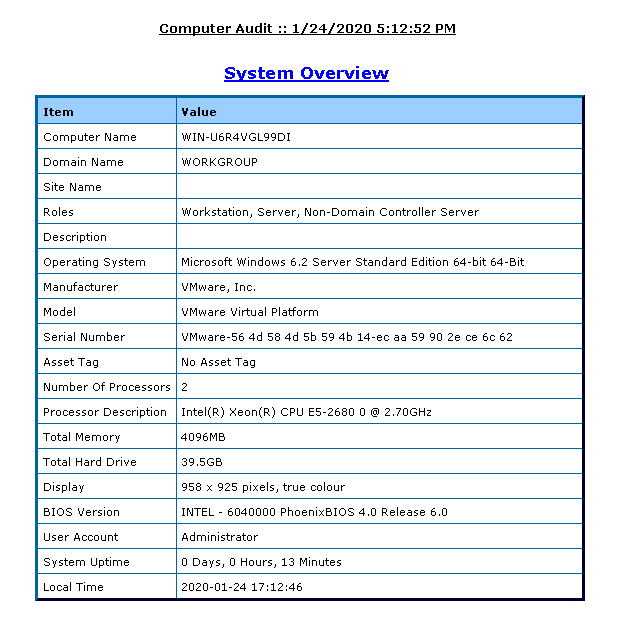
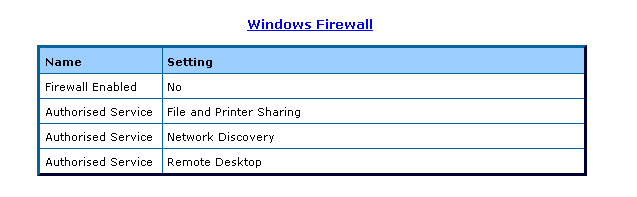
Section 1

