CIS4203.01 **Brandon Thompson**

Dr. Ashokkumar Patel Due: 2/6//21

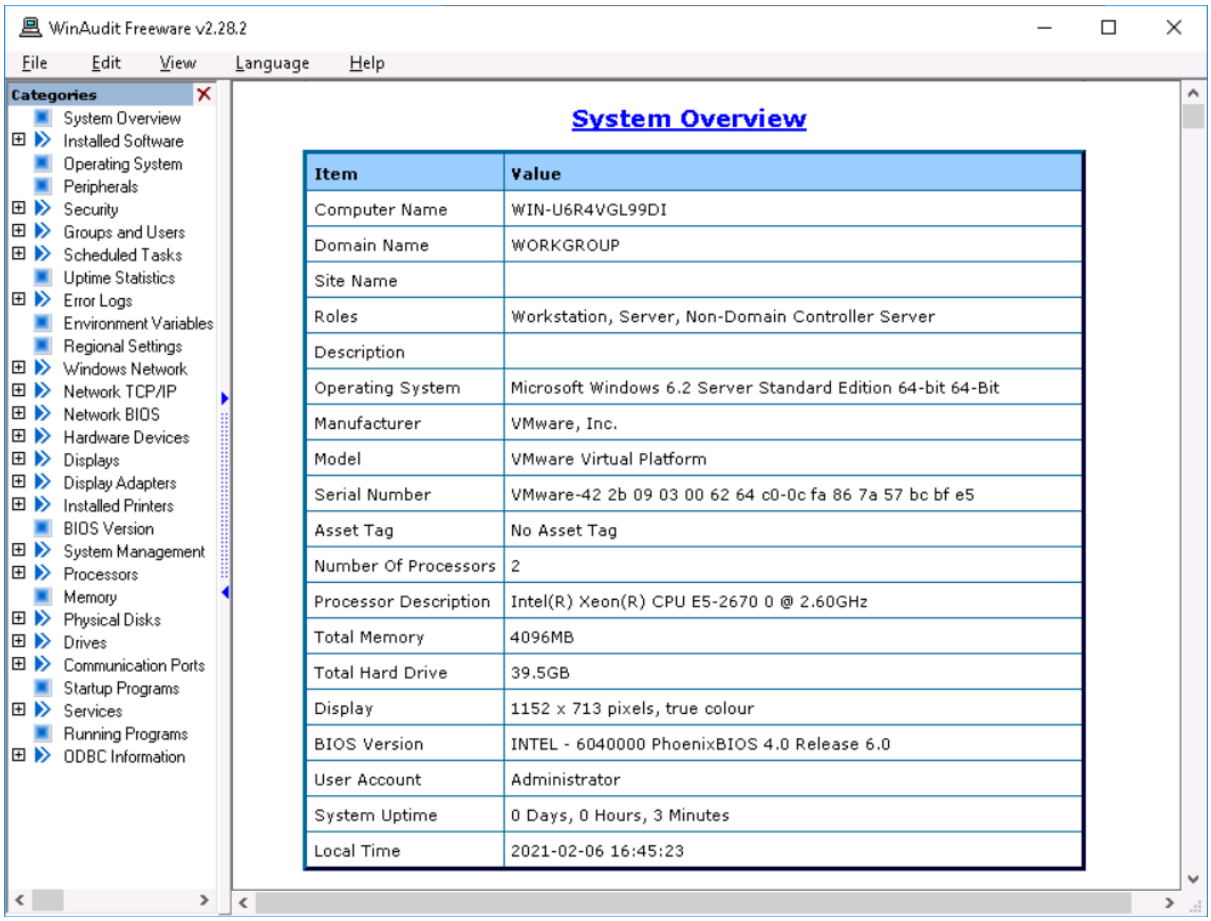
Lab 2: Documenting a Workstation Configuration Using Common Forensic Tools

