

CIS 474 - Digital Forensics

Final Report

Spencer Stein



April 30, 2024: Version 1.0

Table of Contents:

1. Executive

Summary	4
1.1 Investigative item.....	4
1.2 Methodology/Techniques Used.....	5
1.2.1 FTK Imager	5
1.2.2 Autopsy.....	5
1.2.3 Volatile Data Commands.....	5
1.2.4 WinAudit.....	6
2. Findings	6
2.1 Autopsy Findings.....	6
2.1.1 File Types.....	6
2.1.2 Installed Programs.....	7
2.1.3 Recent Documents.....	8
2.1.4 USB Devices Attached.....	8
2.1.5 Web Activity.....	9
2.1.6 Encryption Suspected.....	10
2.2 Volatile Data Findings	
2.2.1 cprocess.exe.....	10
2.2.2 cports.exe.....	10
2.2.3 psloggedon.exe.....	11
2.2.4 psinfo.exe.....	11
2.2.5 pslist.exe.....	11
2.2.6 autorun.exe.....	12

2.3 WinAudit Findings.....	12
2.3.1 System Overview.....	12
2.3.2 Computer Details.....	13
2.3.3 Active Setup Programs	13
2.3.4 Groups and Users.....	14
2.3.5 Windows Firewall Details.....	14
2.3.6 Disk Drives.....	14
2.3.7 Physical Drives.....	15
2.3.8 Hardware Devices.....	15
2.3.9 Memory.....	16
2.3.10 Network BIOS.....	16
3. Conclusion and Recommendations.....	16

1. Executive Summary

For Digital Forensics CIS 474, Professor Beckham prompted us to create a report based on our findings from various tools. The purpose of this report is to examine and analyze a live E01 image of a virtual machine to identify potential suspicious activity, security vulnerabilities, and unauthorized activity. The analysis was conducted using forensic tools and techniques to extract, analyze, and interpret data from the E01 image.

1.1. Investigative Item

System	Item 01	
Data of Acquisition	February 12, 2024	
Time of Acquisition	03:35 PM EDT	
Volatile Data Captured?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Memory Captured?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
System function	Unknown	
Manufacturer of Item	Unknown	
Series / type of item	Windows 10 Virtual Machine	
Serial number of item	Unknown	
Manufacturer HDD	Unknown	
Type / Model HDD	Unknown	
Serial number HDD	Unknown	
Size of HDD	63.68 MB	
Operating System	Windows 10	
BIOS Time	Unknown	
Image filename	SAS.aut	

1.2. Methodology/Techniques Used

For the analysis of this virtual machine, the tools used consisted of FTK Imager, Autopsy, Volatile Data command prompts, and WinAudit. Below is the description of each tool and how it was used.

1.2.1 FTK Imager

FTK Imager is a forensic imaging software widely used by forensic investigators. The software creates images of digital devices and analyzes them. Some key functions include disk imaging, file extraction, and capturing any suspicious activity. In this instance, FTK was used to capture an E01 image of the Virtual Machine. With this image, the next tool can be used to examine the device's activities, processes, and other important information.

1.2.2 Autopsy

Autopsy is a forensic platform commonly used alongside FTK Imager for analyzing images. Autopsy can read E01 images to view files and folders, metadata, hash values, and a timeline of when the user performed certain actions. Autopsy provides built-in reporting and documentation to generate reports, findings, and results that can help support investigations and incident response efforts.

1.2.3 Volatile Data Commands

Volatile data is data in transit, in the cache, RAM, memory or registry. This is pulled from using two different types of commands, Nirsoft and Sysinternal.

Nirsoft commands:

- cports.exe - sees all the open source ports (TCP/IP and UDP)
- cprocess.exe - sees all the processes and information of each process

Sysinternal commands:

- psloggedon - checks what users are on the system
- psinfo - shows information of the system as well as who is register to the computer
- pslist - shows a list of the current processes
- autorunsc - automatically runs a script when an instance or process happens

