Jackson Warren

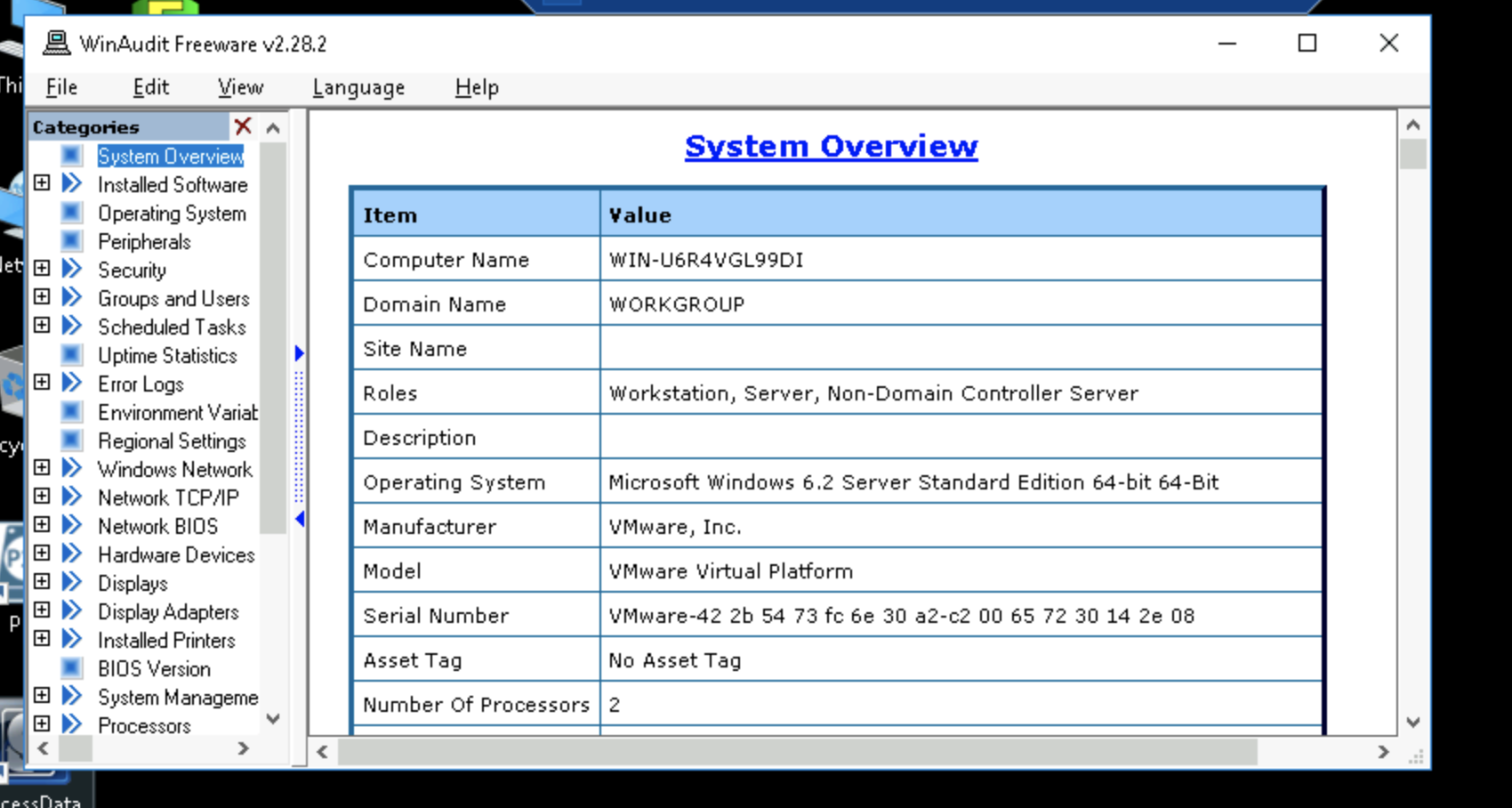
Jeremy Bergen