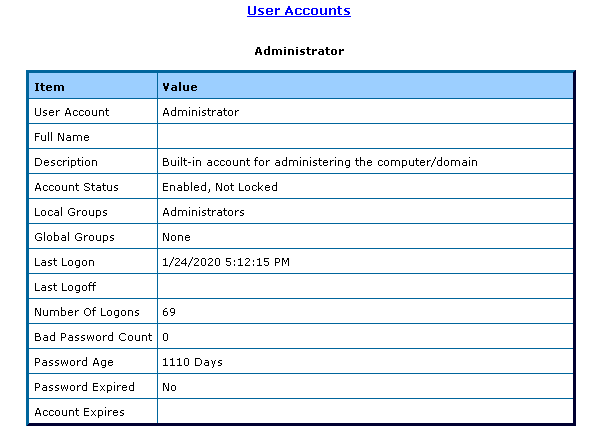
System Overview



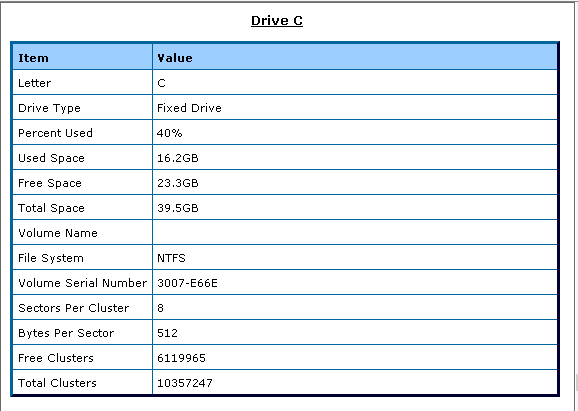
Windows firewall



User account

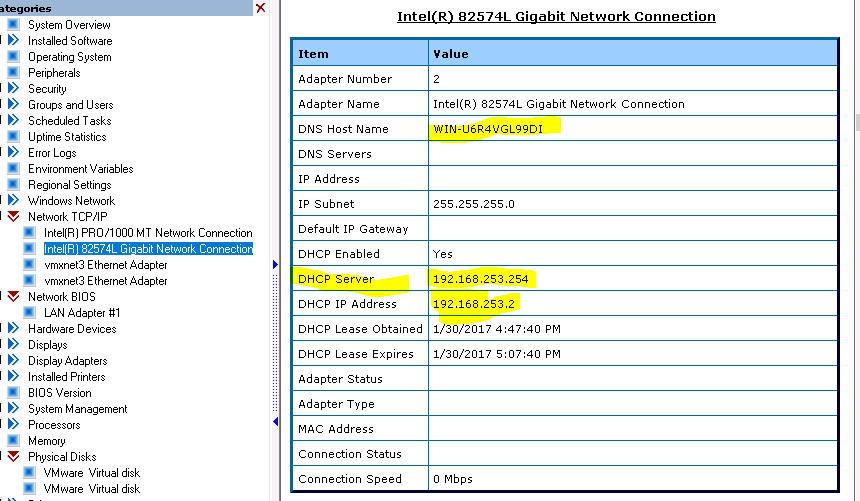


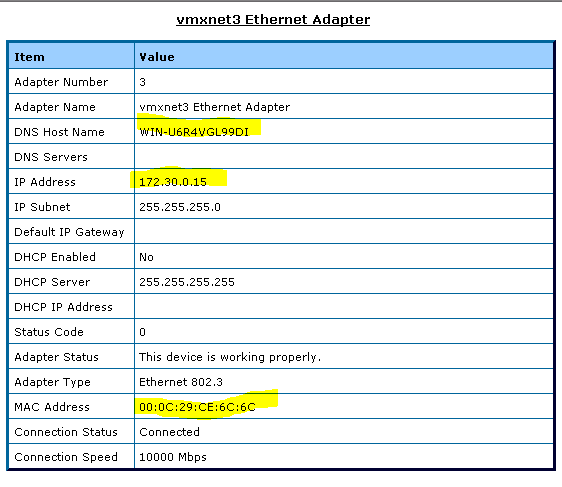
C drive

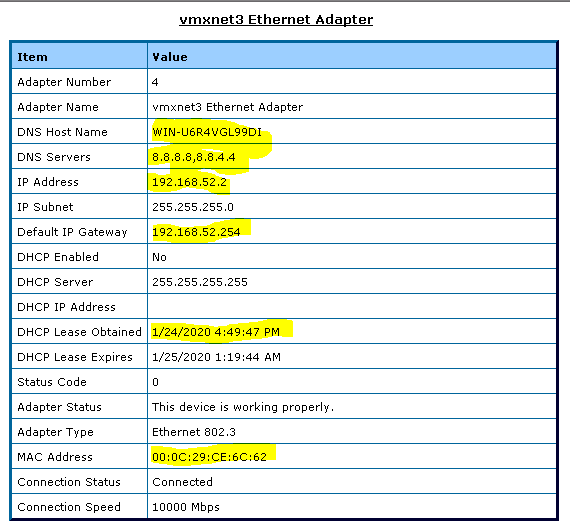


