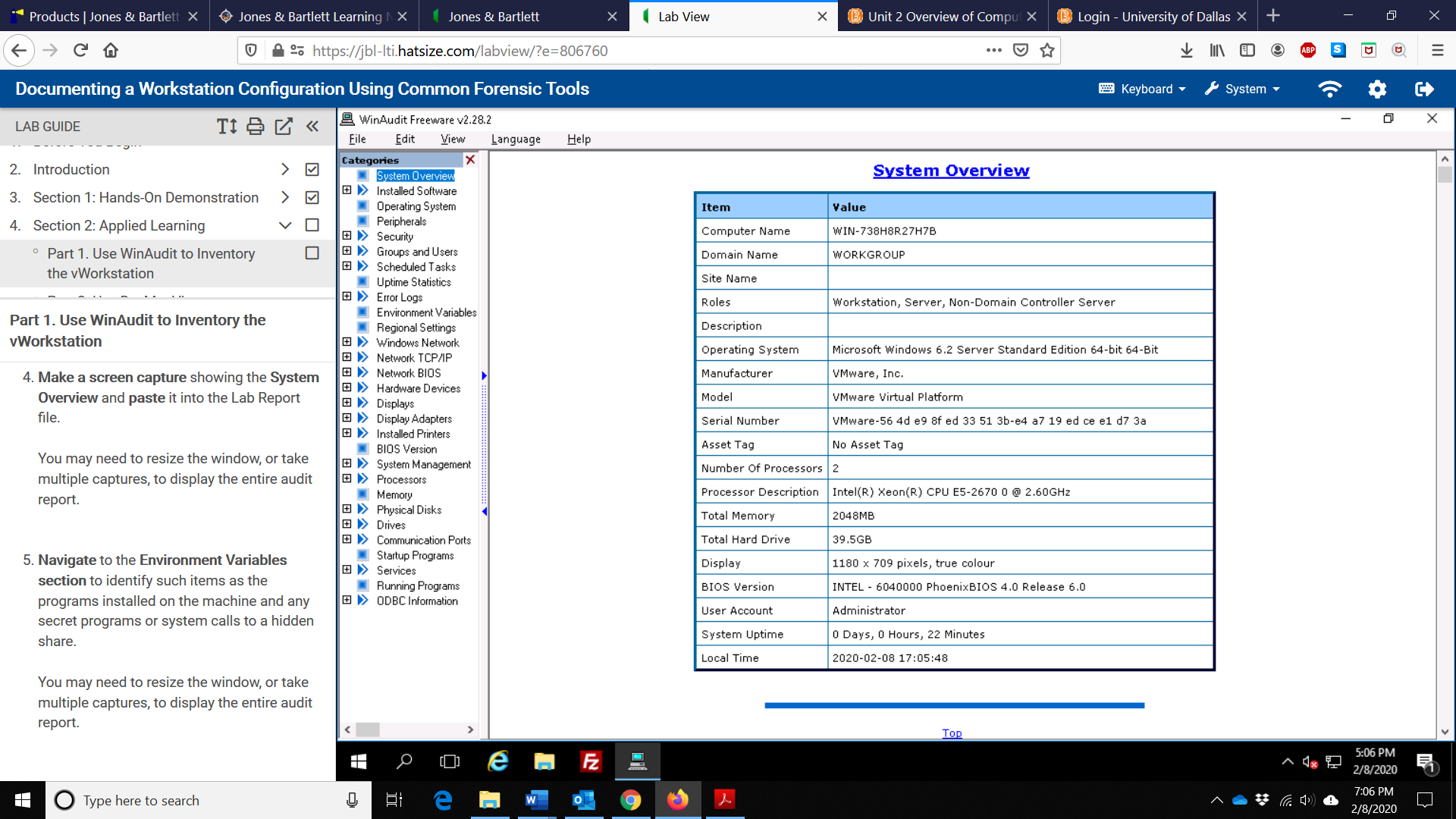
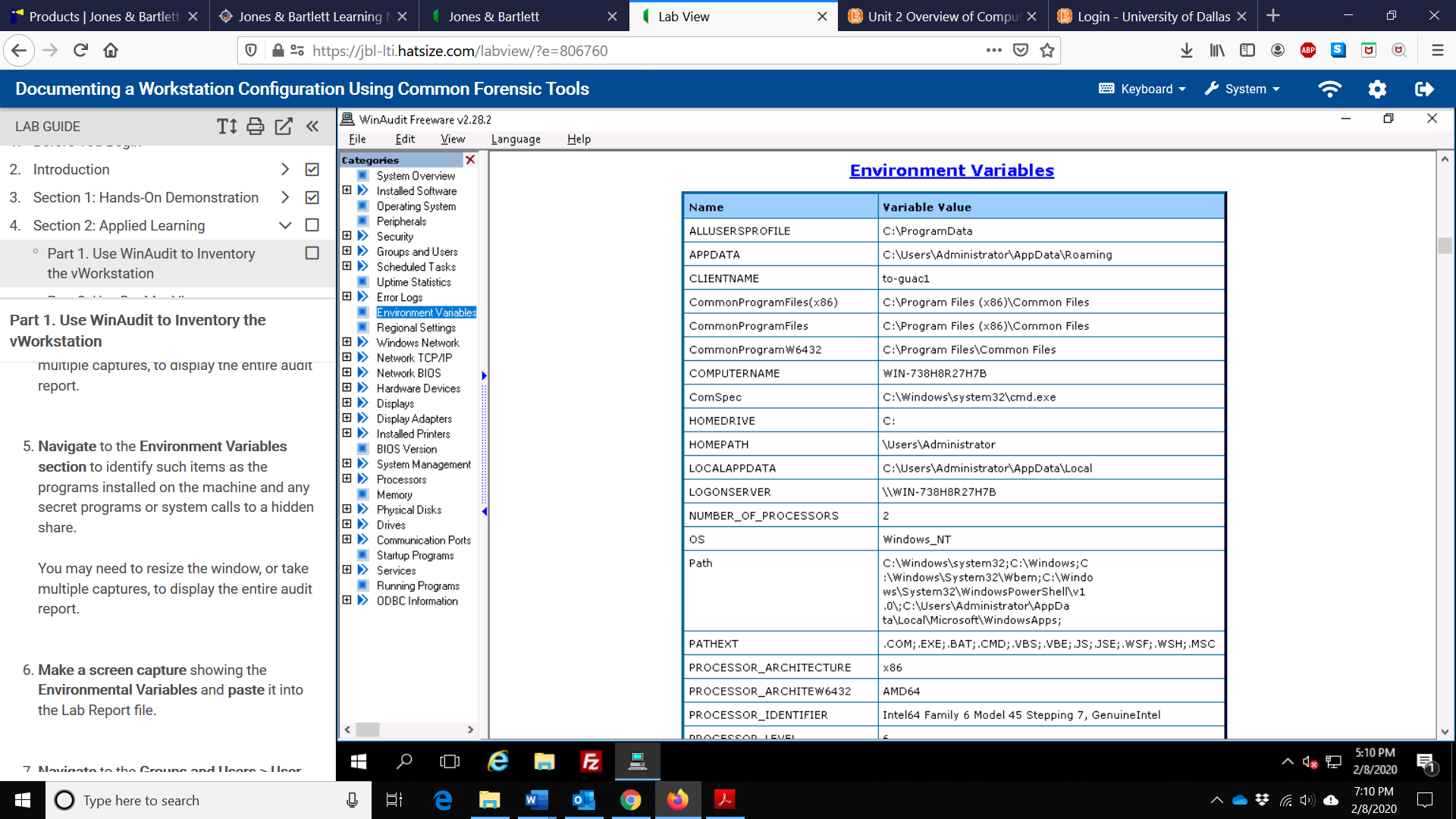