1.2.4 WinAudit

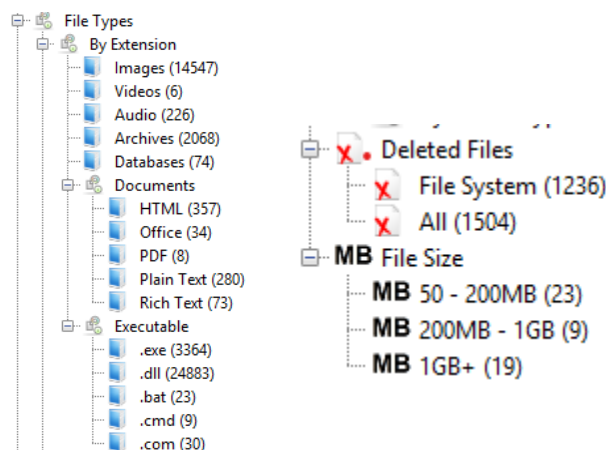
WinAudit is a free and open-source software utility for Windows that performs a detailed audit of the hardware and software configuration of a computer system. It gathers comprehensive information about various aspects of the system, including hardware components and software, network, and security configurations.

2. Findings

2.1. Autopsy Findings

With the E01 Image, Autopsy showed many issues with the virtual machine. The most important things I pulled from Autopsy were file types, installed programs, recent documents, USB devices, web activity, and suspected encryption.

2.1.1 File Types



This section provides an overview of the types of files discovered. Among the findings are a substantial number of image files, totaling 14,547, encompassing formats such as JPEG, PNG, and GIF. Additionally, there were six videos identified, which were mostly MP4 files. The dataset also contains 226 audio files, ranging from MP3 to AV and some MID formats. There were 2,068 archives detected, serving as containers for multiple files, with examples including ZIP and RAR formats. 74 databases have been uncovered, housing structured data, such as ActivitiesCache and SecStore entries. Various document types were also present, including

HTML, Office, PDF, plain text, and rich text formats. Finally, Autopsy identified five executable files, including .exe, .dll, .bat, .cmd, and .com extensions, with thousands of instances within each category.

Autopsy also uncovered crucial data regarding deleted files and file sizes. Among the findings, there were a total of 1,504 deleted files, contrasting with 1,236 files still present on the system. Most file sizes fell within the 50-200MB range, with 23 instances, followed by over 1GB, which occurred 19 times. Notably, only nine files were observed within the 200MB to 1TB range.

2.1.2 Installed Programs

Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	Spice webdavd 2.5 (ARM64) v.2.5.0	2024-01-31 02:11:53 EST	SS.E01
SOFTWARE			0	Microsoft Visual C++ 2022 Arm64 Runtime - 14.30.307...	2024-01-31 02:11:50 EST	SS.E01
SOFTWARE			0	mstsc-4b0a31aa-df6a-4307-9b47-d5cc50009643	2024-01-31 01:10:15 EST	SS.E01
SOFTWARE			0	DXM_Runtime	2024-01-06 20:33:41 EST	SS.E01
SOFTWARE			0	MPlayer2	2024-01-06 20:33:41 EST	SS.E01
SOFTWARE			0	AddressBook	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	DirectDrawEx	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	Fontcore	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	IE40	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	IE4Data	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	IE5BAKEX	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	IEData	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	MobileOptionPack	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	SchedulingAgent	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	WIC	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	Microsoft Edge WebView2 Runtime v.121.0.2277.98	2024-02-04 21:25:26 EST	SS.E01
SOFTWARE			0	Microsoft Edge v.121.0.2277.98	2024-02-04 06:47:45 EST	SS.E01
SOFTWARE			0	Microsoft Edge Update v.1.3.183.29	2024-01-31 22:19:17 EST	SS.E01
SOFTWARE			0	SPICE Guest Tools 0.164 v.0.164	2024-01-31 02:11:57 EST	SS.E01
SOFTWARE			0	Microsoft Visual C++ 2022 Redistributable (Arm64) - 1...	2024-01-31 02:11:50 EST	SS.E01
SOFTWARE			0	DXM_Runtime	2024-01-06 20:33:41 EST	SS.E01
SOFTWARE			0	MPlayer2	2024-01-06 20:33:41 EST	SS.E01
SOFTWARE			0	AddressBook	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	Connection Manager	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	DirectDrawEx	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	Fontcore	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	IE40	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	IE4Data	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	IE5BAKEX	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	IEData	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	MobileOptionPack	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	SchedulingAgent	2024-01-06 15:00:22 EST	SS.E01
SOFTWARE			0	WIC	2024-01-06 15:00:22 EST	SS.E01

Autopsy detected these 33 software applications, or programs, that were installed. These ranged from web browsers like Microsoft Edge to utilization software like Scheduling Agent.

