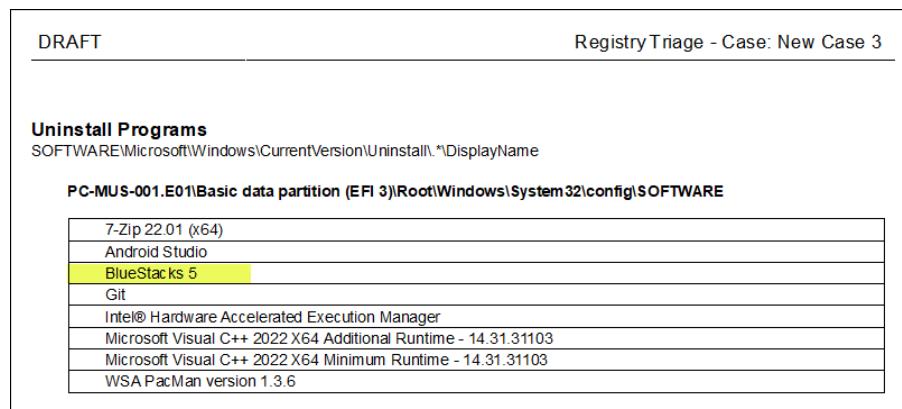
BlueStacks 5 - 5.10.10.1014

BlueStacks X - 0.19.21.1002

## Q. FORENSIC EXPLORER METHODOLOGY

Information about installed applications is contained in the Forensic Explorer Triage report. This identifies from registry information the mobile device emulation program called **BlueStacks 5**.

Figure 11: Reports > Triage Report



DRAFT Registry Triage - Case: New Case 3

**Uninstall Programs**  
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\.\*DisplayName

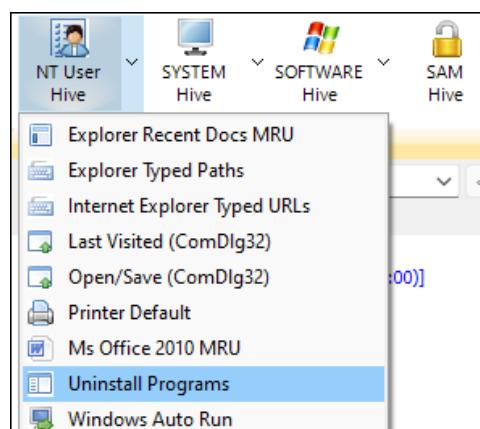
PC-MUS-001.E01\Basic data partition (EFI 3)\Root\Windows\System32\config\SOFTWARE

7-Zip 22.01 (x64)
Android Studio
BlueStacks 5
Git
Intel® Hardware Accelerated Execution Manager
Microsoft Visual C++ 2022 X64 Additional Runtime - 14.31.31103
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.31.31103
WSA PacMan version 1.3.6

Switching to the Forensic Explorer Registry module, there are two places where information about installed applications can be extracted.

1. NT User Hive > Uninstall Programs
2. Software Hive > Uninstall Programs (metadata)

Figure 12: Registry > NTUser Hive > Uninstall Programs



NT User Hive SYSTEM Hive SOFTWARE Hive SAM Hive

- Explorer Recent Docs MRU
- Explorer Typed Paths
- Internet Explorer Typed URLs
- Last Visited (ComDlg32)
- Open/Save (ComDlg32)
- Printer Default
- Ms Office 2010 MRU
- Uninstall Programs
- Windows Auto Run

Figure 13: Output from Registry > NT User Hive > Uninstall Programs

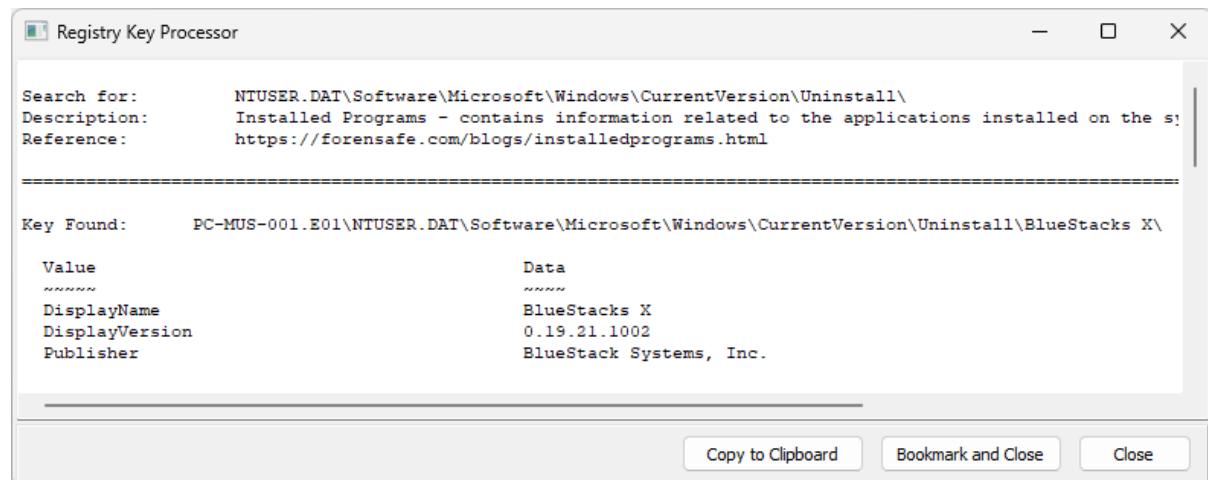
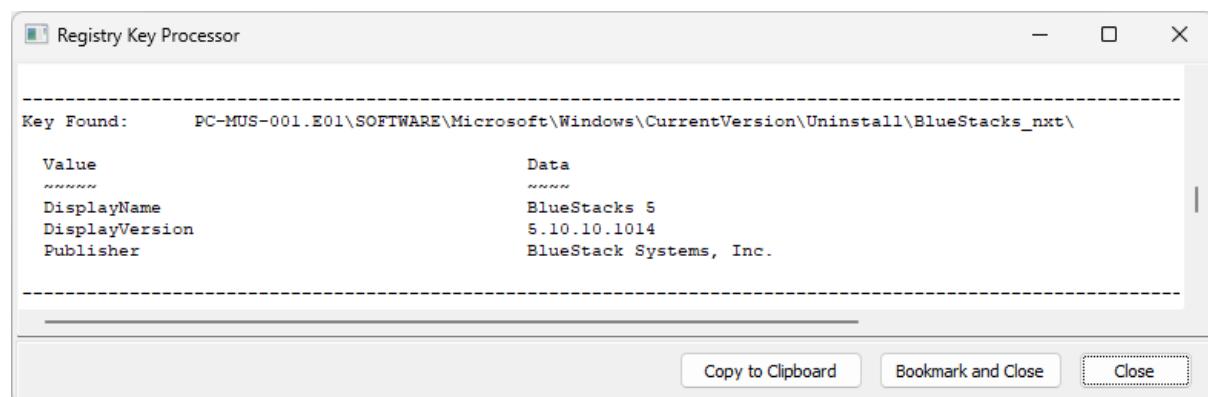


Figure 14: Output from Registry > SOFTWARE Hive > Uninstall Programs (metadata)



Once registry key names have been identified, it is possible to branch plate the entire Registry module and then use filtering techniques to read individual keys and their contents.