Other winAudit info.

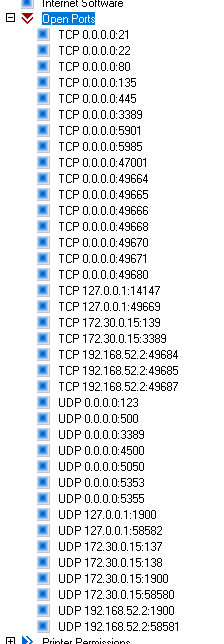
Network related info like IP,DHCP server, and DNS names found on this machine.



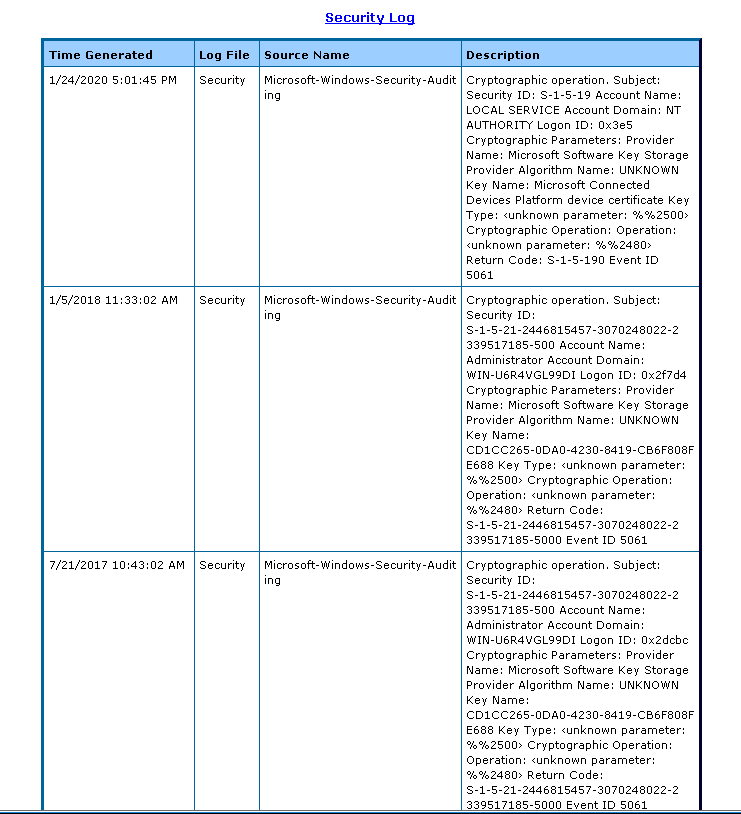




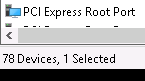
List of open ports.