2.1.3 Recent Documents

Source Name	S	C	O	Path	Date Accessed
CD Drive.Ink				D:\	2024-01-30 21:24:22 EST
Digital Forensics.Ink				C:\Users\Spencer\Digital Forensics	2024-02-04 21:05:56 EST
Documents.Ink				C:\Users\Spencer\Documents	2024-01-30 21:25:28 EST
Downloads.Ink				C:\Users\Spencer\Downloads	2024-02-01 17:49:31 EST
feedback-hub---contextid=606.Ink				No preferred path found	2024-01-30 20:57:35 EST
FTK_CIS_474.Ink				C:\Users\Spencer\Documents\FTK_CIS_474	2024-01-30 21:27:01 EST
Live_Validation_Jobe_Beckhom_02_01_24.Ink				C:\Users\Spencer\Downloads\Live_Validation_Jobe_Be...	2024-02-01 17:49:31 EST
ms-actioncentercontrolcenter-&suppressAnimation				No preferred path found	2024-01-30 20:19:41 EST
ms-settingsaccounts.Ink				No preferred path found	2024-01-30 20:25:14 EST
ms-settingswindowsupdatewinsettingshome.Ink				No preferred path found	2024-01-30 20:25:19 EST
SS.E01.Ink				C:\Users\Spencer\Digital Forensics\SS.E01	2024-02-04 21:05:56 EST
The Internet.Ink				No preferred path found	2024-01-30 20:19:41 EST
Windows Defender Firewall.Ink				No preferred path found	2024-01-30 20:32:30 EST
windowsdefender--network-.Ink				No preferred path found	2024-01-30 20:32:18 EST
No preferred path found.Ink				No preferred path found	0000-00-00 00:00:00
Live_Validation_Jobe_Beckhom_02_01_24.png.Ink				C:\Users\Spencer\Downloads\Live_Validation_Jobe_Be...	0000-00-00 00:00:00
Pictures.Ink				C:\Users\Spencer\Pictures	0000-00-00 00:00:00
Videos.Ink				C:\Users\Spencer\Videos	0000-00-00 00:00:00
Music.Ink				C:\Users\Spencer\Music	0000-00-00 00:00:00
Desktop.Ink				C:\Users\Spencer\Desktop	0000-00-00 00:00:00
NTUSER.DAT				C:\Windows\system32\devmgmt.msc	
NTUSER.DAT				C:\Windows\system32\wf.msc	

Autopsy detected these 22 documents that had been accessed or modified recently. These documents include mostly .Ink file extensions that are shortcuts to other programs or files.

2.1.4 USB Devices Attached

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID
SYSTEM			0	2024-02-04 20:42:26 EST		ROOT_HUB30	48156726038080
SYSTEM			0	2024-02-04 20:42:26 EST		ROOT_HUB30	481d2d9bc8080
SYSTEM			0	2024-01-30 20:41:40 EST		ROOT_HUB30	482cc4d7158080
SYSTEM			0	2024-01-30 20:41:40 EST		ROOT_HUB30	489a1dcae8080
SYSTEM			0	2024-01-30 20:41:40 EST	NEC Corp.	Hub	MSFT20314159-0000:00:03.0-4
SYSTEM			0	2024-02-04 20:42:27 EST	NEC Corp.	Hub	MSFT20314159-0000:00:04.0-4
SYSTEM			0	2024-01-30 20:41:40 EST	Adomax Technology Co., Ltd	Product: 0001	28754-0000:00:03.0-1
SYSTEM			0	2024-02-04 20:42:26 EST	Adomax Technology Co., Ltd	Product: 0001	28754-0000:00:04.0-1
SYSTEM			0	2024-01-30 20:41:40 EST	Adomax Technology Co., Ltd	Product: 0001	68284-0000:00:03.0-3
SYSTEM			0	2024-02-04 20:42:26 EST	Adomax Technology Co., Ltd	Product: 0001	68284-0000:00:04.0-3
SYSTEM			0	2024-01-30 20:41:40 EST	Adomax Technology Co., Ltd	Product: 0001	89126-0000:00:03.0-2
SYSTEM			0	2024-02-04 20:42:27 EST	Adomax Technology Co., Ltd	Product: 0001	89126-0000:00:04.0-2
SYSTEM			0	2024-02-04 01:52:25 EST	Western Digital Technologies, Inc.	Product: 25FC	575837314133374E384E3534
SYSTEM			0	2024-01-30 20:41:41 EST	QEMU	Product: 0001	1-0000:00:03.0-4.1
SYSTEM			0	2024-02-04 20:42:27 EST	QEMU	Product: 0001	1-0000:00:04.0-4.1

Autopsy revealed that 15 USB devices have been connected or were connected at some point in time. These devices may include external storage drives (utilized during the investigation), input devices such as keyboards or mice, printers, cameras, smartphones, or any other peripherals.