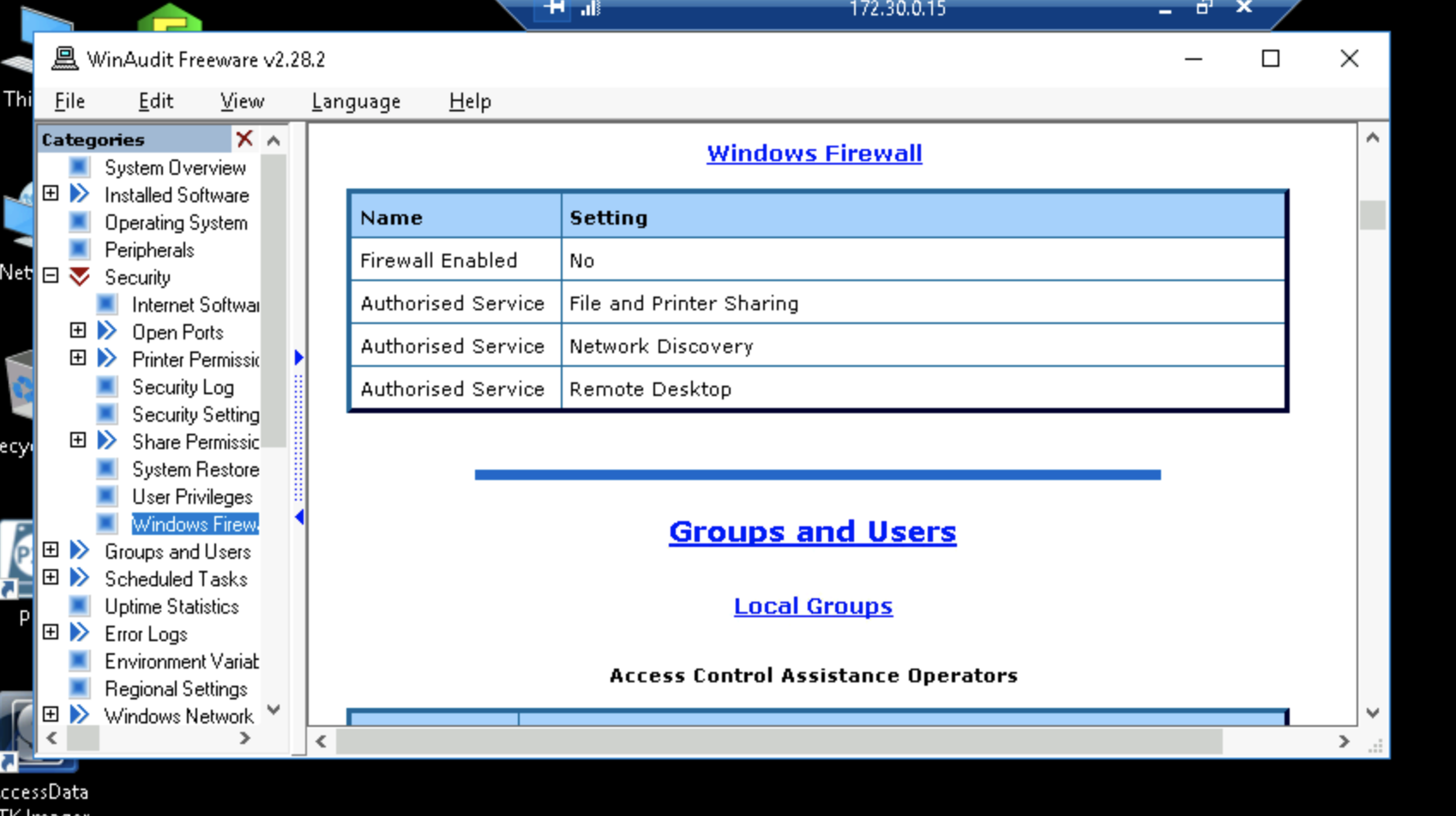
CSCI 370

10/1/21