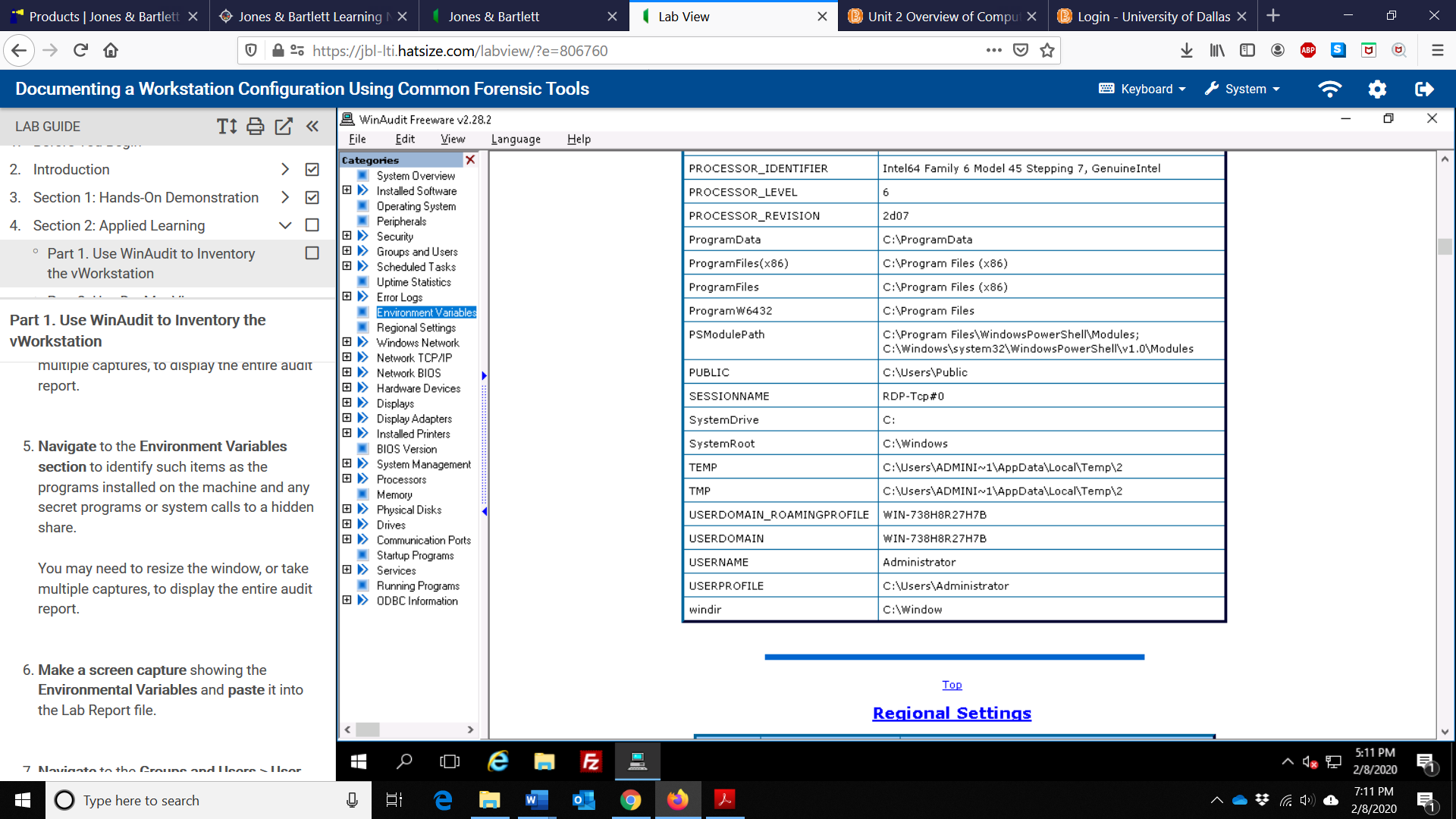
**Section 2**