Security log



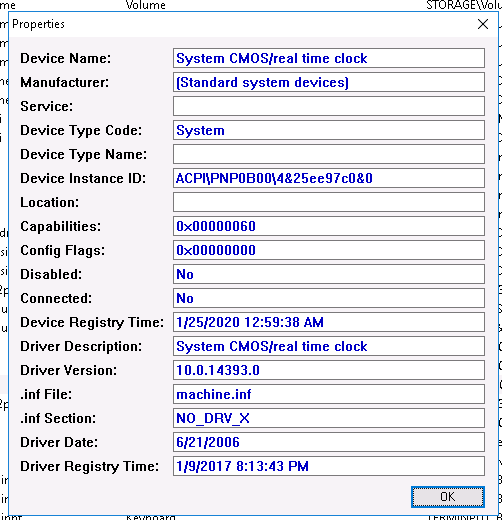
Number of devices In DevManView



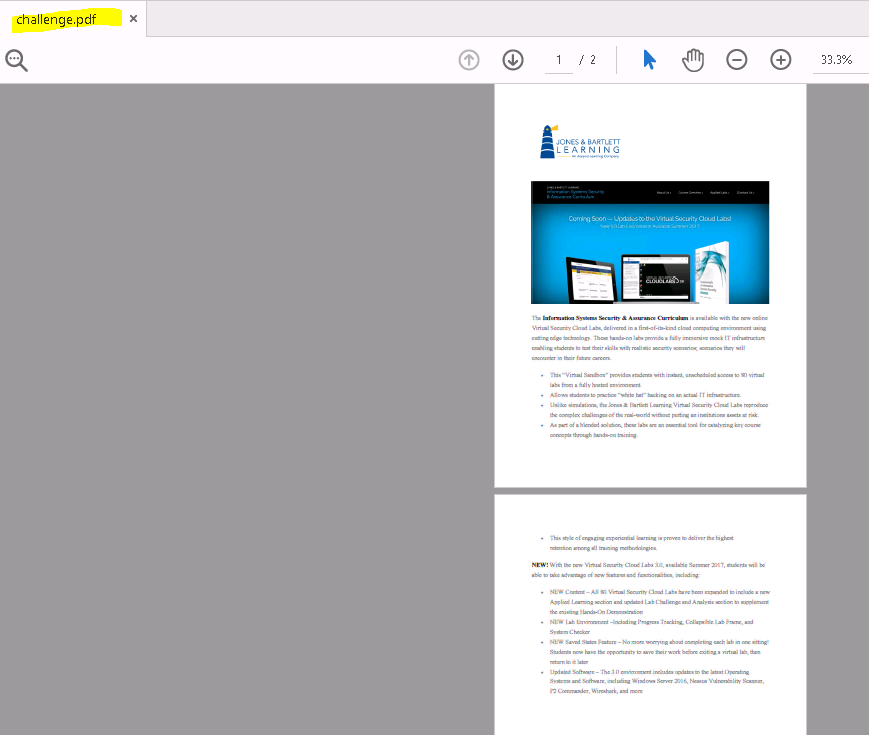
Number of devices in DevManView after toggling select only connected devices.



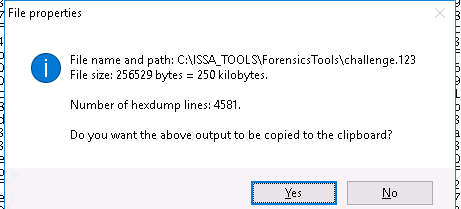
System CMOS/real time clock properties.



Challenge pdf file.