Figure 15: Registry > DisplayName > BlueStacks 5

	Key Name	Key Type	Key Data	Key Path
1	DisplayIcon	REG_SZ	C:\Program Files\Blu...	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\BlueStacks_nxt\
2	DisplayName	REG_SZ	BlueStacks 5	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\BlueStacks_nxt\
3	DisplayVersion	REG_SZ	5.10.10.1014	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\BlueStacks_nxt\
4	EstimatedSize	REG_DWORD	0x001FFC00 (20961...)	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\BlueStacks_nxt\
5	InstallDate	REG_SZ	20230104	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\BlueStacks_nxt\
6	NoModify	REG_DWORD	0x00000001 (1)	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\BlueStacks_nxt\
7	NoRepair	REG_DWORD	0x00000001 (1)	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\BlueStacks_nxt\
8	Publisher	REG_SZ	BlueStack Systems, I...	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\BlueStacks_nxt\
9	UninstallString	REG_SZ	C:\Program Files\Blu...	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\BlueStacks_nxt\
10	~SecDesc	REG_UNKNOWN	(unknown)	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\BlueStacks_nxt\

### QUESTION 3 - LITENING FAST WRITE SPEEDS! (5 POINTS)

**The user's system is equipped with a 256GB NVMe SSD. What is the make and model of this drive?**

#### Q3. ANSWER

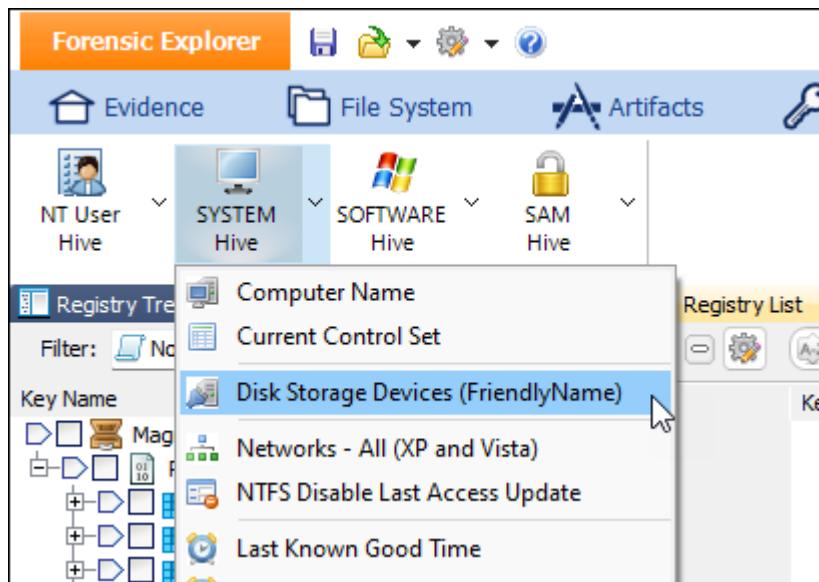
LITEON CA1-8D256-HP

#### Q3. FORENSIC EXPLORER METHODOLOGY

Disk storage information is held in the Windows registry, SYSTEM hive. For fast access select:

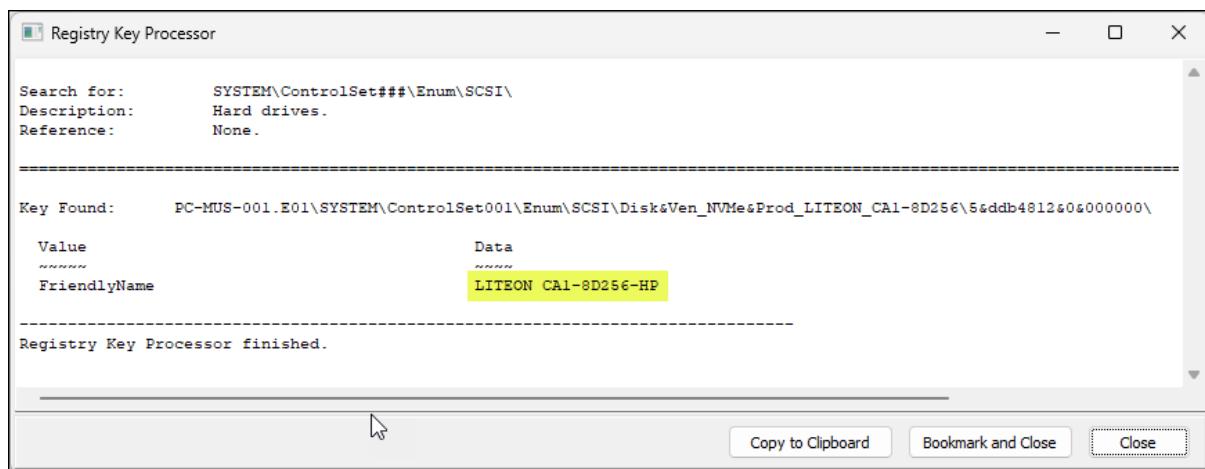
1. SYSTEM HIVE > Disk Storage Devices (Friendly Name).

Figure 16: Registry Module > System Hive > Disk Storage Devices (FriendlyName)



With the following output:

Figure 17: Registry Module > System Hive > Disk Storage Devices (FriendlyName) > Output



An alternative method is to:

1. In the Registry module, branch plate the entire case so that all registry items are shown in the Registry List.
2. Use **nvme** (or other keywords) in the **Key Name** column filter.

Figure 18: Registry Module > Column Filter

The screenshot shows the Magnet Forensic Explorer interface with the 'Registry List' module open. The 'Key Name' column is filtered to show only entries containing 'nvme'. The list includes registry keys such as 'Microsoft-Windows-Storage-NvmeDisk/Operational', 'NVMeDisablePerfThrottling', and 'SCSI\Disk\Ven\_NVMe&Prod\_LITEON\_CA1-8D256\5&ddb481280&000'. The 'Registry Tree' pane on the left shows the hierarchical structure of the registry, with the 'nvme' key visible under the 'DeviceContainerPropertyUpd' key.

Once the parent folder for the relevant registry key has been identified, it can be isolated with the Branch Plate and individual keys examined.

Figure 19: Registry Module > Branch Plate of SCSI folder

The screenshot shows the Magnet Forensic Explorer interface with the 'Registry List' module open. A specific SCSI folder, 'SCSI\Disk\Ven\_NVMe&Prod\_LITEON\_CA1-8D256\5&ddb481280&000000', is selected in the 'Registry Tree' pane. The 'Key Name' column in the list shows various registry keys for this SCSI device, such as 'FriendlyName' (LITEON CA1-8D256-HP), 'HardwareID' (SCSI\DiskNVMe\_), and 'PartitionTableCache' (01 00 00 00 04 00 00 00 04 98 1E 07 CC). The 'Key Data' column provides detailed information for each key.

Key Name	Key Data
ClassGuid	{53380000-0000-1000-8000-000000000000}
8	SCSI\Disk SCSI\RAW Disk1667
9	0x00000000 (0)
10	{00000000-0000-0000-ffff-ffffffffffff}
11	@disk.inf,%disk_devdesc%;Disk drive
12	{4d36e967-e325-11ce-bfc1-08002be103}
13	LITEON CA1-8D256-HP
14	SCSI\DiskNVMe_
15	Bus Number 0, Target Id 0, LUN 0
16	@disk.inf,%genmanufacturer%;(Standard disk
17	Service
18	~SecDesc (unknown)
19	Partmgr (unknown)
20	Storport (unknown)
21	~SecDesc (unknown)
22	Attributes 0x00000000 (0)
23	DiskId {23d20ec5-61db-11ed-8c41-806e6f6e69}
24	PartitionTableCache 01 00 00 00 04 00 00 00 04 98 1E 07 CC

## QUESTION 4 - REALLY...? PLAINTEXT...? (10 POINTS)

**The user frequently accesses a Chrome Remote Desktop virtual machine. What password is used to log into this VM?**

### Q4. ANSWER

,a]JEU0yG^+]2O]

### Q4. FORENSIC EXPLORER METHODOLOGY

Passwords are sometimes kept by users in non-secure formats like .txt files.

Most recently used documents is a fast way to establish recent activities of the user. **RecentDocs** information in the Report module > Triage Report lists one such file called **Employee Logins.txt**.