1 Section 1: Hands-On Demonstration

1.1 Part 1: Use WinAudit to Inventory TargetWindows1

1. The lab begins by establishing the remote connection to the target machine: TargetMachine01.

2. Then, WinAudit is used to perform an audit on the remote computer.



Item	Value
Computer Name	WIN-U6R4VGL99DI
Domain Name	WORKGROUP
Site Name	
Roles	Workstation, Server, Non-Domain Controller Server
Description	
Operating System	Microsoft Windows 6.2 Server Standard Edition 64-bit 64-Bit
Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
Serial Number	VMware-42 2b 09 03 00 62 64 c0-0c fa 86 7a 57 bc bf e5
Asset Tag	No Asset Tag
Number Of Processors	2
Processor Description	Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz
Total Memory	4096MB
Total Hard Drive	39.5GB
Display	1152 x 713 pixels, true colour
BIOS Version	INTEL - 6040000 PhoenixBIOS 4.0 Release 6.0
User Account	Administrator
System Uptime	0 Days, 0 Hours, 3 Minutes
Local Time	2021-02-06 16:45:23

Figure 1: System overview of the audited machine, including information such as domain name, serial numbers, and BIOS versions.

Windows Firewall

Name	Setting
Firewall Enabled	No
Authorised Service	File and Printer Sharing
Authorised Service	Network Discovery
Authorised Service	Remote Desktop

Figure 2: Shows information about the Windows firewall that is set up.

User Accounts

Administrator

Item	Value
User Account	Administrator
Full Name	
Description	Built-in account for administering the computer/domain
Account Status	Enabled, Not Locked
Local Groups	Administrators
Global Groups	None
Last Logon	2/6/2021 4:45:01 PM
Last Logoff	
Number Of Logons	69
Bad Password Count	0
Password Age	1489 Days
Password Expired	No
Account Expires	

DefaultAccount

Item	Value
User Account	DefaultAccount
Full Name	
Description	A user account managed by the system.
Account Status	Disabled, Not Locked
Local Groups	System Managed Accounts Group
Global Groups	None
Last Logon	
Last Logoff	
Number Of Logons	0
Bad Password Count	0
Password Age	0 Days
Password Expired	No
Account Expires	

Guest

Item	Value
User Account	Guest
Full Name	
Description	Built-in account for guest access to the computer/domain
Account Status	Disabled, Not Locked
Local Groups	Guests
Global Groups	None
Last Logon	
Last Logoff	
Number Of Logons	0
Bad Password Count	0
Password Age	0 Days
Password Expired	No
Account Expires	

Figure 3: Authorized users of the machine.

Drive C

Item	Value
Letter	C
Drive Type	Fixed Drive
Percent Used	40%
Used Space	15.9GB
Free Space	23.6GB
Total Space	39.5GB
Volume Name	
File System	NTFS
Volume Serial Number	3007-E66E
Sectors Per Cluster	8
Bytes Per Sector	512
Free Clusters	6198439
Total Clusters	10357247

Figure 4: C: drive and the allocated and unallocated space within it.

vmxnet3 Ethernet Adapter

Item	Value
Adapter Number	4
Adapter Name	vmxnet3 Ethernet Adapter
DNS Host Name	WIN-U6R4VGL99DI
DNS Servers	8.8.8.8,8.8.4.4
IP Address	192.168.24.2
IP Subnet	255.255.255.0
Default IP Gateway	192.168.24.254
DHCP Enabled	No
DHCP Server	255.255.255.255
DHCP IP Address	
DHCP Lease Obtained	2/6/2021 4:32:14 PM
DHCP Lease Expires	2/7/2021 1:02:11 AM
Status Code	0
Adapter Status	This device is working properly.
Adapter Type	Ethernet 802.3
MAC Address	00:50:56:AB:B4:69
Connection Status	Connected
Connection Speed	10000 Mbps

Figure 5: Network TCP/IP Settings are important because they display information, like the IP addresses associated with the machine

Startup Programs

Name	Settings Folder	Startup Command
desktop.ini	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\	
Start VNC Server.lnk	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\	
desktop.ini	C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\	

Figure 6: List of programs the run on startup.

2 Section 2: Applied Learning

2.1 Part 1: Use WinAudit to Inventory the vWorkstation.

In this part of the lab, we are performing a WinAudit of the vWorkstation.