2.1.5 Web Activity

The four main areas of interest with web activity on this VM was the accounts, history, searches, and downloads. These show us online activities and the behavior of the user.







Web Accounts (2)

Source Name	S	C	O	URL	Date Created	Decoded URL	Username
 Login Data				https://cas.messiah.edu/	2024-01-30 21:19:28 EST	messiah.edu	Default
 Login Data				https://login.microsoftonline.com/	2024-01-30 21:20:28 EST	microsoftonline.com	Default






Web History (138) - Findings were repetitive with the search of Canvas Instructure

Source Name	S	C	O	URL	Date Accessed	Referrer URL
 History			1	https://www.bing.com/search?q=canvas&cvid=db54...	2024-01-30 21:15:41 EST	https://www.bing.com/search?q=
 History			1	https://www.bing.com/ck/a?!&&p=b326bfeed75608e...	2024-01-30 21:15:41 EST	https://www.bing.com/ck/a?!&&
 History			1	https://www.bing.com/search?q=canvas&cvid=db54...	2024-01-30 21:15:41 EST	https://www.bing.com/search?q=
 History			1	https://canvas.instructure.com/	2024-01-30 21:15:42 EST	https://canvas.instructure.com/
 History			1	https://canvas.instructure.com/login	2024-01-30 21:15:42 EST	https://canvas.instructure.com/lc

Web Search (6) - Only showed the recent searches

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
 History				bing.com	canvas	Microsoft Edge	2024-01-30 21:15:41 EST	SS.E01
 History				bing.com	canvas	Microsoft Edge	2024-01-30 21:15:41 EST	SS.E01
 History				bing.com	canvas login	Microsoft Edge	2024-01-30 21:16:00 EST	SS.E01
 History				bing.com	canvas login	Microsoft Edge	2024-01-30 21:16:00 EST	SS.E01
 History				bing.com	canvas login	Microsoft Edge	2024-01-30 21:16:00 EST	SS.E01
 History				bing.com	canvas login	Microsoft Edge	2024-01-30 21:16:00 EST	SS.E01

Web Downloads (294) - Anything downloaded from the web

Source Name	S	C	O	Path
 ADIsoDLL.dll:Zone.Identifier				/Users/Spencer/Documents/FTK_CIS_474/FTK Imager/...
 ADIsoDLL.dll:Zone.Identifier				/Users/Spencer/Documents/FTK_CIS_474/FTK_CIS_474...
 ADIsoDLL.dll:Zone.Identifier				/Users/Spencer/Downloads/FTK_CIS_474/FTK_CIS_474...
 ADIsoDLL.dll:Zone.Identifier				/Users/Spencer/Downloads/FTK_CIS_474 (1)/FTK_CIS_...
 FTK Imager.exe:Zone.Identifier				/Users/Spencer/AppData/Local/Temp/6c8e8a54-9e8c-...

2.1.6 Encryption Suspected

Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification
mpenginedb.db			0	File	Likely Notable			Suspected encryption due to high entropy (7.993415).

Autopsy identified one database that appears to be encrypted. Encryption is a security technique employed to safeguard data, allowing only authorized parties to access it. The database is flagged as potentially encrypted due to its high entropy, indicating characteristics typical of sensitive data.

2.2 Volatile Data Findings

Utilizing volatile data commands and tools such as Nirsoft and Sysinternals, we extracted crucial information from the VM. This data was essential for obtaining details about ports, processes, and other system information.