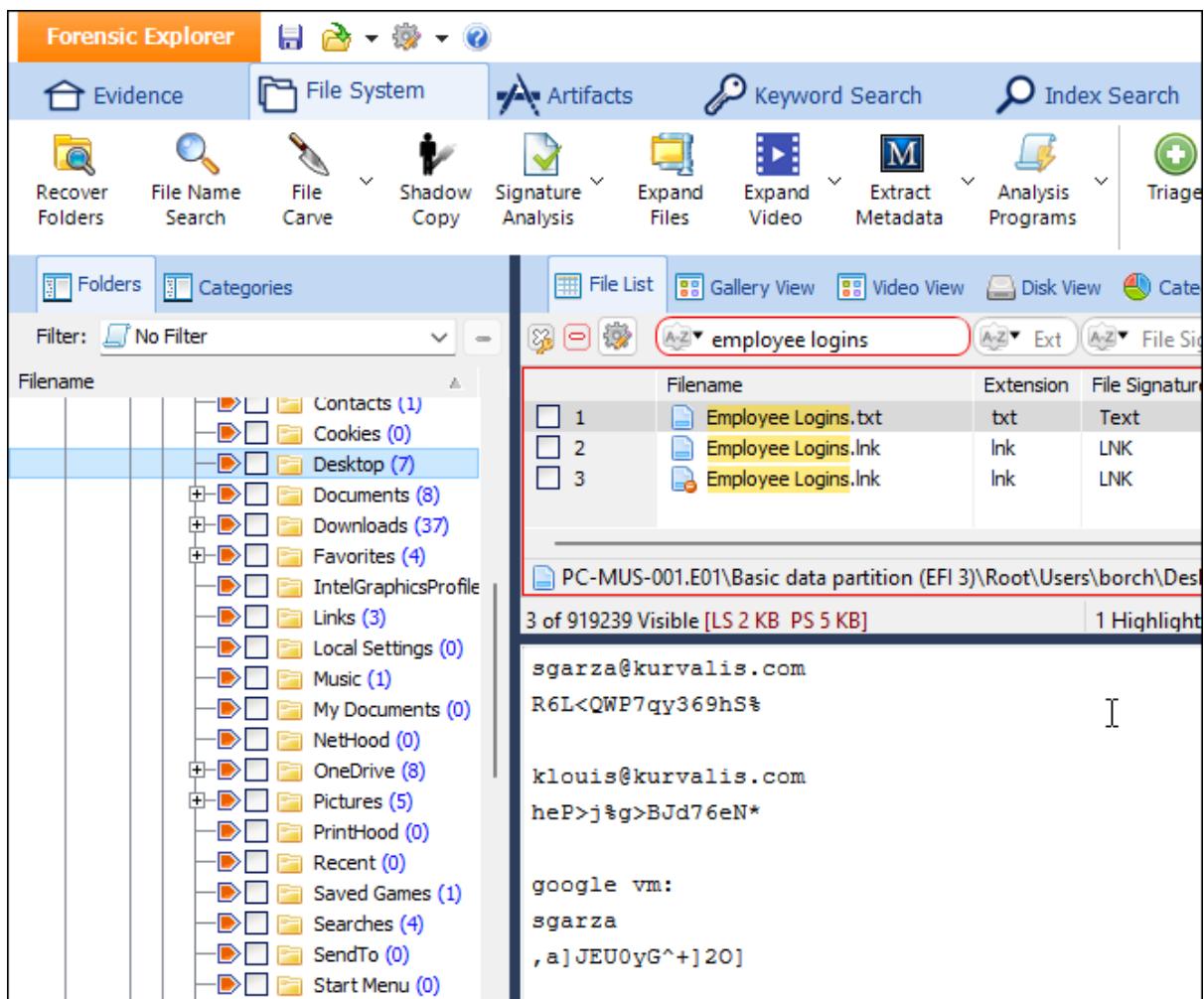
Figure 20: Reports > Triage Report > RecentDocs

DRAFT	Registry Triage - Case: Magnet CTF 2023 WIN11
<b>RecentDocs</b>	
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\	
PC-MUS-001.E01\Basic data partition (EFI 3)\Root\Users\borch\NTUSER.DAT	
<pre>?action_view=amzn://apps/android? asin=9NJHK44TTKSX&amp;launchsource=microsoftstore&amp;discoverysource=other account-recovery-sms-pin.gif Accusation.txt Customer Information.txt Customer Information.txt D: Downloads Employee Logins.txt Gmail_2022.11.13.490644112.Release_Apkpure.apk Google Chat_2022.11.13.493395953.Release_Apkpure.apk Google Drive_2.22.497.2.all.alldpi_Apkpure.xapk GroupMe_5.80.12_Apkpure.apk idea.log kgl\check/ log ms-gamingoverlay:///br/&gt;New Text Document.txt New Volume (D:) Note to self.txt spotlight?q=cape+peninsula+africa&amp;spotlightId=CapePeninsulaSouthAfrica&amp;FORM=EMSDS0 The Internet</pre>	

To locate this file in the Forensic Explorer File System module:

1. Branch Plate the entire case.
2. Use the **Filename** column filter tool to filter for **employee logins.\**
3. Use the **Display View** tab to show the contents of the file.

Figure 21: File System module > Filename column filter > employee logins



The screenshot shows the Forensic Explorer interface with the 'File System' tab selected. A search bar at the top right contains the filter 'employee logins'. The main pane displays a table of files found in the 'Desktop' folder:

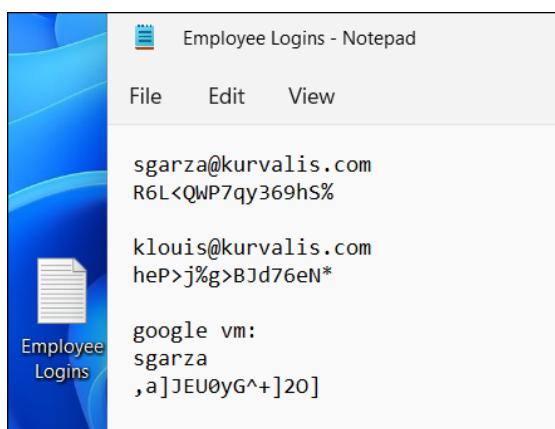
Filename	Extension	File Signature
1 Employee Logins.txt	txt	Text
2 Employee Logins.lnk	lnk	LNK
3 Employee Logins.lnk	lnk	LNK

Below the table, a preview pane shows the contents of the 'Employee Logins.txt' file:

```
sgarza@kurvalis.com
R6L<QWP7qy369hs%
klouis@kurvalis.com
heP>j%g>BJd76eN*
google vm:
sgarza
,a]JEU0yG^+]20]
```

The presence of **Employee Logins.txt** was also identified on the desktop of the computer during the Live Boot process described in Preparing the Case in Forensic Explorer.

Figure 22: Live Boot Virtualization > Desktop > Employee Logins



## QUESTION 5 - WHY WAS 6 AFRAID OF 7? BECAUSE 7 CAN UNARCHIVE VIRTUAL DRIVES! (10 POINTS)

**Within the past 2 years, a popular unarchiving program gained the ability to unarchive VHDX virtual disk images. What version of the program was this upgrade implemented?**

### Q5. ANSWER

7-Zip - 21.07

### Q5. FORENSIC EXPLORER METHODOLOGY

This question can be answered without use of the forensic image. A Perplexity AI query identified 7-Zip as the likely answer, which was confirmed using the 7-Zip version history on their website.

Figure 23: Perplexity AI

#### ☰ Answer

You can unarchive VHDX files using various programs such as PowerShell, VHD Recovery Wizard, PowerISO, and 7-Zip. Here are the steps for each:

Figure 24: Perplexity AI

#### ☰ Answer

The ability to unarchive VHDX files was added in 7-Zip version 21.07 <sup>1</sup>. This version introduced support for extracting VHDX disk images, allowing users to extract the contents of these Microsoft Hyper-V Virtual Hard Disk v2 format files using 7-Zip. Therefore, 7-Zip version 21.07 or later is capable of unarchiving VHDX files.