1. Make a screen capture showing the system overview and paste it into the Lab Report file.



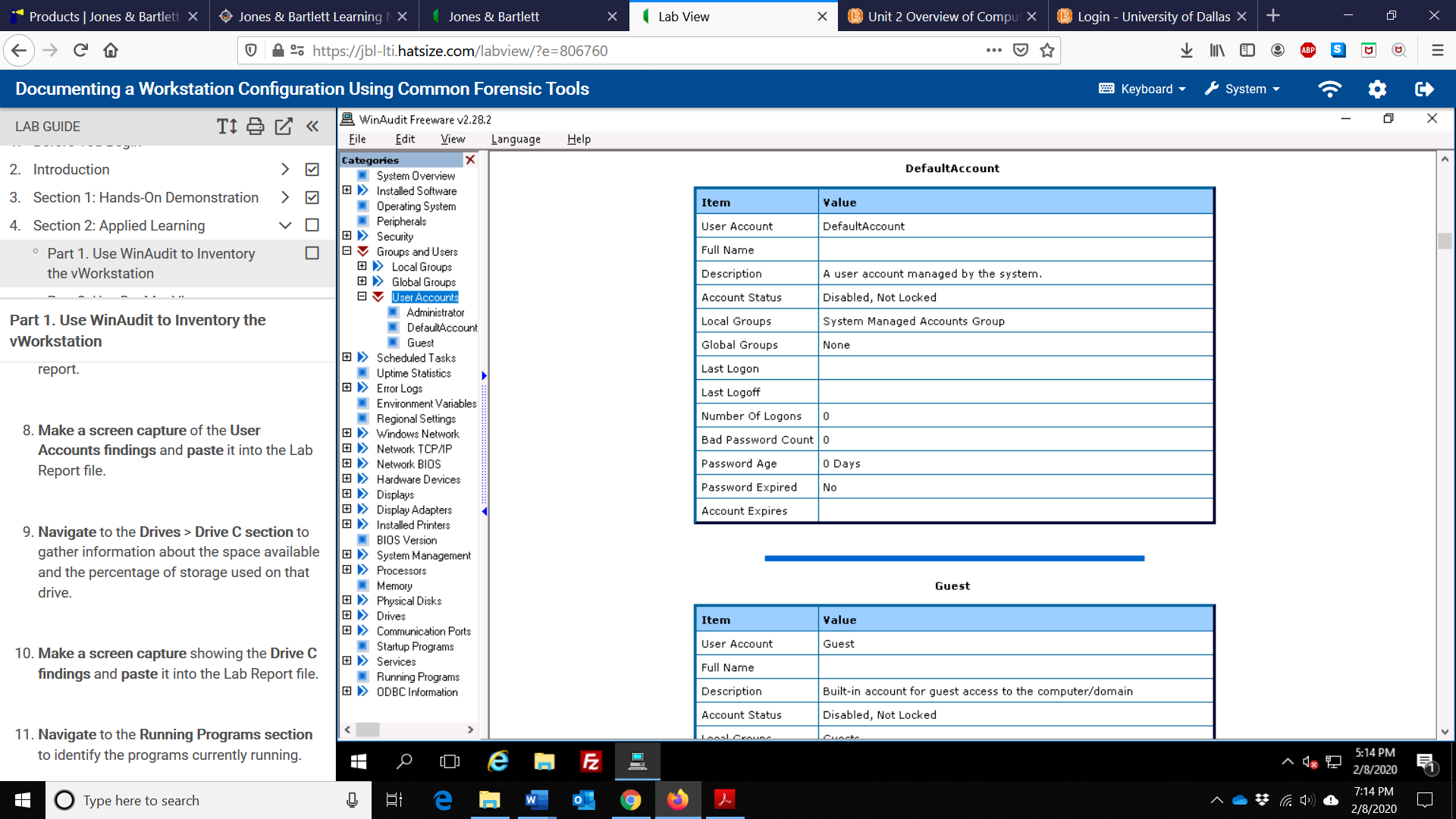
1. Make a screen capture showing the environmental variables and paste it into your Lab Report file.