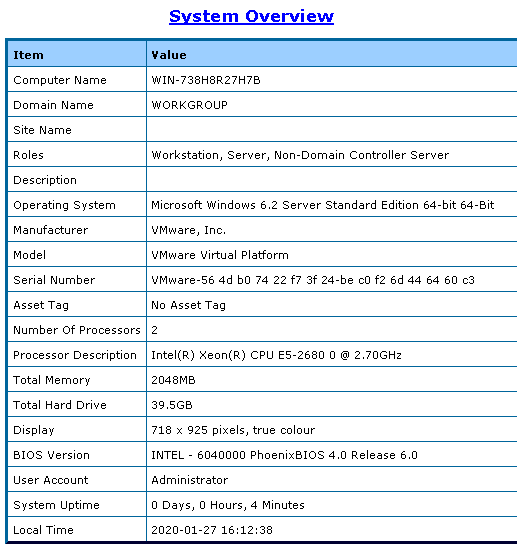


File properties

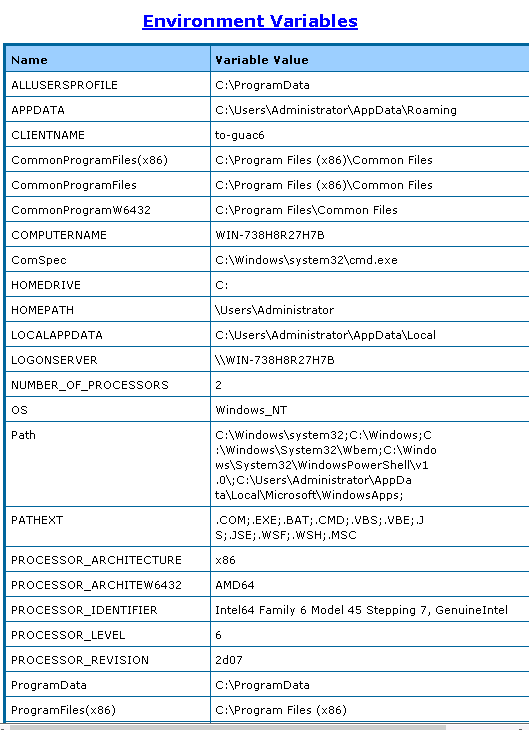


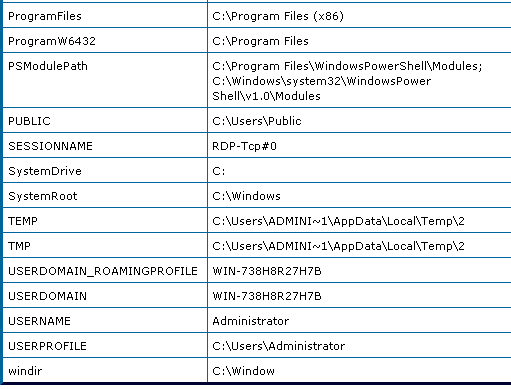
Section2

System overview

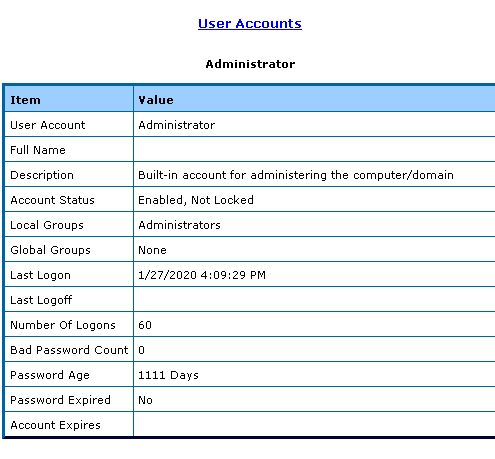


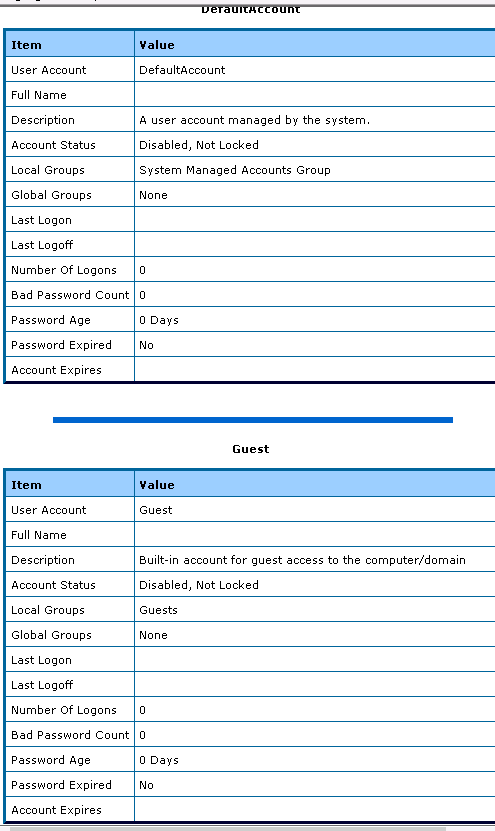
Environment variables



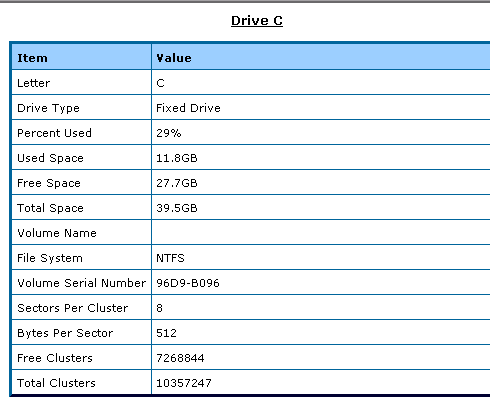