Figure 25: <https://7-zip.org>

#### 7-Zip ChangeLog

[History of 7-zip changes](#)

Figure 26: <https://7-zip.org/history.txt>

21.07 2021-12-26

- 
- 7-Zip now can extract VHDX disk images (Microsoft Hyper-V Virtual Hard Disk v2 format).
  - New switches: -spm and -im!{file\_path} to exclude directories from processing for specified paths that don't contain path separator character at the end of path.
  - In the "Add to Archive" window, now it is allowed to use -m prefix for "Parameters" field as in command line: -mparam.
  - The sorting order of files in archives was slightly changed to be more consistent for cases where the name of some directory is the same as the prefix part of the name of another directory or file.
  - TAR archives created by 7-Zip now are more consistent with archives created by GNU TAR program.

## QUESTION 6 - WE'RE NOT IN KANSAS ANYMORE... (25 POINTS)

***The user has established an RDP connection to one destination more than any other. What is the Geolocation of this destination? (Format: City, ST)?***

### Q6. ANSWER

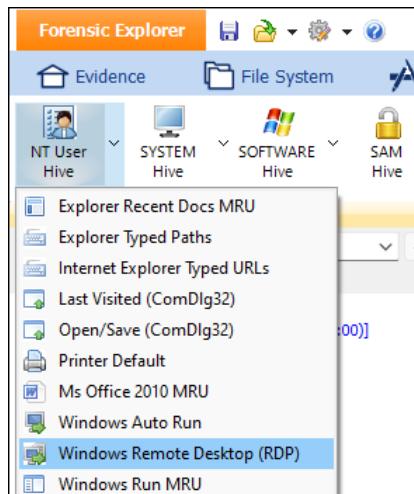
34.162.97.100 – Columbus, Ohio.

### Q6. FORENSIC EXPLORER METHODOLOGY

Windows Remote Desktop (RDP) information is located in the Windows Registry.

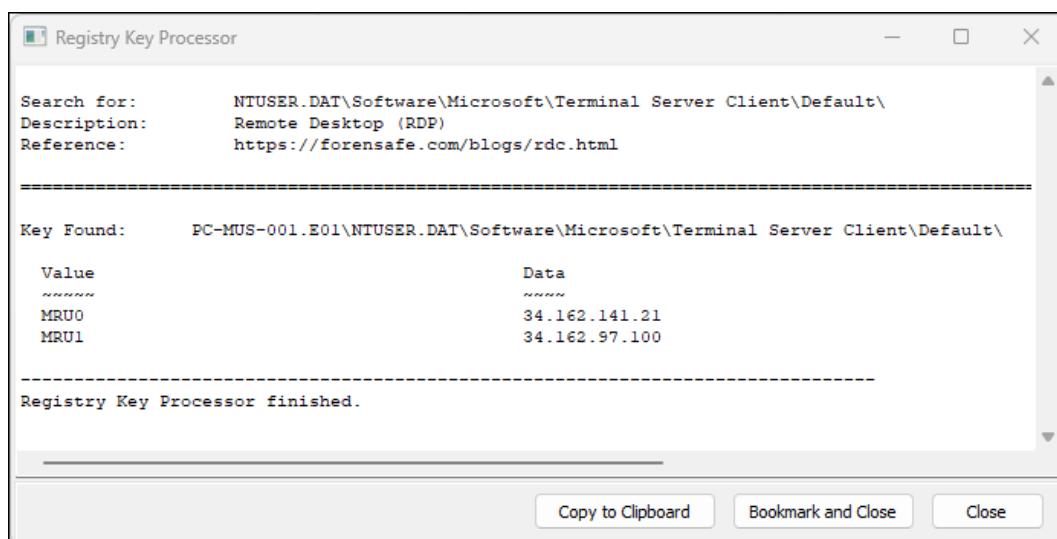
1. Select Registry > NT User Hive > Windows Remote Desktop (RDP).

Figure 27: Registry > NT User Hive > Windows Remote Desktop (RDP)



The following relevant I.P. addresses are identified.

Figure 28: Registry > NT User Hive > Windows Remote Desktop (RDP) output



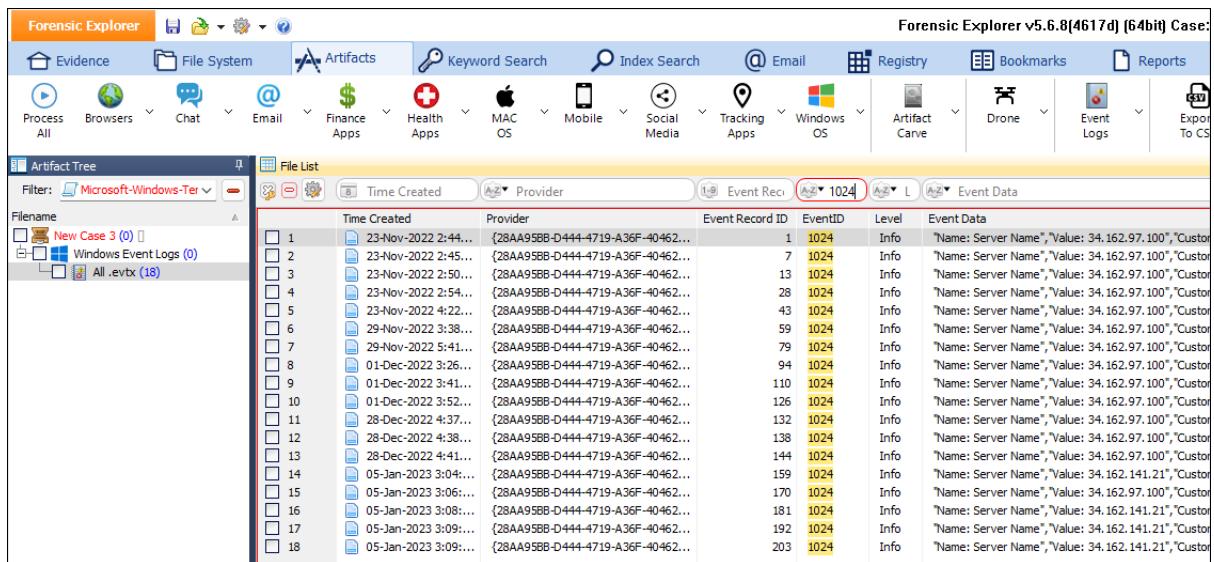
More detailed RDP information can be located in Windows Event Logs. The Windows event with ID 1024 is related to RDP (Remote Desktop Protocol) connections. It is generated when a user initiates an RDP connection using the RDP client MSTSC.exe in Windows by pressing 'connect'.

To filter RDP Event logs:

1. Switch to the **Artifacts** module.
2. In the **Artifact Tree**, select the drop-down filter **Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx**.
3. Or use **1024** in the **EventID** column filter.

The output shows the most frequent connection is to I.P. address 34.162.97.100.

Figure 29: Artifacts > Windows Event Logs > Folders and/or Column Filter > RDP Event ID 1024



The screenshot shows the Forensic Explorer interface with the 'Artifacts' tab selected. In the 'Artifact Tree' pane, 'Windows Event Logs' is selected. The 'Event Data' table is displayed with the following columns: Time Created, Provider, Event Record ID, EventID, Level, and Event Data. A filter for 'EventID' is applied, showing only entries with ID 1024. The 'Event Data' column shows repeated entries for the IP address 34.162.97.100.