2.2.1 cprocess.exe - Only two main processes happening on the virtual machine.

```
Process Name      : chrome.exe
ProcessID         : 7472
Priority           : Above Normal
Product Name      : Google Chrome
Version           : 121.0.6167.161
Description        : Google Chrome
Company           : Google LLC
Window Title      :
File Size         : 2,169,120
File Created Date : 2/9/2024 8:36:01 PM
File Modified Date : 2/6/2024 12:45:45 AM
Filename          : C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Base Address      : 0x000A0000
Created On        : 2/15/2024 3:05:03 PM
Visible Windows   : 0
Hidden Windows    : 0
User Name         : DESKTOP-SUHSQD0\Spencer
Mem Usage         : 62724 K
Mem Usage Peak    : 97792 K
Page Faults       : 422676
Pagefile Usage    : 37464 K
Pagefile Peak Usage : 43072 K
File Attributes    : A
```

```
Process Name      : CProcess.exe
ProcessID         : 8976
Priority           : Normal
Product Name      : CurrProcess
Version           : 1.13
Description        : CurrProcess
Company           : Nirsoft
Window Title      :
File Size         : 36,352
File Created Date : 8/5/2014 6:21:56 AM
File Modified Date : 2/15/2024 11:08:28 PM
Filename          : C:\Users\Spencer\Downloads\Vol_Data\Vol_Data\nirsoft\CProcess.exe
Base Address      : 0x00400000
Created On        : 2/15/2024 3:32:48 PM
Visible Windows   : 0
Hidden Windows    : 0
User Name         : DESKTOP-SUHSQD0\Spencer
Mem Usage         : 14720 K
Mem Usage Peak    : 14736 K
Page Faults       : 4209
Pagefile Usage    : 6020 K
Pagefile Peak Usage : 7312 K
File Attributes    : A
```

2.2.2 cports.exe Hundreds of different ports with TCP being the most important.

```
Process Name      : System
Process ID        : 1020
Protocol          : TCP
Local Port        : 135
Local Port Name   : epmap
Local Address     : 0.0.0.0
Remote Port       :
Remote Port Name  :
Remote Address    : 0.0.0.0
Remote Host Name  :
State             : Listening
Process Path      :
Product Name      :
File Description  :
File Version      :
Company           :
Process Created On : N/A
User Name         :
Process Services  : RpcEptMapper, RpcSs
Process Attributes :
Added On         : 2/15/2024 3:33:52 PM
Module Filename   :
Remote IP Country :
Window Title      :
```

2.2.3 psloggedon.exe

```
Users logged on locally:
    2/15/2024 3:04:27 PM      DESKTOP-SUHSQDO\Spencer

No one is logged on via resource shares.
```

There is only one user on the system at the time of collection.

2.2.4 psinfo.exe

```
PsInfo
System information for \\DESKTOP-SUHSQDO:
Uptime: 0 days 0 hours 24 minutes 37 seconds
Kernel version: Windows 10 Enterprise, Multiprocessor Free
Product type: Professional
Product version: 6.3
Service pack: 0
Kernel build number: 23615
Registered organization:
Registered owner: Spencer
IE version: 9.0000
System root: C:\Windows
Processors: 4
Processor speed: 1.0 GHz
Processor type: virt-7.2
Physical memory: 4872 MB
Video driver: Red Hat VirtIO GPU DOD controller

Volume Type      Format      Label      Size      Free      Free
C: Fixed         NTFS              63.68 GB   17.13 GB   26.9%
D: CD-ROM        CDFS            UTM        137.47 MB   0.0%
Z: Remote        FAT              63.68 GB   17.13 GB   26.9%
```

The key components highlighted in Psinfo include the operating system details, ownership information, processor and memory specifications, disk volumes, and the video driver.

2.2.5 pslist.exe

```
Process information for DESKTOP-SUHSQDO:

Name                Pid Pri Thd  Hnd  Priv      CPU Time  Elapsed Time
Idle                 0  0  8    0    56      1:17:35.328 0:25:07.530
System              4  8 152 3672   172      0:01:28.343 0:25:07.530
Registry            112 8   4    0  12732     0:00:00.625 0:25:08.693
smss                 400 11  2   57   1704     0:00:00.062 0:25:07.522
csrss                516 13 11  526   2252     0:00:00.781 0:25:06.538
wininit              588 13  2  144   1788     0:00:00.093 0:25:06.465
```

There were several processes on the system when pslist.exe was run. These were the first five on the list and it shows the name, process ID, priority in the list, thread and handle count, private working set, CPU time, and elapsed time.