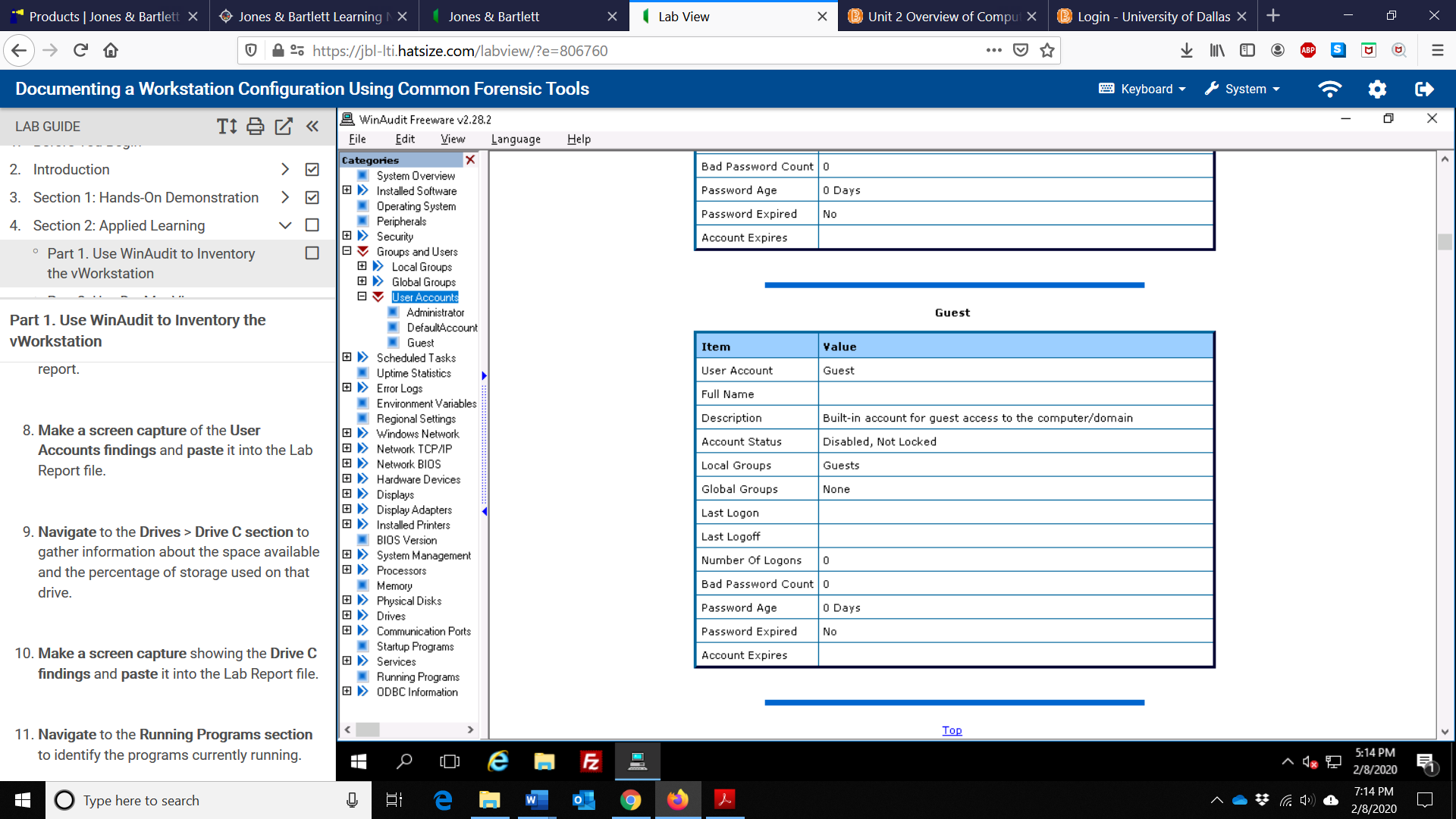




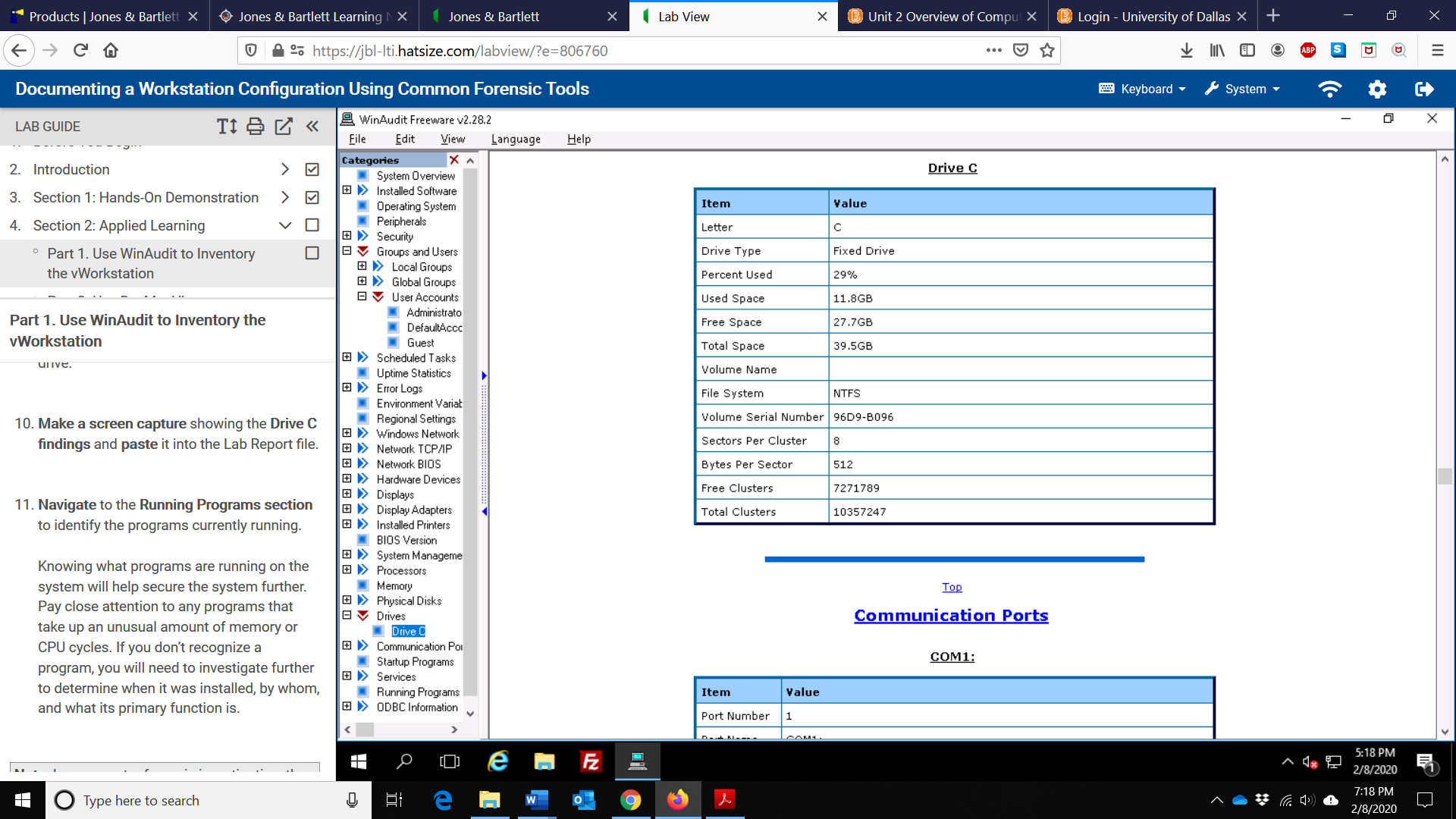
1. Make a screen capture of the User Account findings and paste it into the La Report file.