User accounts



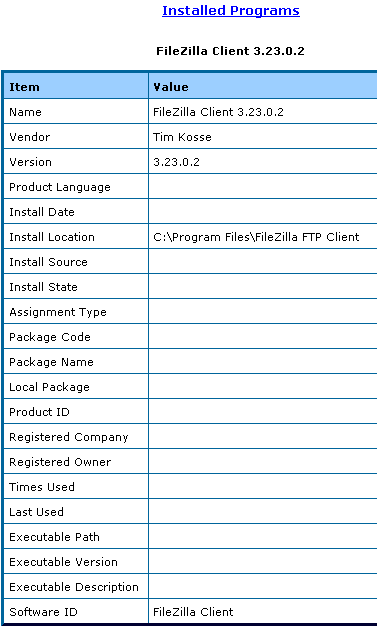


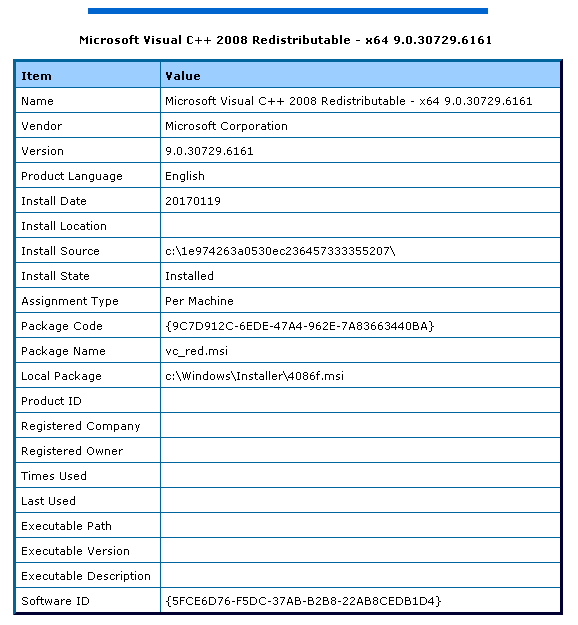
Drive C

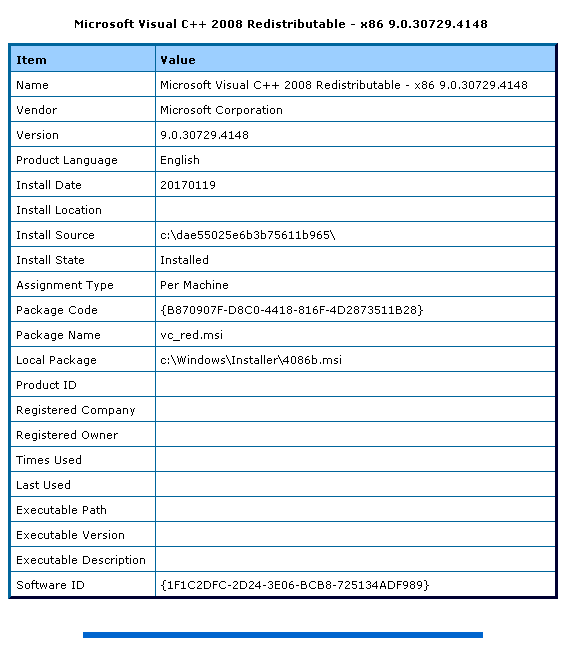


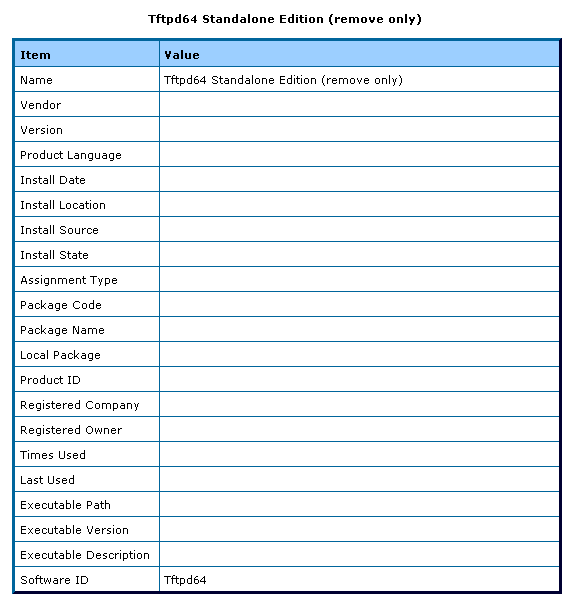
Other WinAudit findings.

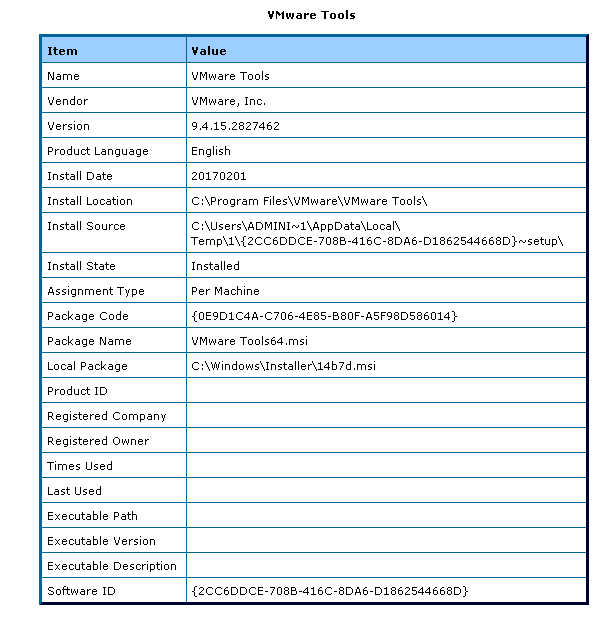
Installed software (Good to know what was running on system.)