System Overview

Item	Value
Computer Name	WIN-738H8R27H7B
Domain Name	WORKGROUP
Site Name	
Roles	Workstation, Server, Non-Domain Controller Server
Description	
Operating System	Microsoft Windows 6.2 Server Standard Edition 64-bit 64-Bit
Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
Serial Number	VMware-42 2b d2 d6 65 ee a1 05-bd 04 cc a0 db a9 96 cc
Asset Tag	No Asset Tag
Number Of Processors	2
Processor Description	Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz
Total Memory	2048MB
Total Hard Drive	39.5GB
Display	1152 x 713 pixels, true colour
BIOS Version	INTEL - 6040000 PhoenixBIOS 4.0 Release 6.0
User Account	Administrator
System Uptime	0 Days, 0 Hours, 22 Minutes
Local Time	2021-02-06 17:04:10

Figure 7: System overview of the audited machine, including information such as domain name, serial numbers, and BIOS versions.

Environment Variables

Name	Variable Value
ALLUSERSPROFILE	C:\ProgramData
APPDATA	C:\Users\Administrator\AppData\Roaming
CLIENTNAME	to-guac6
CommonProgramFiles(x86)	C:\Program Files (x86)\Common Files
CommonProgramFiles	C:\Program Files (x86)\Common Files
CommonProgramW6432	C:\Program Files\Common Files
COMPUTERNAME	WIN-738H8R27H7B
ComSpec	C:\Windows\system32\cmd.exe
HOMEDRIVE	C:
HOMEPATH	\Users\Administrator
LOCALAPPDATA	C:\Users\Administrator\AppData\Local
LOGONSERVER	\\WIN-738H8R27H7B
NUMBER_OF_PROCESSORS	2
OS	Windows_NT
Path	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Users\Administrator\AppData\Local\Microsoft\WindowsApps;
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;JS;JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	x86
PROCESSOR_ARCHITEW6432	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 45 Stepping 7, GenuineIntel
PROCESSOR_LEVEL	6
PROCESSOR_REVISION	2d07
ProgramData	C:\ProgramData
ProgramFiles(x86)	C:\Program Files (x86)
ProgramFiles	C:\Program Files (x86)
ProgramW6432	C:\Program Files
PSModulePath	C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
PUBLIC	C:\Users\Public
SESSIONNAME	RDP-Tcp#0
SystemDrive	C:
SystemRoot	C:\Windows
TEMP	C:\Users\ADMINI~1\AppData\Local\Temp\2
TMP	C:\Users\ADMINI~1\AppData\Local\Temp\2
USERDOMAIN_ROAMINGPROFILE	WIN-738H8R27H7B
USERDOMAIN	WIN-738H8R27H7B
USERNAME	Administrator
USERPROFILE	C:\Users\Administrator
windir	C:\Window

Figure 8: Shows environmental variables, such as hidden programs.

User Accounts

Administrator

Item	Value
User Account	Administrator
Full Name	
Description	Built-in account for administering the computer/domain
Account Status	Enabled, Not Locked
Local Groups	Administrators
Global Groups	None
Last Logon	2/6/2021 4:42:35 PM
Last Logoff	
Number Of Logons	58
Bad Password Count	0
Password Age	1488 Days
Password Expired	No
Account Expires	

DefaultAccount

Item	Value
User Account	DefaultAccount
Full Name	
Description	A user account managed by the system.
Account Status	Disabled, Not Locked
Local Groups	System Managed Accounts Group
Global Groups	None
Last Logon	
Last Logoff	
Number Of Logons	0
Bad Password Count	0
Password Age	0 Days
Password Expired	No
Account Expires	

Guest

Item	Value
User Account	Guest
Full Name	
Description	Built-in account for guest access to the computer/domain
Account Status	Disabled, Not Locked
Local Groups	Guests
Global Groups	None
Last Logon	
Last Logoff	
Number Of Logons	0
Bad Password Count	0
Password Age	0 Days
Password Expired	No
Account Expires	

Figure 9: Authorized users of the machine.

Drive C

Item	Value
Letter	C
Drive Type	Fixed Drive
Percent Used	30%
Used Space	11.9GB
Free Space	27.7GB
Total Space	39.5GB
Volume Name	
File System	NTFS
Volume Serial Number	96D9-B096
Sectors Per Cluster	8
Bytes Per Sector	512
Free Clusters	7248876
Total Clusters	10357247

Figure 10: Shows the C: drive and the allocated and unallocated space within it.