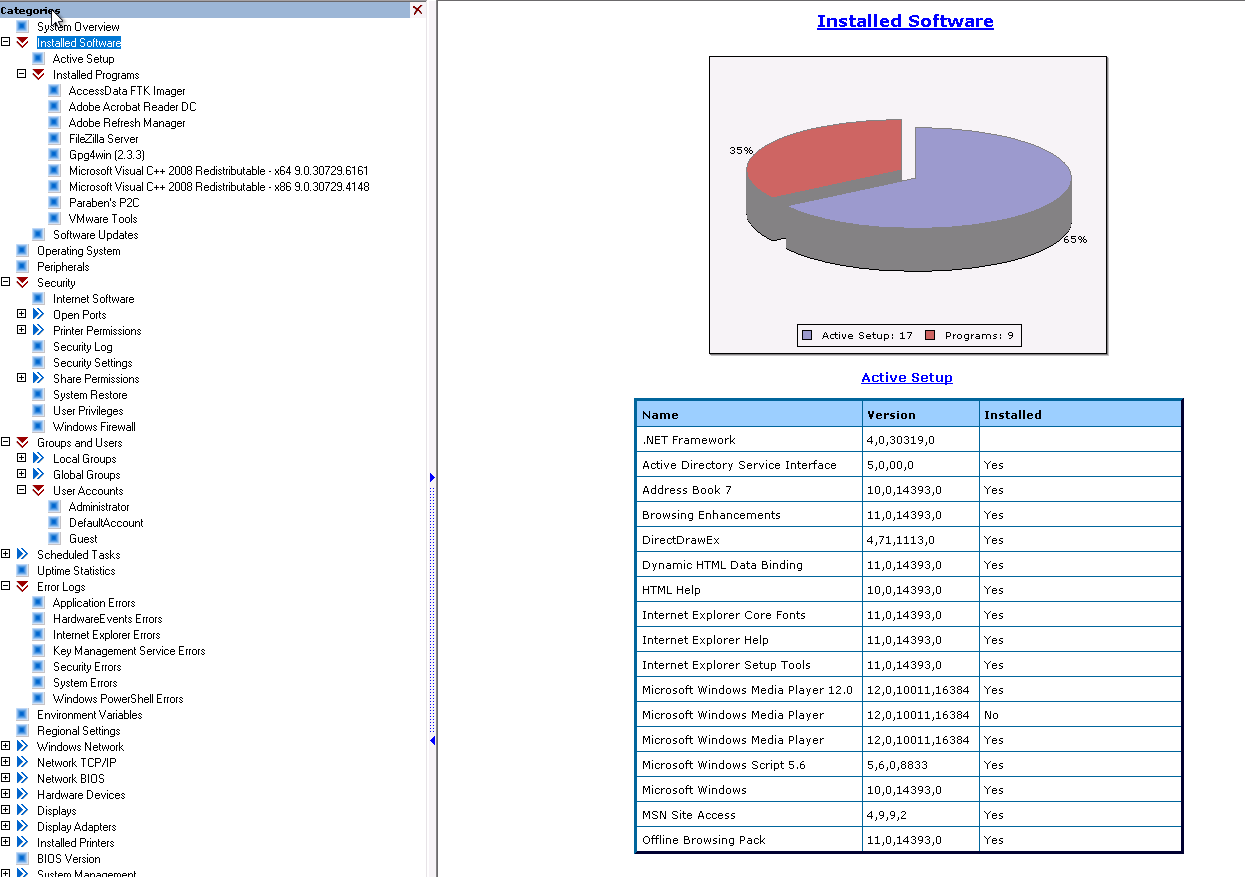


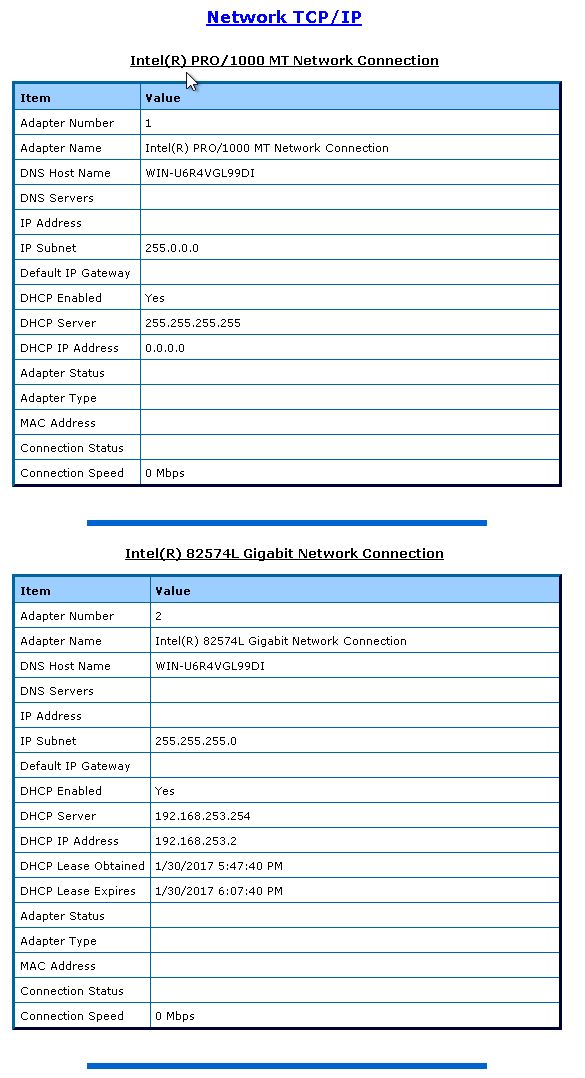


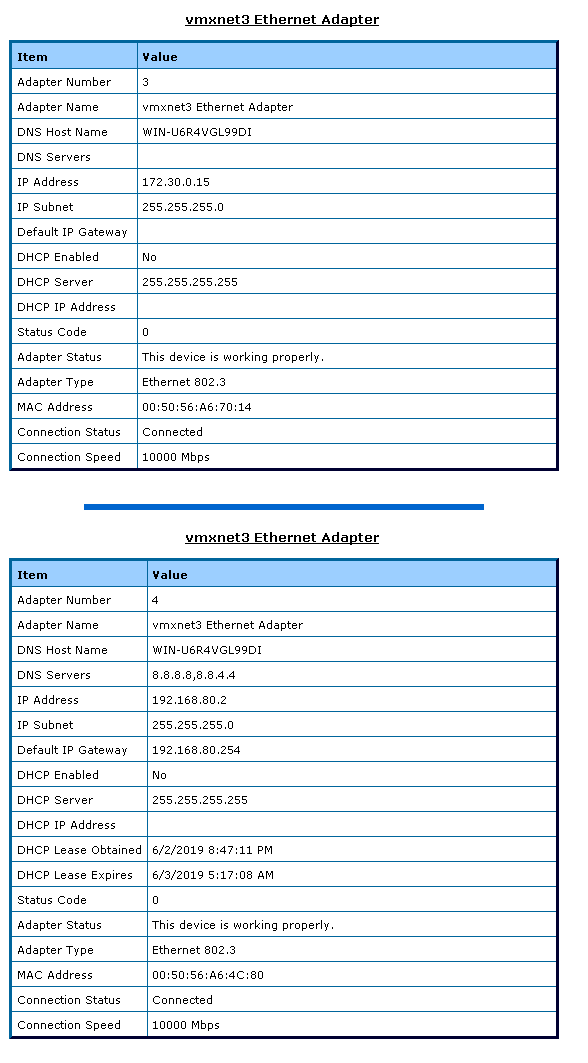
1. Make a screen capture showing the Drive C findings and paste it into the Lab Report file.



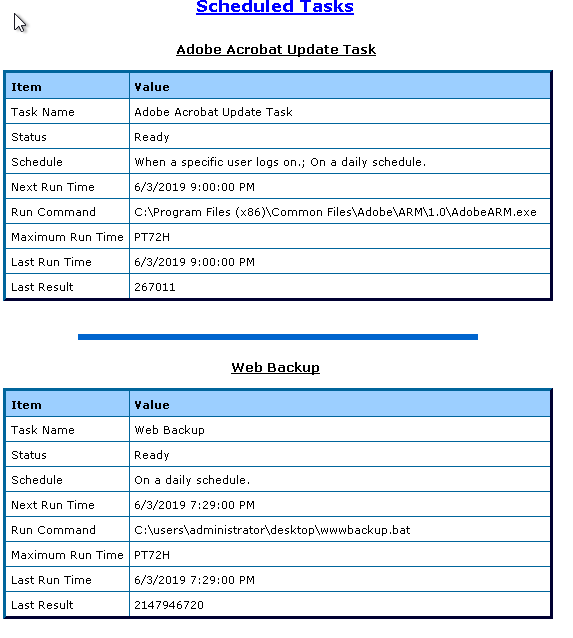
1. Make a screen capture showing any other WinAudit findings that you feel are critically important to a forensic investigation and paste them into the Report file.