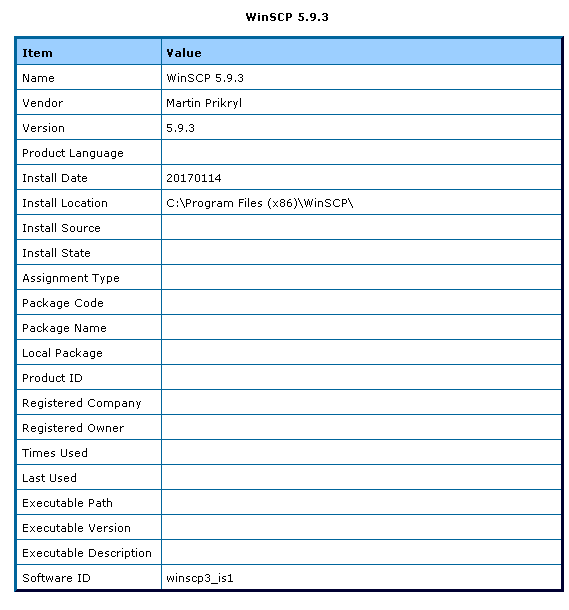




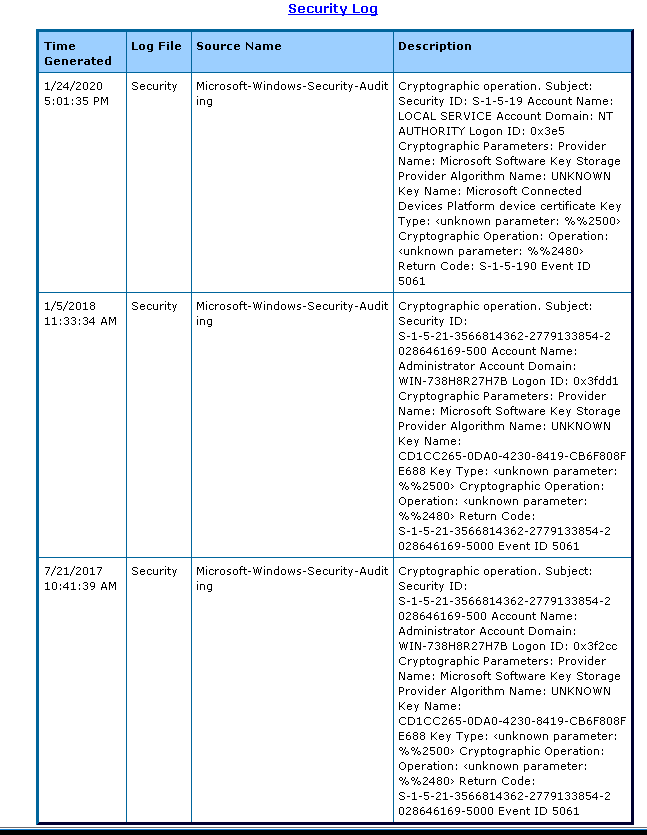


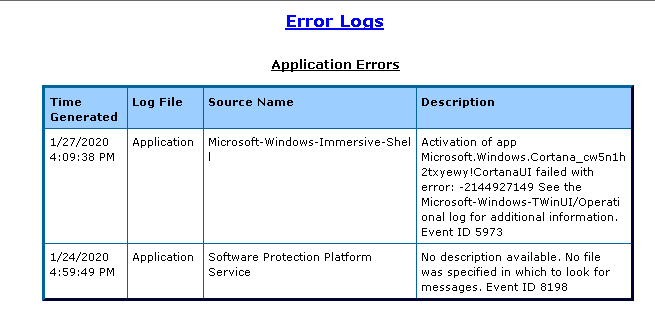


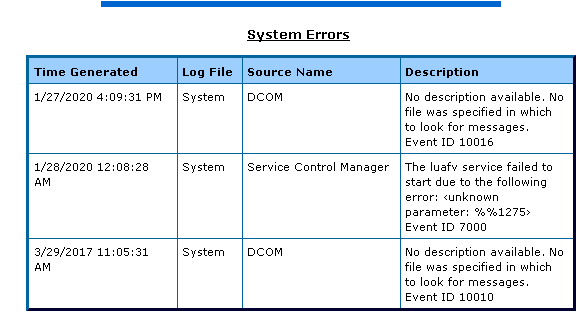




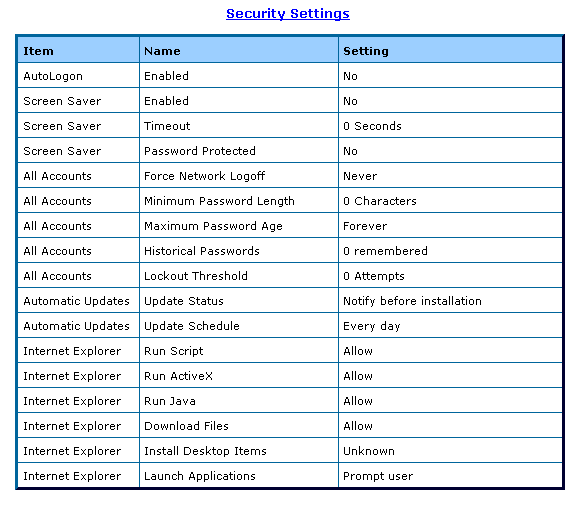
Security log



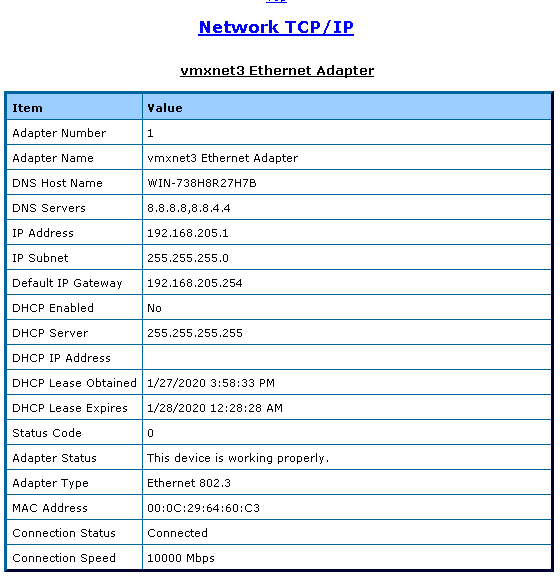


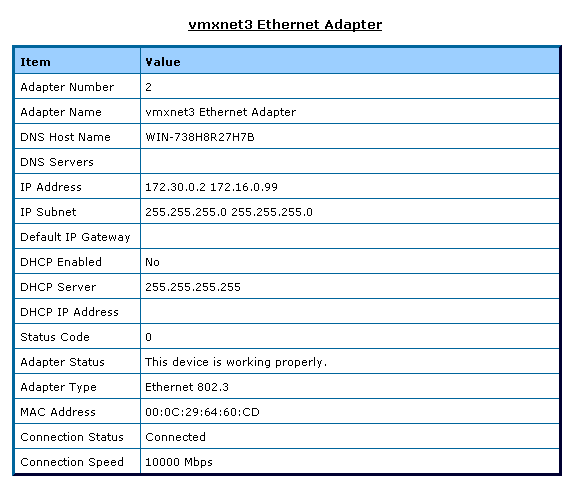


Security settings. ( See what services and settings were allowed.)

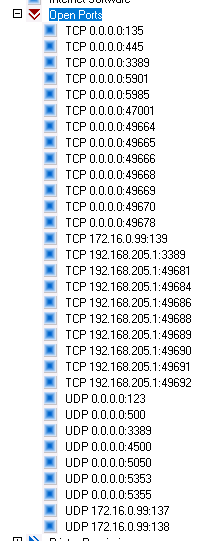


Network info(Good for tracing MAC address and IP)





Open ports (What ports were able to communicate)



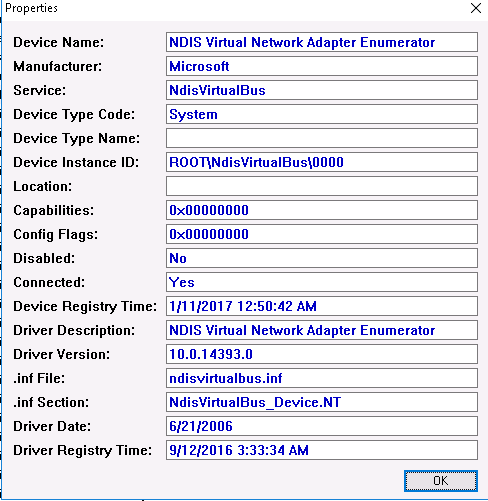
Dev man view devices



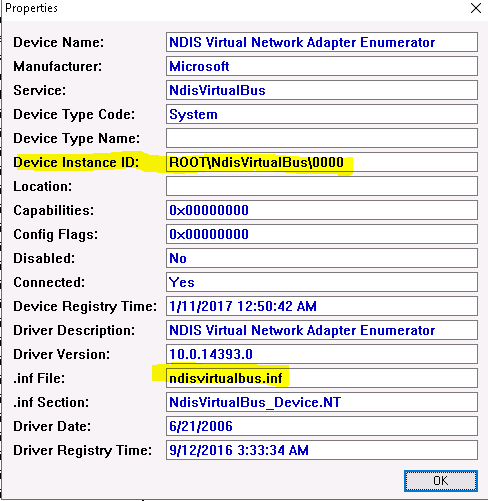
Dev man view connected devices