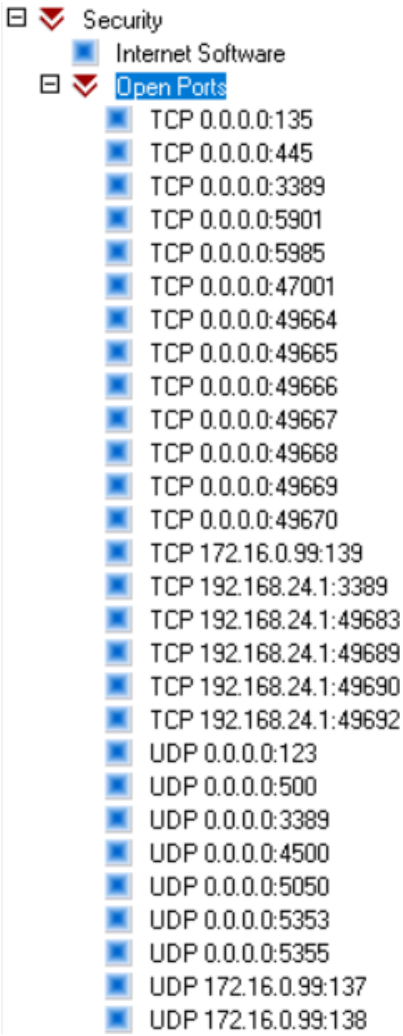


Figure 11: Shows a list of open ports on the machine. This is important because they allow communication between machines.

Windows Firewall

Name	Setting
Firewall Enabled	No
Authorised Service	File and Printer Sharing
Authorised Service	Network Discovery
Authorised Service	Remote Desktop

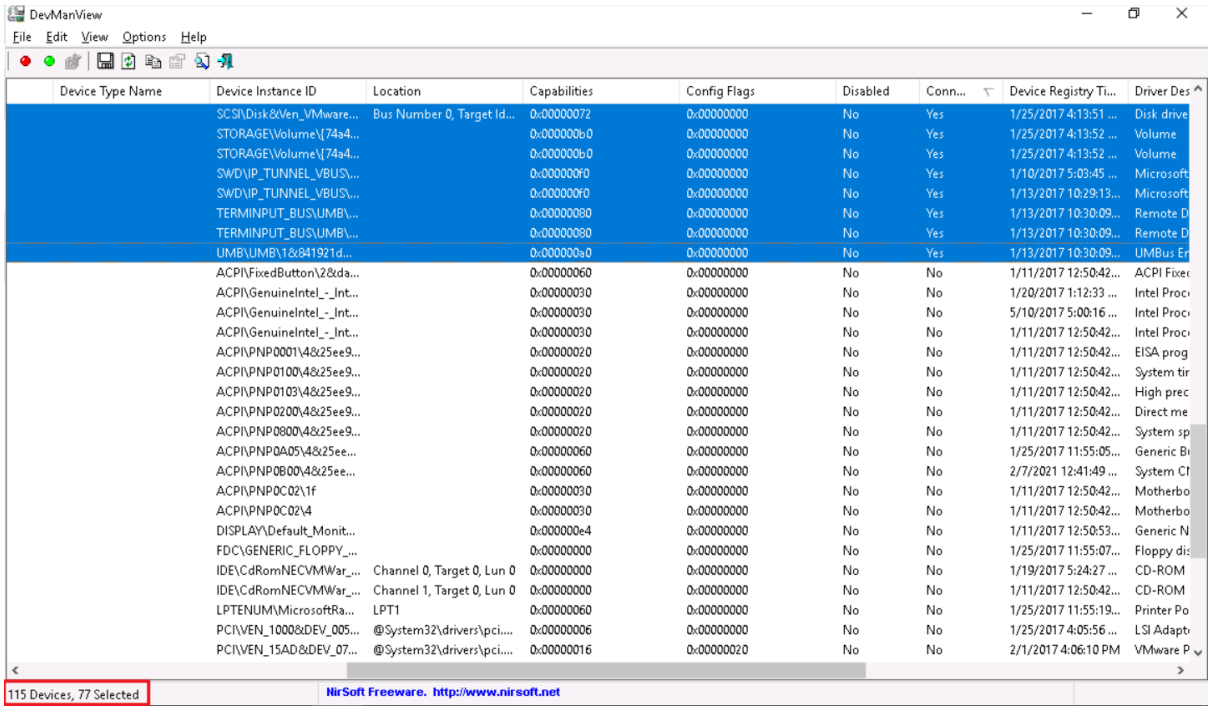
Figure 12: Shows the firewall settings. This is important because for this machine, the firewall is off.