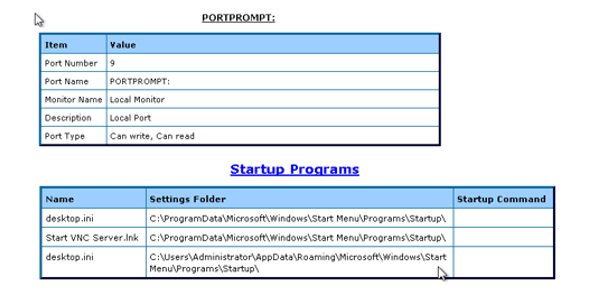


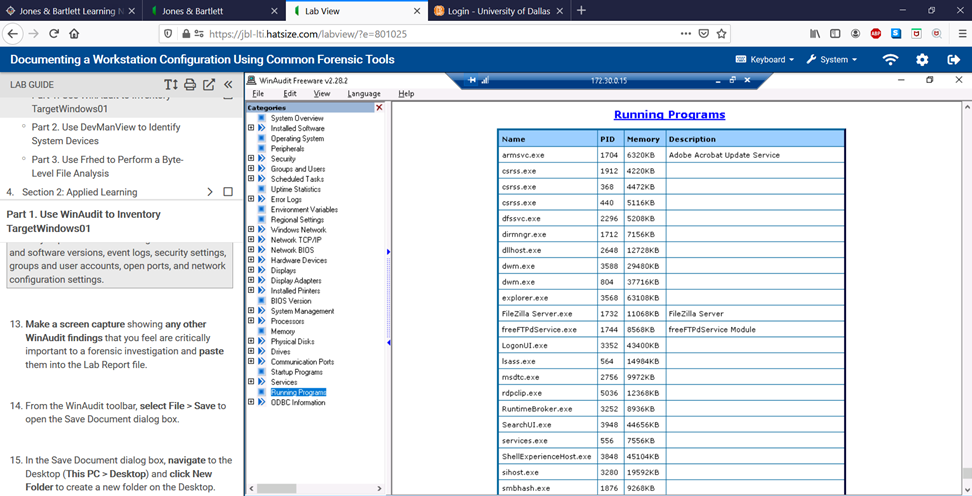


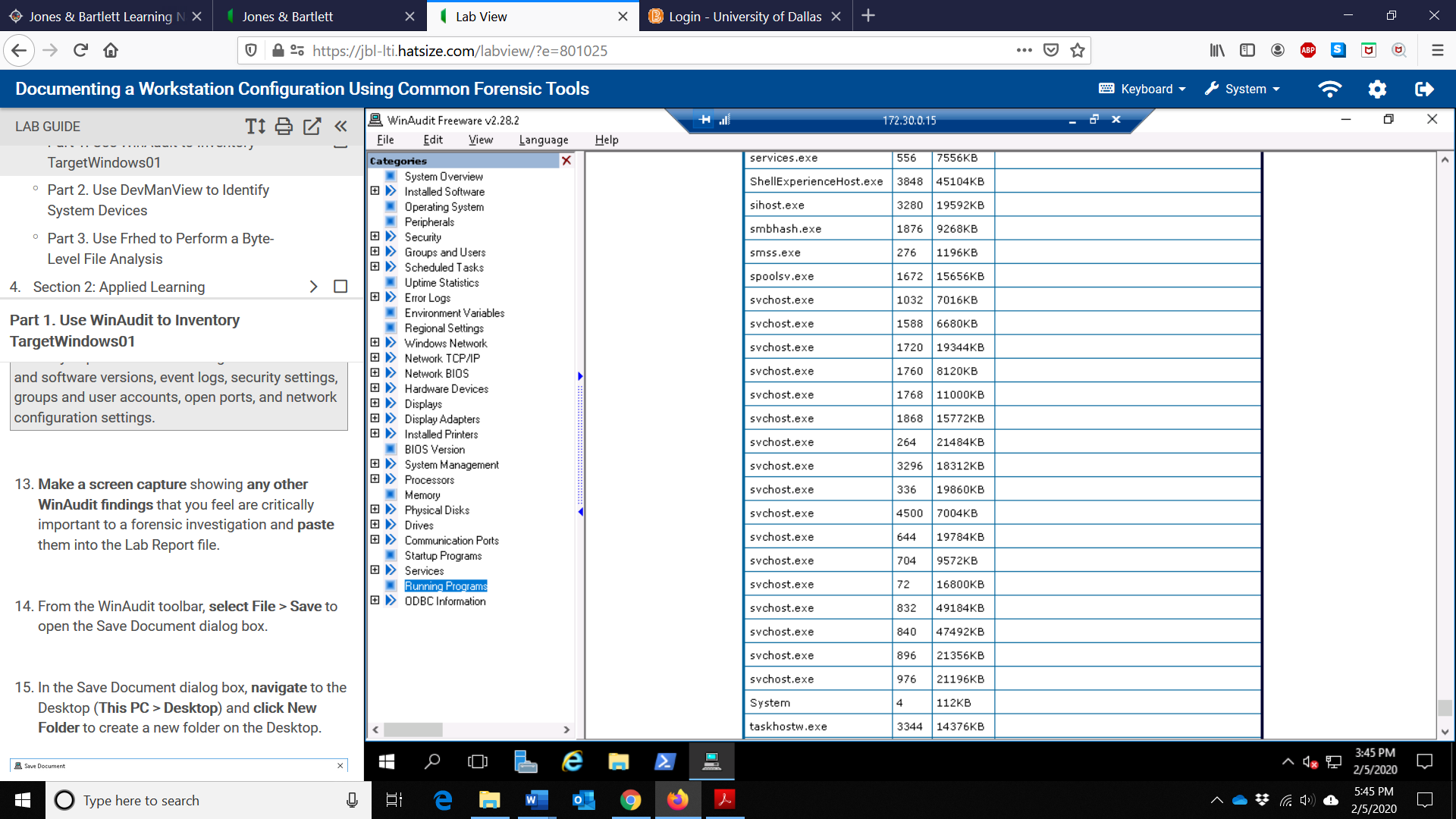


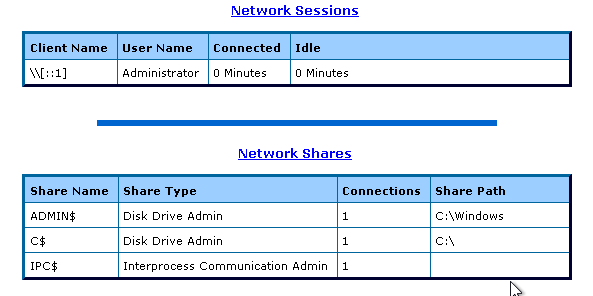
A screenshot of a social media post

Description automatically generated



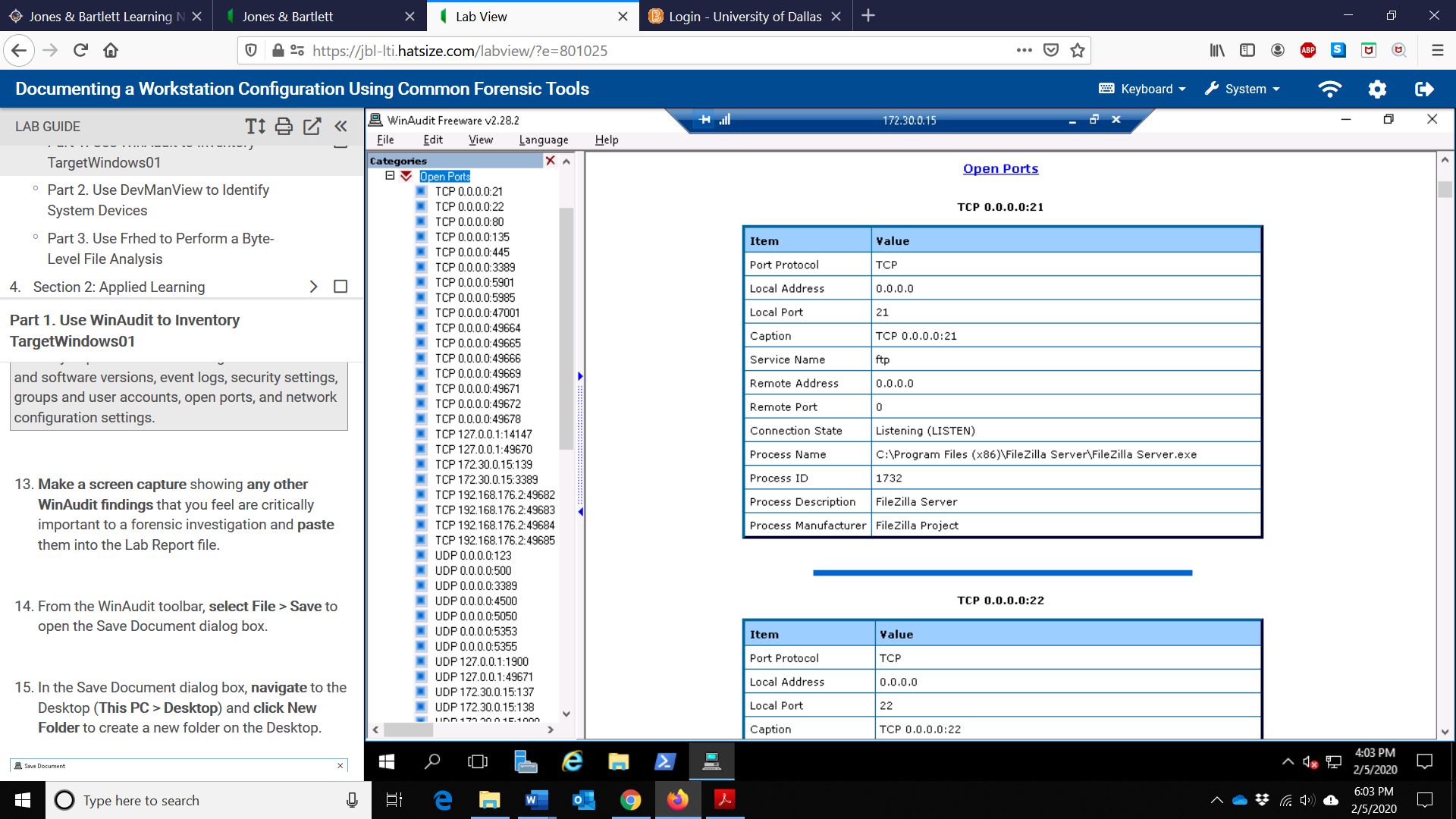






A screenshot of a social media post

Description automatically generated