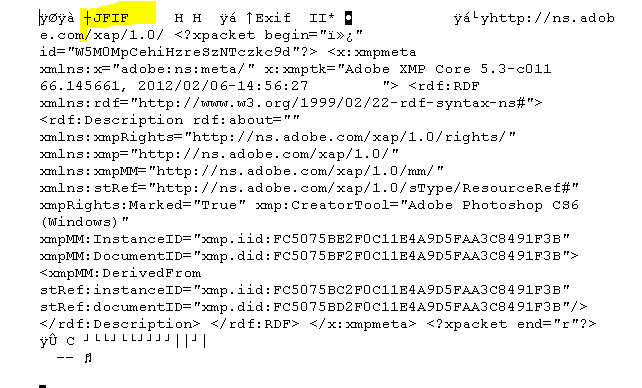
NDIS virtual network adapter enumerator properties.



Device instance ID and .INF file name.



Hint that identifies the correct file type. (jfif)



Target file as JFIF



Explain why it is important to use tools like WinAudit, DevManView, and Frhert?

It is important to use these tools because the automate the forensics process and can also be used to dive deeper into your analysis.

WinAudit gives a quick overview / audit of the data at hand.

DevManView allows you to quickly view the device manager and its contents.

Frhert allows you to look at data in its hexadecimal form, allowing you to dive deeper than the surface level into your investigation.