2.2.6 autorunsc.exe

Time	Entry Location	Entry	Enabled	Category	Description
2/15/24 15:04	HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute			Boot Execute	
11/4/00 3:59	HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute	autocheck autochk *	enabled	Boot Execute	Auto Check Utility
1/6/24 6:58	HKLM\System\CurrentControlSet\Services			Services	

The system contained numerous autorun scripts primarily initiated by software installations or setups on device startup. The graph illustrates key details such as the time, entry location, enabled status, boot category, and description of each script's function.

2.3 WinAudit Findings

WinAudit helped discover various system components, which I categorized into three main groups. The first category encompasses system configurations, providing an overview of the system, detailed computer specifications, and an active setup of installed programs. The second category focuses on user and group management, detailing user types and permissions, including those related to the active firewall. The final category comprises hardware information, covering disk drives, physical drives, hardware devices, memory, and network BIOS.

2.3.1 System Overview

Item	Value
Computer Name	DESKTOP-SUHSQDO
Domain Name	WORKGROUP
Site Name	
Roles	Workstation, Server
Description	
Operating System	Microsoft Windows 6.2 Professional 64-bit
Manufacturer	QEMU
Model	QEMU Virtual Machine
Serial Number	
Asset Tag	
Total Memory	4096MB
Total Hard Drive	995GB
Display	1440 x 910 pixels, true colour
BIOS Version	BOCHS - 1 0.0.0 EDK II - 10000
User Account	Spencer
System Uptime	0 Days, 0 Hours, 4 Minutes
Local Time	2024-04-23 15:16:27

This provides details such as the system name, operating system, manufacturer, model, total hard drive capacity, memory size, and system/local time. These fundamental computing details are essential for understanding the system configuration.

2.3.2 Computer Details

QEMU QEMU Virtual Machine

Item	Value
Device Type	Computer
Device Name	QEMU QEMU Virtual Machine
Description	Computer Device
Manufacturer	Microsoft
Location	
Driver Provider	Microsoft
Driver Version	10.0.23615.1000
Driver Date	6-21-2006
Status Code	0
Status Message	OK
Class GUID	{4D36E966-E325-11CE-BFC1-08002BE10318}
Device ID	SWD\COMPUTER\MFG_QEMU&PROD_QEMU_VIRTUAL_MACHINE

This emphasizes the device and driver specifications by giving the type and name of device, and the driver provider, version, and date. It also gives us the class GUID and device ID which are important for various system operations and configurations.

2.3.3 Active Setup Programs

Name	Version	Installed
.NET Framework	4,0,30319,0	
Active Directory Service Interface	5,0,00,0	Yes
Address Book 7	10,0,23615,1000	Yes
Browsing Enhancements	11,1000,23615,0	Yes
DirectDrawEx	4,71,1113,0	Yes
Dynamic HTML Data Binding	11,1000,23615,0	Yes
HTML Help	10,0,23615,1000	Yes
Internet Explorer Core Fonts	11,1000,23615,0	Yes
Internet Explorer Help	11,1000,23615,0	Yes
Internet Explorer Setup Tools	11,1000,23615,0	Yes
Microsoft Windows Media Player 12.0	12,0,10011,16384	Yes
Microsoft Windows Media Player	12,0,10011,16384	No
Microsoft Windows Media Player	12,0,10011,16384	Yes
Microsoft Windows Script 5.6	5,6,0,8833	Yes
MSN Site Access	4,9,9,2	Yes
Offline Browsing Pack	11,1000,23615,0	Yes

This gives an overview of the active setup programs for the system with the name, version and if it is installed. Most of the programs are associated with Internet Explorer or Microsoft.

2.3.4 Groups and Users

Group Name	Member Name
Administrators	Administrator
Administrators	Spencer

Only two groups of users were found on the system: the administrator and the registered owner of the machine on which the VM is running.

2.3.5 Windows Firewall Details

Name	Setting
Firewall Enabled	Yes
Authorised Application	Google Chrome
Authorised Application	Java(TM) Platform SE binary
Authorised Application	autopsy64
Authorised Service	File and Printer Sharing
Authorised Service	Network Discovery
Authorised Service	Remote Desktop

This gives the status of the firewall, the applications, and the allowed services.