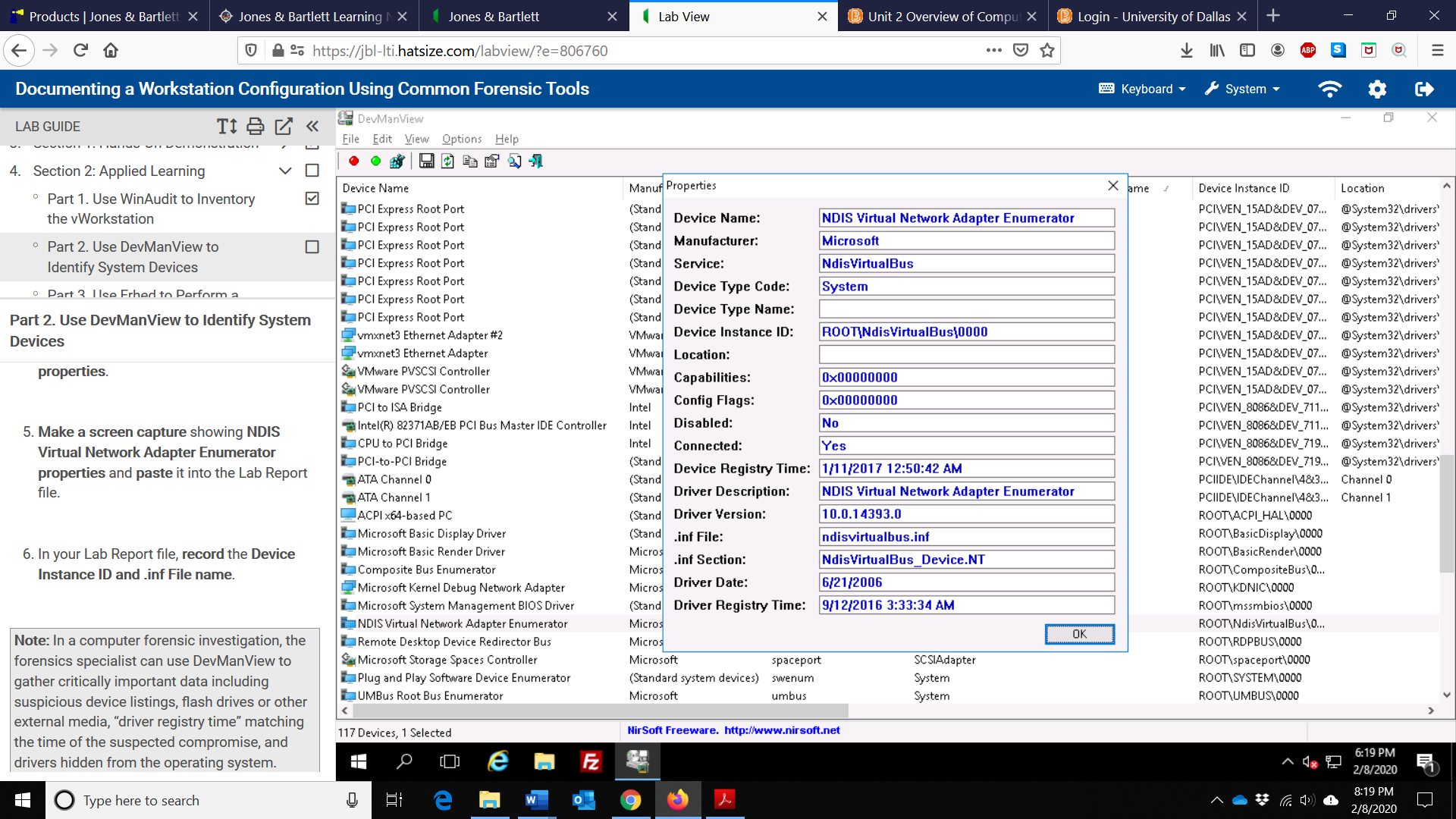
A screenshot of a computer

Description automatically generated

1. In the Lab Report file, explain why you chose to include the information you collected.

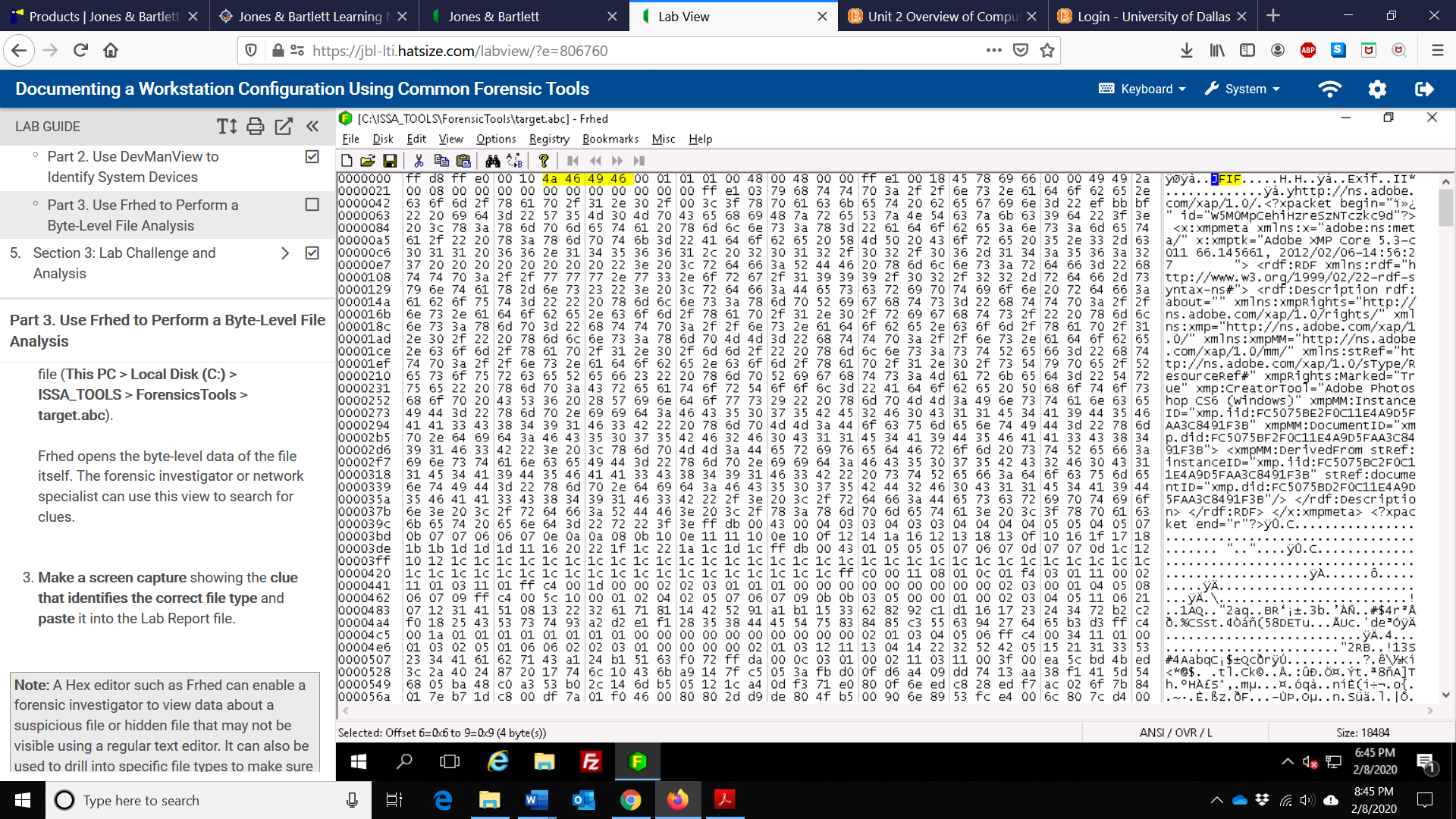
I chose to include the information I collected above in the forensic investigation due to the following reasons:

1. Startup Programs determine if there are any suspicious scripts or programs run that run automatically during the boot of a Windows machine.
2. Network Session and Shares determine any suspicious users establishing sessions over the network as well as shares that they're not supposed to have (resource on a local network that can be accessed by them).
3. Running programs help identify any suspicious programs with high resource usage.
4. Scheduled Tasks help identify any suspicious tasks automatically scheduled to start on Windows for any correlation.
5. Network/TCPIP helps understand all network connections to the machine and the related IP addresses.
6. Communication port will also give an understanding of how the interaction between various devices was possible.
7. Installed Software to audit software helps identify any suspiciously named or owned software in order to carry out further investigation on it.
8. OS details help identify the behavior of the computer and any suspicious activity that can occur due to the vulnerabilities of the OS.
9. Open ports give an idea of any vulnerabilities at specific ports that were exploited to execute a malicious action.
10. Hardware devices and peripherals allow us to gather information on how a suspicious activity occurred using physical objects. These objects will also need to be documented.
11. Make a screen capture showing NDIS Virtual Network Adapter Enumerator properties and paste it into the Lab Report file.

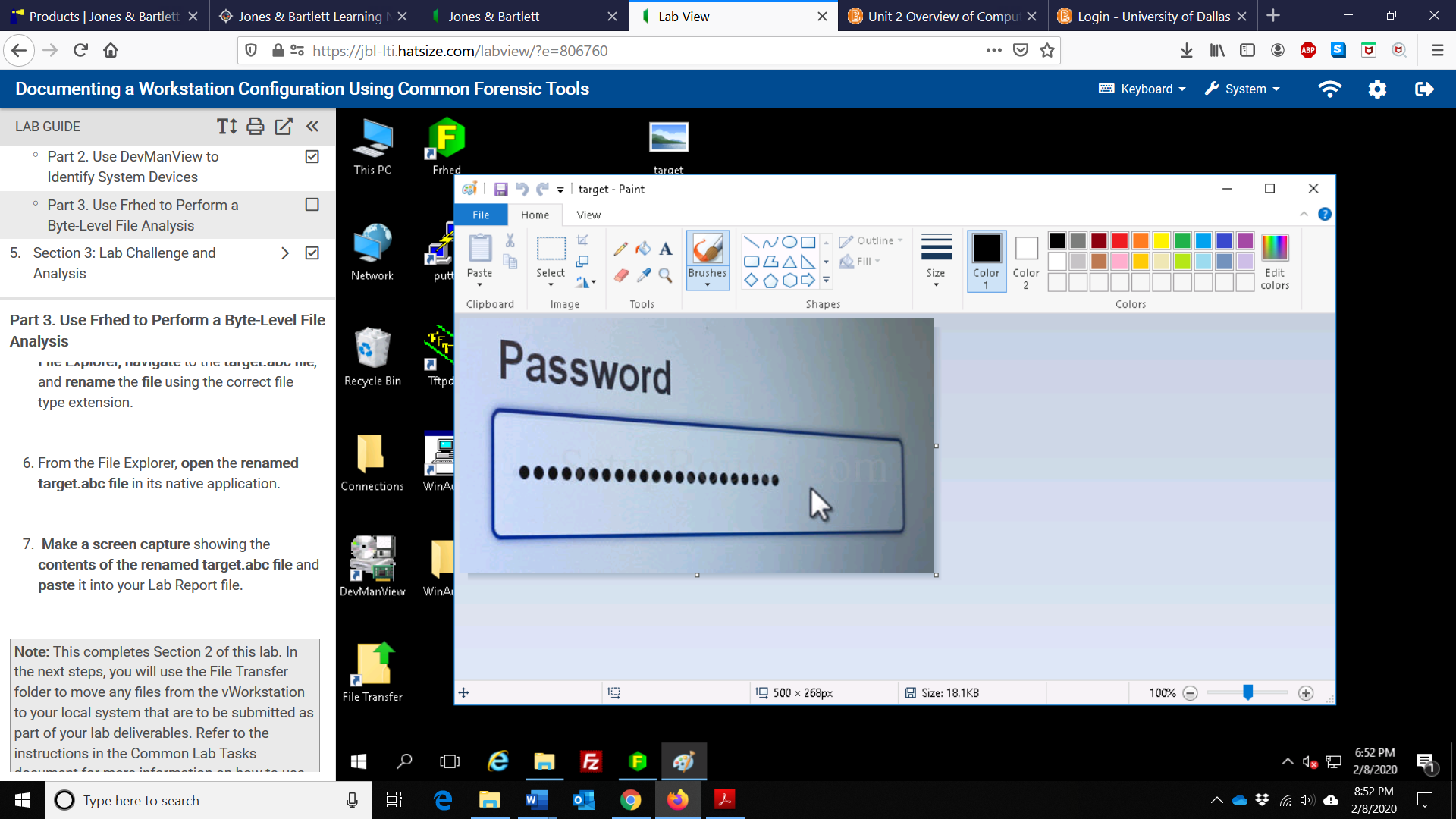


1. Make a screen capture showing rh clue that identifies the correct file type and paste it into the Lab Report file.

* The file header JFIF represents JPEG File Interchange Format (JFIF) which is the .jpeg file format standard



1. Make a screen capture showing the contents of the renames target.abc file and paste it into you Lab Report file.



Any additional information as directed by the lab:

The number of connected devices identified by DevManView: 77

The total number of devices identified by DevManView: 117

NDIS Virtual Network Adapter Enumerator Device Instance ID and .inf File name: ROOT\NdisVirtualBus\0000 and ndisvirtualbus.inf