Time Created	Provider	Event Record ID	EventID	Level	Event Data
23-Nov-2022 2:44...	{28AA958B-D444-4719-A36F-40462...	1	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
23-Nov-2022 2:45...	{28AA958B-D444-4719-A36F-40462...	7	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
23-Nov-2022 2:50...	{28AA958B-D444-4719-A36F-40462...	13	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
23-Nov-2022 2:54...	{28AA958B-D444-4719-A36F-40462...	28	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
23-Nov-2022 4:22...	{28AA958B-D444-4719-A36F-40462...	43	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
29-Nov-2022 3:38...	{28AA958B-D444-4719-A36F-40462...	59	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
29-Nov-2022 5:41...	{28AA958B-D444-4719-A36F-40462...	79	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
01-Dec-2022 3:26...	{28AA958B-D444-4719-A36F-40462...	94	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
01-Dec-2022 3:41...	{28AA958B-D444-4719-A36F-40462...	110	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
01-Dec-2022 3:52...	{28AA958B-D444-4719-A36F-40462...	126	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
28-Dec-2022 4:37...	{28AA958B-D444-4719-A36F-40462...	132	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
28-Dec-2022 4:38...	{28AA958B-D444-4719-A36F-40462...	138	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
28-Dec-2022 4:41...	{28AA958B-D444-4719-A36F-40462...	144	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
05-Jan-2023 3:04...	{28AA958B-D444-4719-A36F-40462...	159	1024	Info	{"Name: Server Name", "Value: 34.162.141.21", "Custom"}
05-Jan-2023 3:06...	{28AA958B-D444-4719-A36F-40462...	170	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
05-Jan-2023 3:08...	{28AA958B-D444-4719-A36F-40462...	181	1024	Info	{"Name: Server Name", "Value: 34.162.141.21", "Custom"}
05-Jan-2023 3:09...	{28AA958B-D444-4719-A36F-40462...	192	1024	Info	{"Name: Server Name", "Value: 34.162.97.100", "Custom"}
05-Jan-2023 3:09...	{28AA958B-D444-4719-A36F-40462...	203	1024	Info	{"Name: Server Name", "Value: 34.162.141.21", "Custom"}

Online I.P. address tracing tools can be used to determine the geographic location of the I.P. address.

Figure 30: Online IP Address tracking



The screenshot shows geolocation data for the IP address 34.162.97.100. The data is presented in a table with the following columns:

Geolocation data from IP2Location (Product: DB6, 2023-12-1)	
 IP ADDRESS:	34.162.97.100
 COUNTRY:	United States 
 REGION:	Ohio
 CITY:	Columbus
 ISP:	Google LLC
 ORGANIZATION:	Not available
 LATITUDE:	39.9614
 LONGITUDE:	-82.9977

## QUESTION 7 - MAKE SURE TO KEEP SOME TABS ON THAT SYSADMIN FROM SOUTHERN CALIFORNIA (25 POINTS)

***The user visited the Mastodon page of one user more than any others on the platform. What is the full legal name of the user Michael visited?***

### Q7. ANSWER

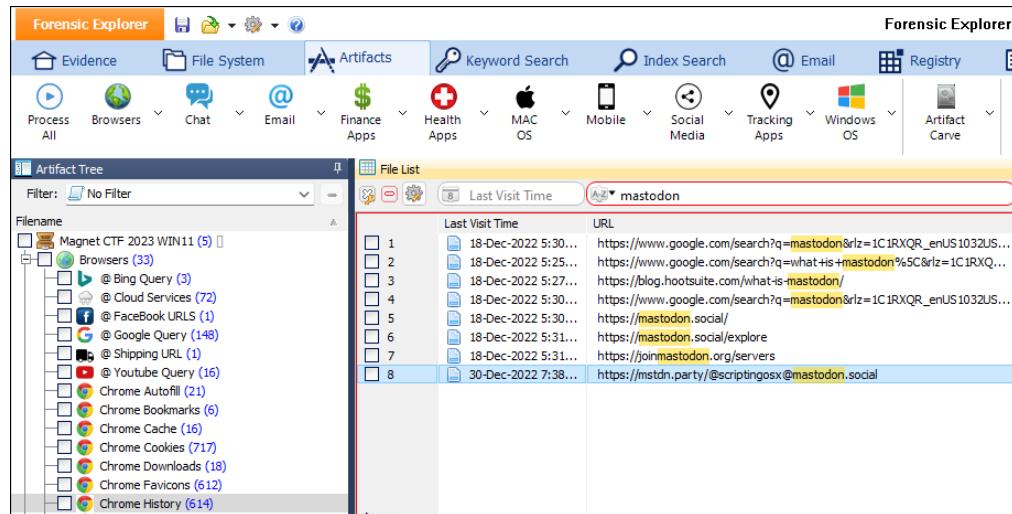
Armin Briegel

### Q7. FORENSIC EXPLORER METHODOLOGY

This answer is found in the Artifacts module browsing history.

1. In the **Artifacts** module, select **Chrome History**.
2. In the **URL** column filter, search for **mastodon**.

Figure 31: Artifacts > Browsers > Chrome History



The screenshot shows the Forensic Explorer interface with the 'Artifacts' module selected. The 'Browsers' category is expanded, and 'Chrome History' is selected. In the 'File List' pane, the URL column is filtered for 'mastodon'. The list shows several entries, with the last one being highlighted in blue. The URL for the last entry is: <https://mstdn.party/@scriptingosx@mastodon.social>.

Right-click, **copy cell**, and paste the URL into a browser

(<https://mstdn.party/@scriptingosx@mastodon.social>) reveals a LinkedIn profile on the page for Armin Briegel.

Figure 32: LinkedIn Profile - Armin Briegel



The screenshot shows a LinkedIn profile for 'Scripting OS X' (@scriptingosx@mastodon.social). The profile includes the following information:

- BIO:** # is not a curse word
- JOINED:** Nov 13, 2017
- WEBLOG:** [scriptingosx.com/](http://scriptingosx.com/)
- SLACK:** [macadmins.slack.com/team/U06R6...](https://macadmins.slack.com/team/U06R6...)
- GITHUB:** [github.com/scriptingosx](https://github.com/scriptingosx)
- LINKEDIN:** [LinkedIn.com/in/armin-briegel](https://www.linkedin.com/in/armin-briegel)

## QUESTION 8 - WE HAVE A HISTORY OF ATTRACTING SOME SIZEABLE DONORS WITH OUR PROJECTS (25 POINTS)

**Michael used PowerShell to clone a particular GitHub utility. What is the account name of one of this repo's most prominent sponsors?**

### Q8. ANSWER

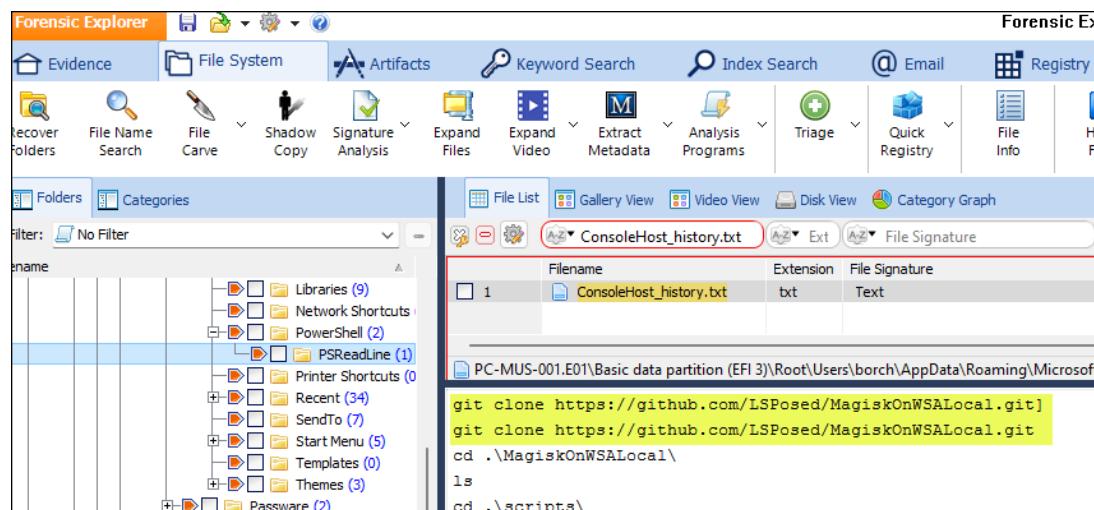
yujincheng08

### Q8. FORENSIC EXPLORER METHODOLOGY

**ConsoleHost\_history.txt** is a known artifact for PowerShell logs. Without this information, this file could also have been identified by running a Keyword Search or Index Search for **github** or similar keywords.