2.2 Part 2: Use DevManView to Identify System Devices

For part 2, DevManView will be used to identify any devices that have been used by the machine. These is also a "registry," where the connections are timestamped and can be

used to match the time of a compromise. After launching DevManView, the following information was found:

- Total number of devices identified: 115
- Number of connected devices identified: 77



Device Type Name	Device Instance ID	Location	Capabilities	Config Flags	Disabled	Conn...	Device Registry Ti...	Driver Des
	SCSI\Disk&Ven_VMware...	Bus Number 0, Target Id...	0x00000072	0x00000000	No	Yes	1/25/2017 4:13:51 ...	Disk drive
	STORAGE\Volume\{74a4...		0x000000b0	0x00000000	No	Yes	1/25/2017 4:13:52 ...	Volume
	STORAGE\Volume\{74a4...		0x000000b0	0x00000000	No	Yes	1/25/2017 4:13:52 ...	Volume
	SWD\IP_TUNNEL_VBUS\...		0x000000f0	0x00000000	No	Yes	1/10/2017 5:03:45 ...	Microsoft
	SWD\IP_TUNNEL_VBUS\...		0x000000f0	0x00000000	No	Yes	1/13/2017 10:29:13...	Microsoft
	TERMINPUT_BUS\UMB\...		0x00000080	0x00000000	No	Yes	1/13/2017 10:30:09...	Remote D
	TERMINPUT_BUS\UMB\...		0x00000080	0x00000000	No	Yes	1/13/2017 10:30:09...	Remote D
	UMB\UMB\1&841921d...		0x000000a0	0x00000000	No	Yes	1/13/2017 10:30:09...	UMBus Er
	ACPI\FixedButton\2&da...		0x00000060	0x00000000	No	No	1/11/2017 12:50:42...	ACPI Fixe
	ACPI\GenuineIntel_-_Int...		0x00000030	0x00000000	No	No	1/20/2017 1:12:33 ...	Intel Proc
	ACPI\GenuineIntel_-_Int...		0x00000030	0x00000000	No	No	5/10/2017 5:00:16 ...	Intel Proc
	ACPI\GenuineIntel_-_Int...		0x00000030	0x00000000	No	No	1/11/2017 12:50:42...	Intel Proc
	ACPI\PNP0001\4&25ee9...		0x00000020	0x00000000	No	No	1/11/2017 12:50:42...	EISA prog
	ACPI\PNP0100\4&25ee9...		0x00000020	0x00000000	No	No	1/11/2017 12:50:42...	System tir
	ACPI\PNP0103\4&25ee9...		0x00000020	0x00000000	No	No	1/11/2017 12:50:42...	High prec
	ACPI\PNP0200\4&25ee9...		0x00000020	0x00000000	No	No	1/11/2017 12:50:42...	Direct me
	ACPI\PNP0800\4&25ee9...		0x00000020	0x00000000	No	No	1/11/2017 12:50:42...	System sp
	ACPI\PNP0A05\4&25ee...		0x00000060	0x00000000	No	No	1/25/2017 11:55:05...	Generic B
	ACPI\PNP0B00\4&25ee...		0x00000060	0x00000000	No	No	2/7/2021 12:41:49 ...	System Cl
	ACPI\PNP0C02\1f		0x00000030	0x00000000	No	No	1/11/2017 12:50:42...	Motherbo
	ACPI\PNP0C02\4		0x00000030	0x00000000	No	No	1/11/2017 12:50:42...	Motherbo
	DISPLAY\Default_Monit...		0x000000e4	0x00000000	No	No	1/11/2017 12:50:53...	Generic N
	FDC\GENERIC_FLOPPY_...		0x00000000	0x00000000	No	No	1/25/2017 11:55:07...	Floppy dis
	IDE\CdRomNECVMWar_...	Channel 0, Target 0, Lun 0	0x00000000	0x00000000	No	No	1/19/2017 5:24:27 ...	CD-ROM
	IDE\CdRomNECVMWar_...	Channel 1, Target 0, Lun 0	0x00000000	0x00000000	No	No	1/11/2017 12:50:42...	CD-ROM
	LPTENUM\MicrosoftRa...	LPT1	0x00000060	0x00000000	No	No	1/25/2017 11:55:19...	Printer Po
	PCI\VEN_1000&DEV_005...	@System32\drivers\pci....	0x00000006	0x00000000	No	No	1/25/2017 4:05:56 ...	LSI Adapt
	PCI\VEN_15AD&DEV_07...	@System32\drivers\pci....	0x00000016	0x00000020	No	No	2/1/2017 4:06:10 PM	VMware P

Figure 13: Shows the total devices and the number of connected devices.