2.3.6 Disk Drives

Item	Value
Device Type	Disk drives
Device Name	QEMU NVMe Ctrl
Description	Disk drive
Manufacturer	(Standard disk drives)
Location	Bus Number 0, Target Id 0, LUN 0
Driver Provider	Microsoft
Driver Version	10.0.23615.1000
Driver Date	6-21-2006
Status Code	0
Status Message	OK
Class GUID	{4D36E967-E325-11CE-BFC1-08002BE10318}
Device ID	SCSI\DISK&VEN_NVME&PROD_QEMU_NVME_CTRL\4&1AFDF2B5&0&000000

This provides details about the disk drives in the system, including their type, manufacturer, and location. It's essential for visualizing the logical storage units and their locations within the system.

2.3.7 Physical Drives

QEMU NVMe Ctrl

Item	Value
Disk Number	1
Capacity	65530MB
Disk Type	Fixed hard disk media
Manufacturer	
Model	QEMU NVMe Ctrl
Serial Number	0AD9D31D-5EDB-49F4-8_00000001.
Firmware Revision	
Controller Rank	Primary
Master/Slave	Master
Total Cylinders	8354
Total Heads	255
Sectors Per Track	63
Buffer Size	
SMART Supported	
SMART Enabled	
SMART Self Test	

This provides details about the physical disk drives in the system, including their type, capacity, and the number of heads and cylinders. This information is crucial for understanding the storage configuration, physical hardware, and physical characteristics of the system.

2.3.8 Hardware Devices

Line In (High Definition Audio Device)

Item	Value
Device Type	Audio inputs and outputs
Device Name	Line In (High Definition Audio Device)
Description	Audio Endpoint
Manufacturer	Microsoft
Location	
Driver Provider	Microsoft
Driver Version	10.0.23615.1000
Driver Date	1-6-2024
Status Code	0
Status Message	OK
Class GUID	{C166523C-FE0C-4A94-A586-F1A80CFB8F3E}
Device ID	SWD\MMDEVAPI\{0.0.1.00000000}-{38731492-2090-4529-973C-1285B3D95931}

Speakers (High Definition Audio Device)

Item	Value
Device Type	Audio inputs and outputs
Device Name	Speakers (High Definition Audio Device)
Description	Audio Endpoint
Manufacturer	Microsoft
Location	
Driver Provider	Microsoft
Driver Version	10.0.23615.1000
Driver Date	1-6-2024
Status Code	0
Status Message	OK
Class GUID	{C166523C-FE0C-4A94-A586-F1A80CFB8F3E}
Device ID	SWD\MMDEVAPI\{0.0.0.00000000}-{88C5B9B6-A4F1-4049-ABF8-37923F5F3851}

The VM had two hardware devices which are both audio inputs and output devices. The specifications of each are shown including description, provider, and device ID.

2.3.9 Memory

Item	Value
Total Memory	4096MB
Free Memory	1576MB
Maximum Swap File	4790MB
Free Swap File	2355MB

This displays the total and free memory allocated to the virtual machine, as well as the maximum and free size of swap files or swap partitions on the virtual disk. The maximum swap file amount represents the operating system's allowed usage for swap storage.

2.3.10 Network BIOS

Item	Value
Adapter Number	1
Software Release	3.0
MAC Address	22:78:f1:a9:3e:b2
Adapter Type	Ethernet
Maximum Sessions	16
Sessions Pending	0
Maximum Data	65535 Bytes
Maximum Datagram	512 Bytes

This provides specific details regarding the Network Basic Input/Output System (NetBIOS) protocol, including adapter number, software release version, MAC address, and adapter type. Additionally, it displays information such as the maximum number of sessions the adapter can handle consecutively, the maximum data packet and datagram size.

3. Conclusion and Recommendations

In summary, the forensic analysis of the virtual machine was successful in learning more about the system and the actions of the user. Through the use of various forensic tools including FTK Imager, Autopsy, Volatile Data commands, and WinAudit, it revealed insights into the VM's system configuration, software installations, recent user activities, and potential security risks. Noteworthy findings include the detection of numerous file types, installed programs, recent documents accessed, connected USB devices, web activity patterns, and suspected encryption within databases. Volatile data analysis provided information about system processes, ports,

logged-on users, and autorun scripts. Meanwhile, WinAudit offered comprehensive details about system configurations, hardware components, memory allocation, and network BIOS specifics. Moving forward, I have learned that security measures, such as regular software updates, password management improvements, and data backup strategies, are essential for a machine to protect data. This report has taught me the numerous areas that a VM can be vulnerable to and the important parts of a machine to look at when performing a digital forensics investigation.