To locate **ConsoleHost\_history.txt**:

1. In the **File System** module, branch place the entire case.
2. In the **Filename** column, apply the column filter **ConsoleHost\_history.txt**.
3. Use the Display, Hex, or Text views to examine the file content.

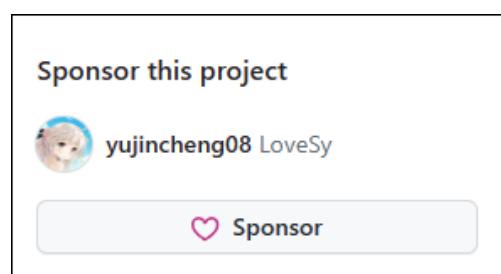


The screenshot shows the Forensic Explorer interface with the 'File System' module selected. In the left pane, a tree view shows the file structure, including 'PowerShell' and 'PSReadLine' subfolders. In the right pane, a table lists files with the filter 'ConsoleHost\_history.txt' applied. One row is selected, showing the file name, extension (txt), and file signature (Text). The content pane displays the PowerShell command history, which includes:

```
git clone https://github.com/LSPosed/MagiskOnWSALocal.git
git clone https://github.com/LSPosed/MagiskOnWSALocal.git
cd .\MagiskOnWSALocal\
ls
cd .\scripts\
```

Visiting the URL <https://github.com/LSPosed/MagiskOnWSALocal.git> identifies the sponsor of the page to be yujincheng08.

Figure 33: Page sponsor - <https://github.com/LSPosed/MagiskOnWSALocal>



The screenshot shows a sponsorship page. It features a profile picture of a person with the name 'yujincheng08 LoveSy'. A button labeled 'Sponsor' with a heart icon is visible at the bottom.

## QUESTION 9 - SCRATCH THAT ITCH.IO (25 POINTS)

**The user viewed a YouTube video by the creator BenBonk surrounding video game developers. Within this video, how many developers were involved with the project?**

### Q9. ANSWER

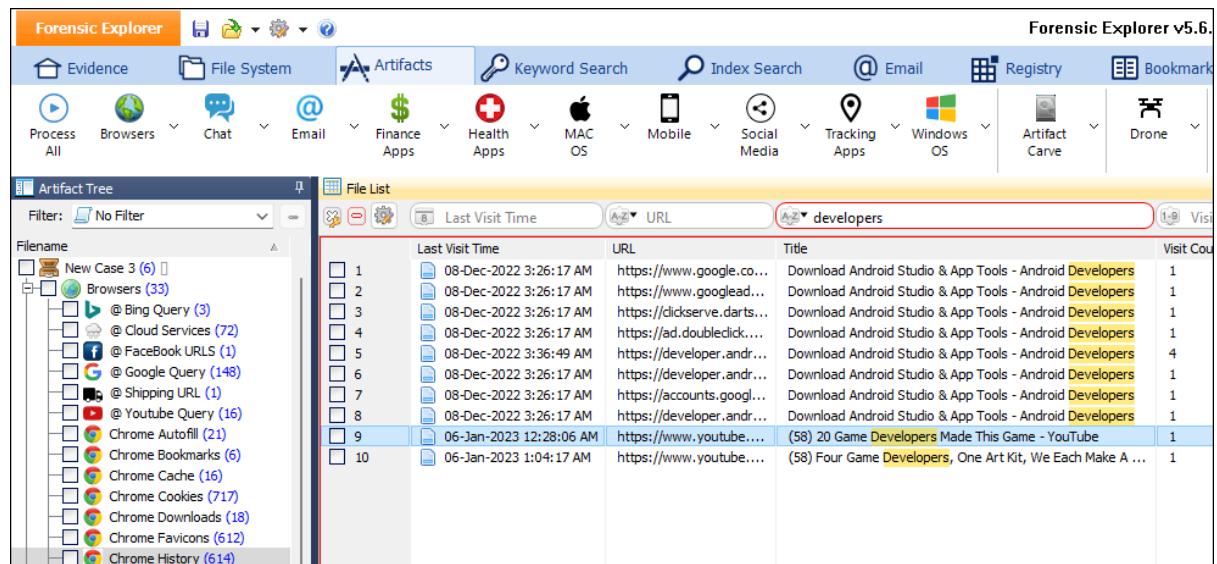
20.

### Q9. FORENSIC EXPLORER METHODOLOGY

This answer is found in the Artifacts module browsing history.

1. In the **Artifacts** module, select **Chrome History**.
2. In the **Title** column filter, search for **developers**.

Figure 34: Artifacts > Browsers > Chrome History



Last Visit Time	URL	Title	Visit Count
08-Dec-2022 3:26:17 AM	https://www.google.co...	Download Android Studio & App Tools - Android Developers	1
08-Dec-2022 3:26:17 AM	https://www.googlead...	Download Android Studio & App Tools - Android Developers	1
08-Dec-2022 3:26:17 AM	https://clickserve.darts...	Download Android Studio & App Tools - Android Developers	1
08-Dec-2022 3:26:17 AM	https://ad.doubleclick....	Download Android Studio & App Tools - Android Developers	1
08-Dec-2022 3:36:49 AM	https://developer.andr...	Download Android Studio & App Tools - Android Developers	4
08-Dec-2022 3:26:17 AM	https://developer.andr...	Download Android Studio & App Tools - Android Developers	1
08-Dec-2022 3:26:17 AM	https://accounts.googl...	Download Android Studio & App Tools - Android Developers	1
08-Dec-2022 3:26:17 AM	https://developer.andr...	Download Android Studio & App Tools - Android Developers	1
06-Jan-2023 12:28:06 AM	https://www.youtube....	(58) 20 Game Developers Made This Game - YouTube	1
06-Jan-2023 1:04:17 AM	https://www.youtube....	(58) Four Game Developers, One Art Kit, We Each Make A ...	1

Right-click, copy cell, and paste the URL into a browser

(<https://www.youtube.com/watch?v=EUDQoGL-Hnk>) reveals the text **20 Game Developers Made This Game**.

Figure 35: URL - <https://www.youtube.com/watch?v=EUDQoGL-Hnk>



## QUESTION 10 - THE BREAKFAST BELL IS RINGING (50 POINTS)

***The user has been doing some research lately on fast food items. What is, according to some experts, the unhealthiest food item of the bunch?***