Then, the NDIS Virtual Network Adapter was selected to view its properties. The following was found:

- Device Instance ID: `ROOT\NdisVirtualBus\0000`
- .inf File Name: `ndisvirtualbus.inf`

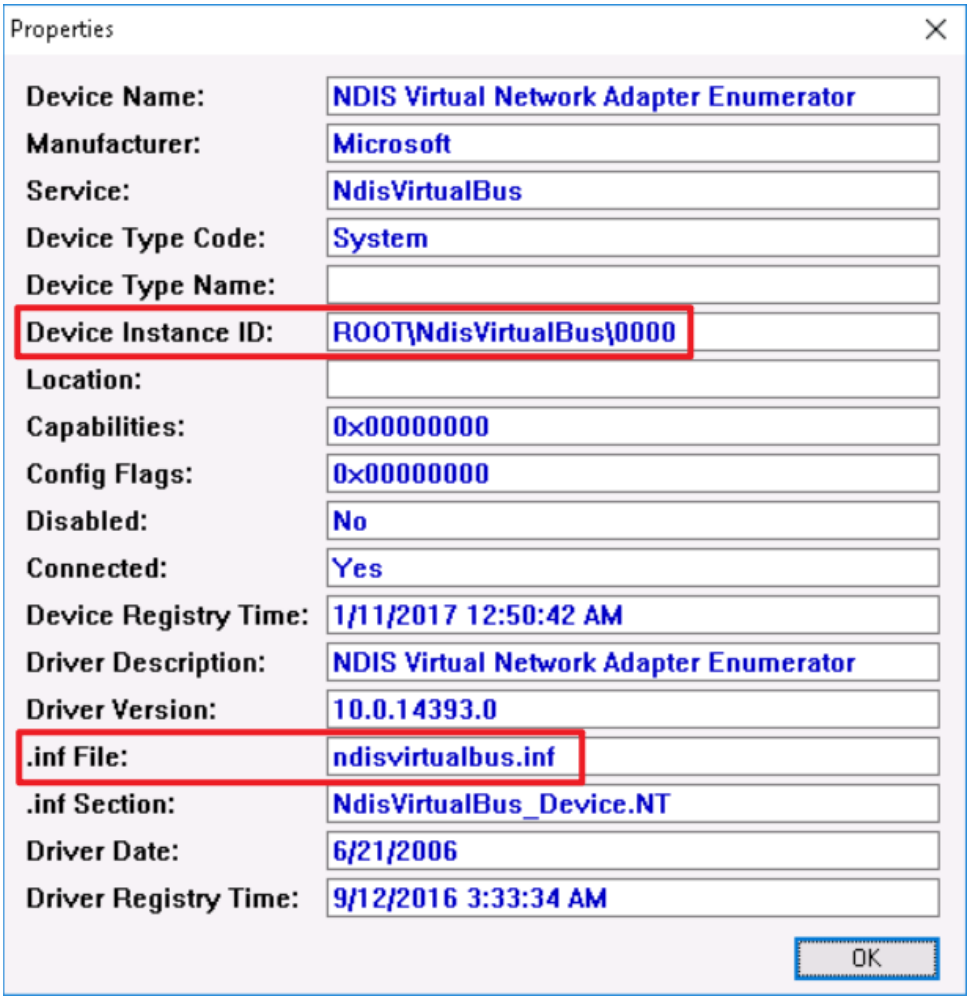


Figure 14: Properties for the NDIS Virtual Network Adapter.

2.3 Part 3: Use Frhed to perform a Byte-Level file analysis.

For part 3, Frhed will be used to identify an unknown file type. It will open the byte-level data, leaving us to search for clues that will lead to the correct file type.

```
øÿà..JFIF.....H.H..ÿá..Exif..II
*.............ÿá.yhttp://ns.adob
e.com/xap/1.0/.<?xpacket begin="
ï»¿" id="W5M0MpCehiHzreSzNTczkc9
d"?> <x:xmpmeta xmlns:x="adobe:n
s:meta/" x:xmptk="Adobe XMP Core
 5.3-c011 66.145661, 2012/02/06-
14:56:27        "> <rdf:RDF xmln
s:rdf="http://www.w3.org/1999/02
/22-rdf-syntax-ns#"> <rdf:Descri
ption rdf:about="" xmlns:xmpRigh
ts="http://ns.adobe.com/xap/1.0/
rights/" xmlns:xmp="http://ns.ad
obe.com/xap/1.0/" xmlns:xmpMM="h
ttp://ns.adobe.com/xap/1.0/mm/"
xmlns:stRef="http://ns.adobe.com
/xap/1.0/sType/ResourceRef#" xmp
Rights:Marked="True" xmp:Creator
Tool="Adobe Photoshop CS6 (windo
ws)" xmpMM:InstanceID="xmp.iid:F
C5075BE2F0C11E4A9D5FAA3C8491F3B"
 xmpMM:DocumentID="xmp.did:FC507
5BF2F0C11E4A9D5FAA3C8491F3B"> <x
mpMM:DerivedFrom stRef:instanceI
D="xmp.iid:FC5075BC2F0C11E4A9D5F
AA3C8491F3B" stRef:documentID="x
mp.did:FC5075BD2F0C11E4A9D5FAA3C
8491F3B"/> </rdf:Description> </
rdf:RDF> </x:xmpmeta> <?xpacket
end="r"?>ÿ0.C...................
.................................
.....  ".."....ÿ0.C..............
```


Figure 15: Shows 'xmp' being used multiple times.

While searching through the data, we found "xmp" to be the file type. After identifying the file type, the original file was renamed with the correct extension and we used Paint to open it.

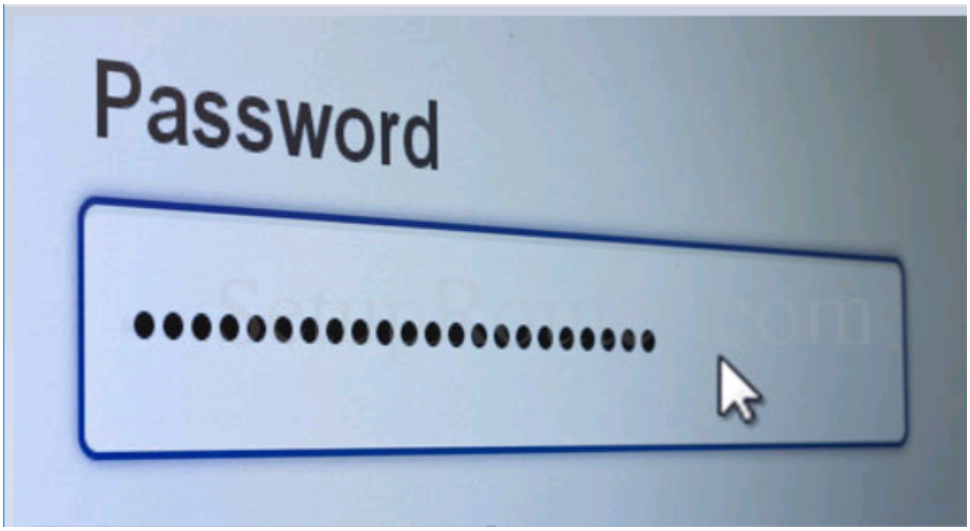


Figure 16: Shows contents of the file.

3 Conclusion

While performing this lab, we learned about and how to use three different forensics tools: WinAudit, DevManView, and Frhed. With WinAudit, we learned how to perform the audit and see what types of information comes up on the report. With DevmanView, we saw how it lists all devices that have or had been connected to the machine. The multiple columns (ex: Connected?) within the results makes it easy to identify what you are looking for. Fhred was the tool that required more attention to find what we needed. After reading through what was intelligible, we determined the file type. Overall, this lab taught us beginners knowledge and how to navigate between the different tools that are frequently used as a digital forensics specialist.