### Q10. ANSWER

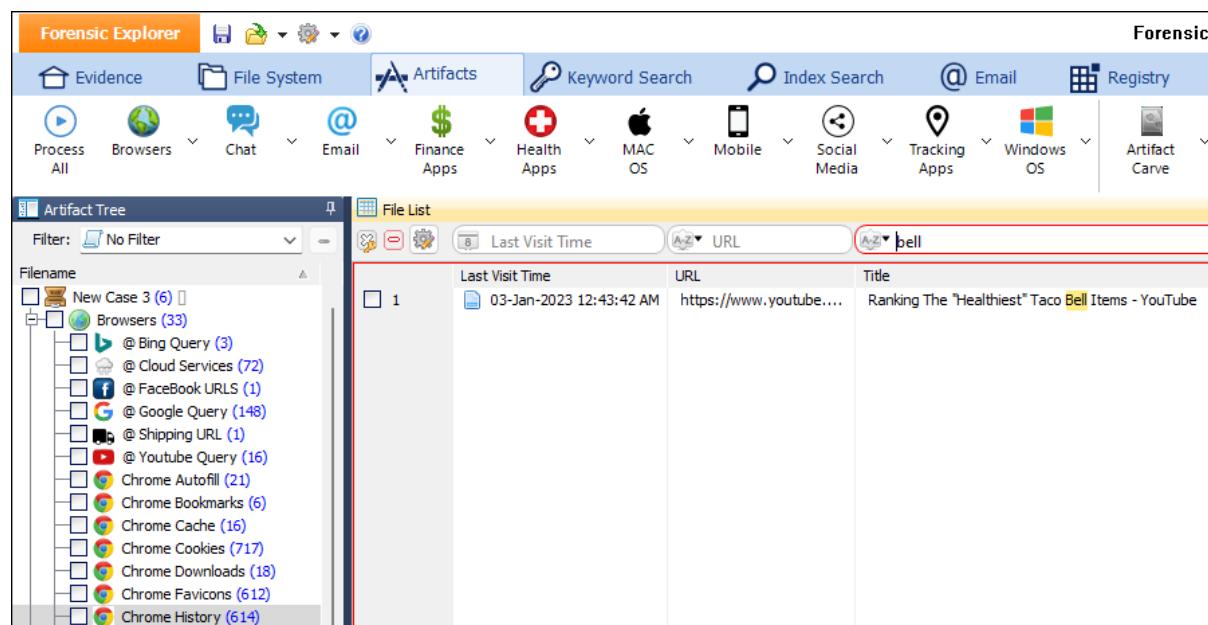
breakfast crunchwrap sausage supreme

### Q4. FORENSIC EXPLORER METHODOLOGY

From the wording of this question, 'user research' suggests web browsing, and 'breakfast bell' suggests Taco Bell. This answer is found in the Artifacts module browsing history.

1. In the **Artifacts** module, select **Chrome History**.
2. In the **Title** column filter, search for **bell**.

Figure 36: Artifacts > Browsers > Chrome History



The screenshot shows the Forensic Explorer interface with the 'Artifacts' tab selected. The 'Browsers' icon is highlighted. The 'File List' pane shows a table with columns: 'Last Visit Time', 'URL', and 'Title'. A single entry is listed: '03-Jan-2023 12:43:42 AM' in 'Last Visit Time', 'https://www.youtube....' in 'URL', and 'Ranking The "Healthiest" Taco Bell Items - YouTube' in 'Title'. The 'Title' column has a filter bar with 'bell' typed into it, which is circled in red. The 'Artifact Tree' pane on the left shows a tree structure with 'Browsers' expanded, showing various sub-items like 'Bing Query', 'Cloud Services', 'FaceBook URLs', etc.

Figure 37: Ranking The "Healthiest" Taco Bell Items – YouTube (<https://www.youtube.com/watch?v=u0V2kYuNOTc>)



## QUESTION 11 - OH DEER...I THINK WE'RE LOST (50 POINTS)

**Michael lives just a mile south of a beautiful body of water. What is the name of this body of water?**

### Q11. ANSWER

Deer Creek.

### Q11. FORENSIC EXPLORER METHODOLOGY

A reliable artifact to find user home address information is the browser autofill, where uses auto complete web forms. To view autofill information:

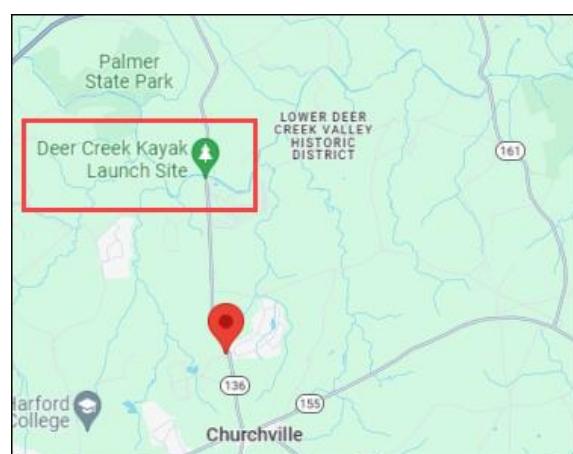
1. In the **Artifacts** module, select **Chrome Autofill**.
2. **ADDRESS\_Line\_1** of **302 preistford rd** is located.

Figure 38: Artifacts > Browsers > Chrome Autofill

Value	Value Name	Date Created	Date Last Used
1	username	23-Nov-2022 1:00...	23-Nov-2022 1:00:02 ...
2	ccmonth	23-Nov-2022 1:34...	23-Nov-2022 2:11:50 ...
3	ccyear	23-Nov-2022 1:34...	23-Nov-2022 2:11:50 ...
4	businessName	23-Nov-2022 2:11...	23-Nov-2022 2:11:50 ...
5	ADDRESS_LINE_1	23-Nov-2022 2:11:50...	23-Nov-2022 2:11:50...
6	_4rif_mat-input-2	23-Nov-2022 2:17...	23-Nov-2022 2:17:50 ...
7	_Orif_mat-input-12	23-Nov-2022 2:29...	23-Nov-2022 2:29:19 ...
8	_Orif_mat-input-21	23-Nov-2022 2:32...	23-Nov-2022 2:32:07 ...
9	username	23-Nov-2022 2:46...	23-Nov-2022 2:46:22 ...

Google Maps shows that the first body of water north of **302 preistford rd** is **Deer Creek**.

Figure 39: Google Maps - 302 preistford rd



## QUESTION 12 - GOTTA GIT GOING FAST WITH SOME ACCELERATED EMULATION! (50 POINTS)

*In order to emulate an Android device, the user required some specialized management tools. What Android port is used by default with these services?*

### Q12. ANSWER

58526

### Q12. FORENSIC EXPLORER METHODOLOGY

The question suggests that there is emulation software has been installed on the PC. Similar to Question2, we can examine the software installed using the Report module triage report, and the source data in the Registry module. The candidate is **WSA PacMan version 1.3.6**:

Figure 40: Registry > Uninstall Programs

PC-MUS-001.E01\Basic data partition (EFI 3)\Root\Windows\System32\config\SOFTWARE	
7-Zip 22.01 (x64)	
Android Studio	
BlueStacks 5	
Git	
Intel® Hardware Accelerated Execution Manager	
Microsoft Visual C++ 2022 X64 Additional Runtime - 14.31.31103	
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.31.31103	
WSA PacMan version 1.3.6	

A check of browsing history in Artifacts > Chrome History and using a column filter for **git** and **android** give as match for [https://github.com/alesimula/wsa\\_pacman](https://github.com/alesimula/wsa_pacman).

Figure 41: Artifacts > Browsers > Chrome History

File List			
	Last Visit Time	git	android
1	04-Jan-2023 9:06:34 PM	https://www.youtube.com/redirect?event=video_des...	Title
2	04-Jan-2023 9:07:08 PM	https://github.com/alesimula/wsa_pacman	GitHub - alesimula/wsa_pacman: A GUI package manager and package installer for Windows Subsystem for Android (WSA)
3	05-Jan-2023 12:10:33 AM	https://github.com/LSPosed/MagiskOnWSALocal	GitHub - LSPosed/MagiskOnWSALocal: Integrate Magisk root and Google Apps into WSA (Windows Subsystem for Android)
4	05-Jan-2023 12:10:33 AM	https://www.youtube.com/redirect?event=video_des...	GitHub - LSPosed/MagiskOnWSALocal: Integrate Magisk root and Google Apps into WSA (Windows Subsystem for Android)

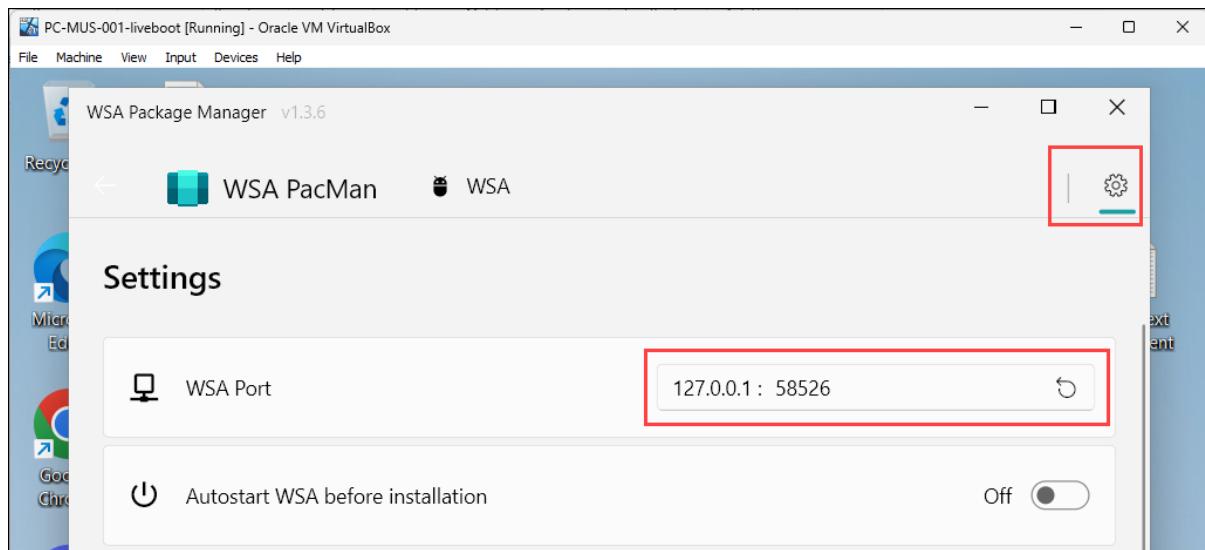
Right-click and copy the URL to a browser confirms the following information on the Git page:

Figure 42: [https://github.com/alesimula/wsa\\_pacman](https://github.com/alesimula/wsa_pacman)

About
A GUI package manager and package installer for Windows Subsystem for Android (WSA)

In Live Boot virtualization, WSA PacMan is launched and the WSA Port is identified in the Settings window:

Figure 43: Live Boot virtualization - WSA PacMan



## QUESTION 13 - PCA - PROGRAM CLANG ASSISTANT? (100 POINTS)

**The user has installed Android Studio with a specialized plugin dedicating to diagnosing and fixing some programming errors. When this plugin runs, what exit code is used upon completion?**

### Q13. ANSWER

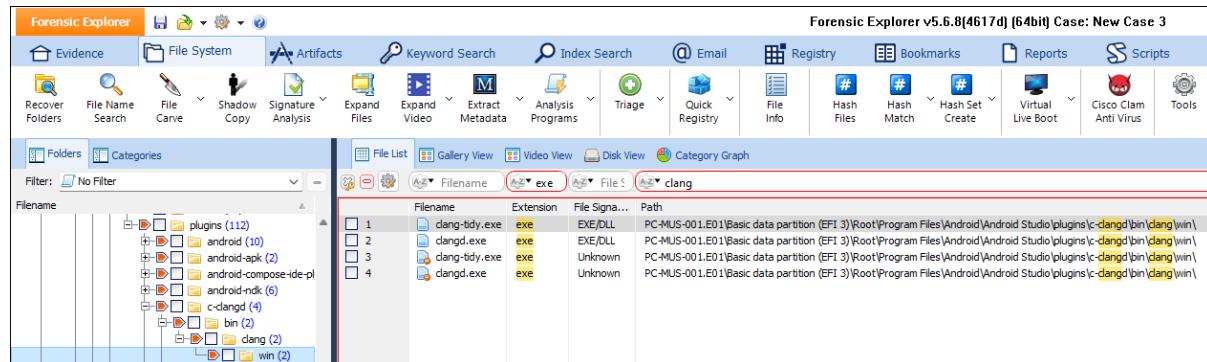
0xc0000135

### Q13. FORENSIC EXPLORER METHODOLOGY

The keyword **clang** provided the most unique entry point to search for files related to this question.

The entire case was branch plated, and then **exe** files were filtered with **clang** in the file path. This identified the potential candidate **clang-tidy.exe**.

Figure 44: File System column filter for .exe files with 'clang' in the path



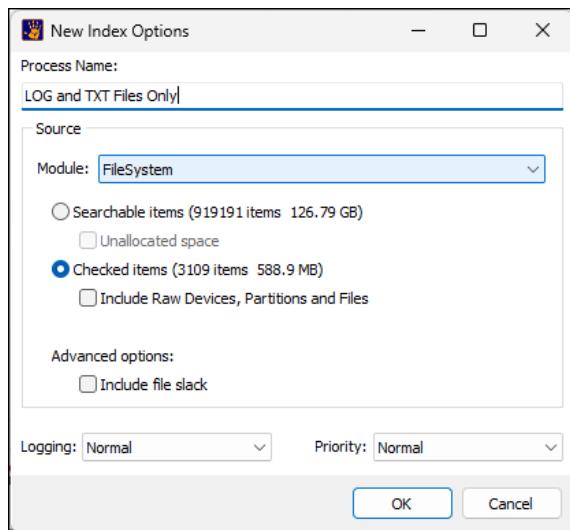
The screenshot shows the Forensic Explorer interface with the 'File System' module selected. A search filter 'clang' is applied to the 'Filename' column. The results table shows four entries:

Filename	Extension	File Sign...	Path
1 clang-tidy.exe	exe	EXE/DLL	PC-MUS-001.E01\Basic data partition (EFI 3)\Root\Program Files\Android\Android Studio\plugins\c-dangd\bin\clang\win\
2 clangd.exe	exe	EXE/DLL	PC-MUS-001.E01\Basic data partition (EFI 3)\Root\Program Files\Android\Android Studio\plugins\c-dangd\bin\clang\win\
3 clang-tidy.exe	exe	Unknown	PC-MUS-001.E01\Basic data partition (EFI 3)\Root\Program Files\Android\Android Studio\plugins\c-dangd\bin\clang\win\
4 clangd.exe	exe	Unknown	PC-MUS-001.E01\Basic data partition (EFI 3)\Root\Program Files\Android\Android Studio\plugins\c-dangd\bin\clang\win\

With the knowledge that application exit codes are usually written to associated **.log** or **.txt**, an **Index Search** was created for just those file types:

1. In the File System module **branch plate** the **entire case**.
2. Right-click in the **File System module Folder Tree** and **Clear All Checks**.
3. In the Extension column, change the column filter type to **Regex** and filter for **log|txt** (log or txt files). 3109 files are located.
4. Click **Ctrl A** in the **File List** view to highlight all 3019 files.
5. Press **Space Bar** to place a checkmark in all 3019 items.
6. In the **Index Search** module, create a **New Index**.
7. Index only the **checked items**.

Figure 45: Index Search module > New Index > LOG and TXT only > Checked Items



Once indexed, a search for “clang-tidy.exe” identified a log file called **PcaGeneralDb0.txt**.

Figure 46: Index Search results

Filename	Display Name	Hits	Extension	Path
1 Amcache.hve.tmp.LOG1	Amcache.hve.tmp.LOG1	9	LOG1	PC-MUS-001.E01\Basic data partition (EFI 3)\Root\log
2 MPLog-20221111-08090...	MPLog-20221111-08090...	3		PC-MUS-001.E01\Basic data partition (EFI 3)\Root
3 PcaGeneralDb0.txt	PcaGeneralDb0.txt	18	txt	PC-MUS-001.E01\Basic data partition (EFI 3)\Root
4 SYSTEM.LOG2	SYSTEM.LOG2	3	LOG2	PC-MUS-001.E01\Basic data partition (EFI 3)\Root

This log file reveals the exit code to be: 0xc0000135.

Figure 47: PcaGeneralDb0.txt

```
\clang-tidy.exe|clang|((14.0.0 (l1vm 14.0.0git)|000623406514916fe8a730bb66e71c6002850000904|Abnormal process exit with code 0xc0000135
\clang-tidy.exe|clang|((14.0.0 (l1vm 14.0.0git)|00003dc162e21f8e083201c5f6999a10e97d0000ffff|Abnormal process exit with code 0xc0000135
```