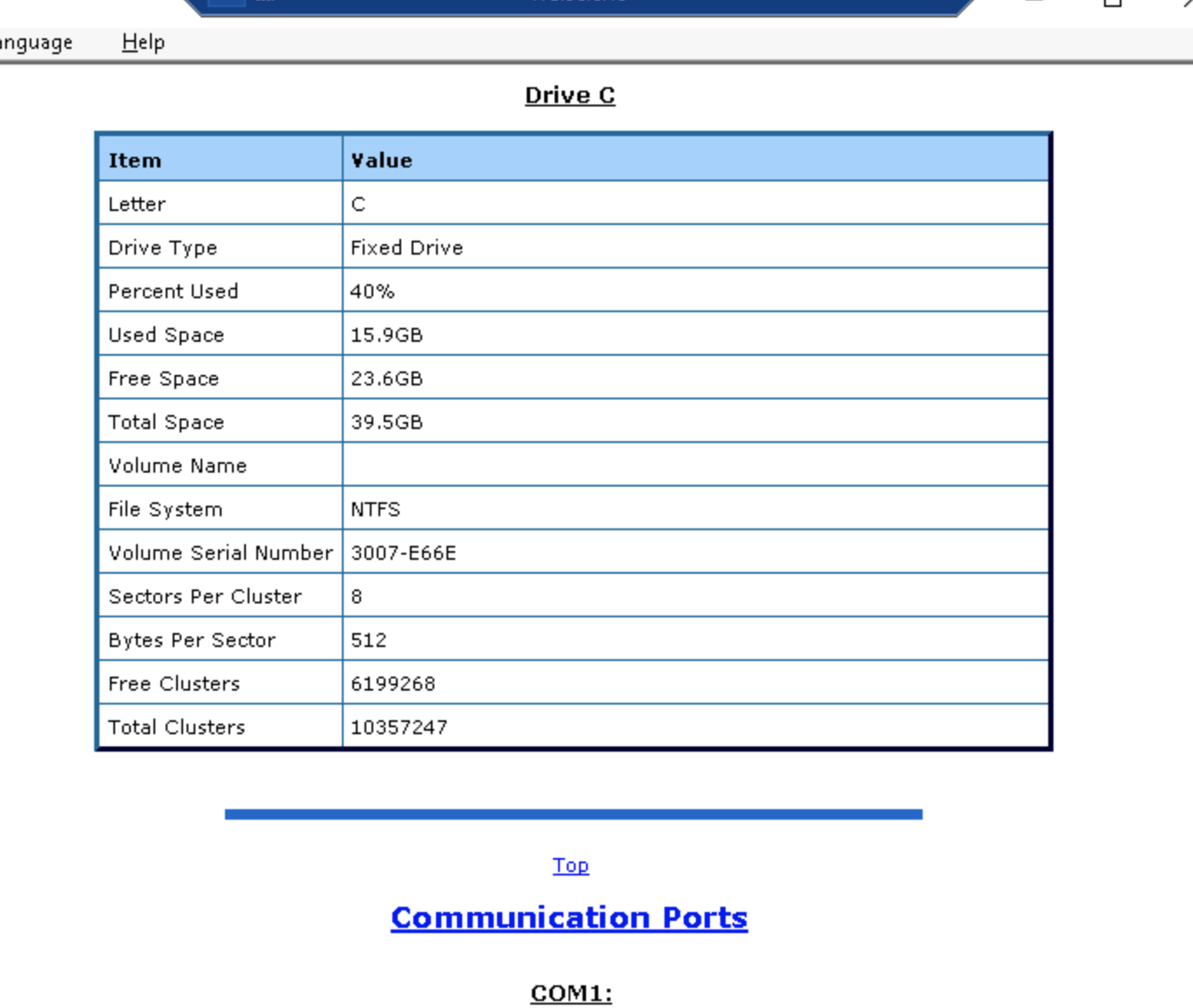
Week 5 Lab

Section 1:



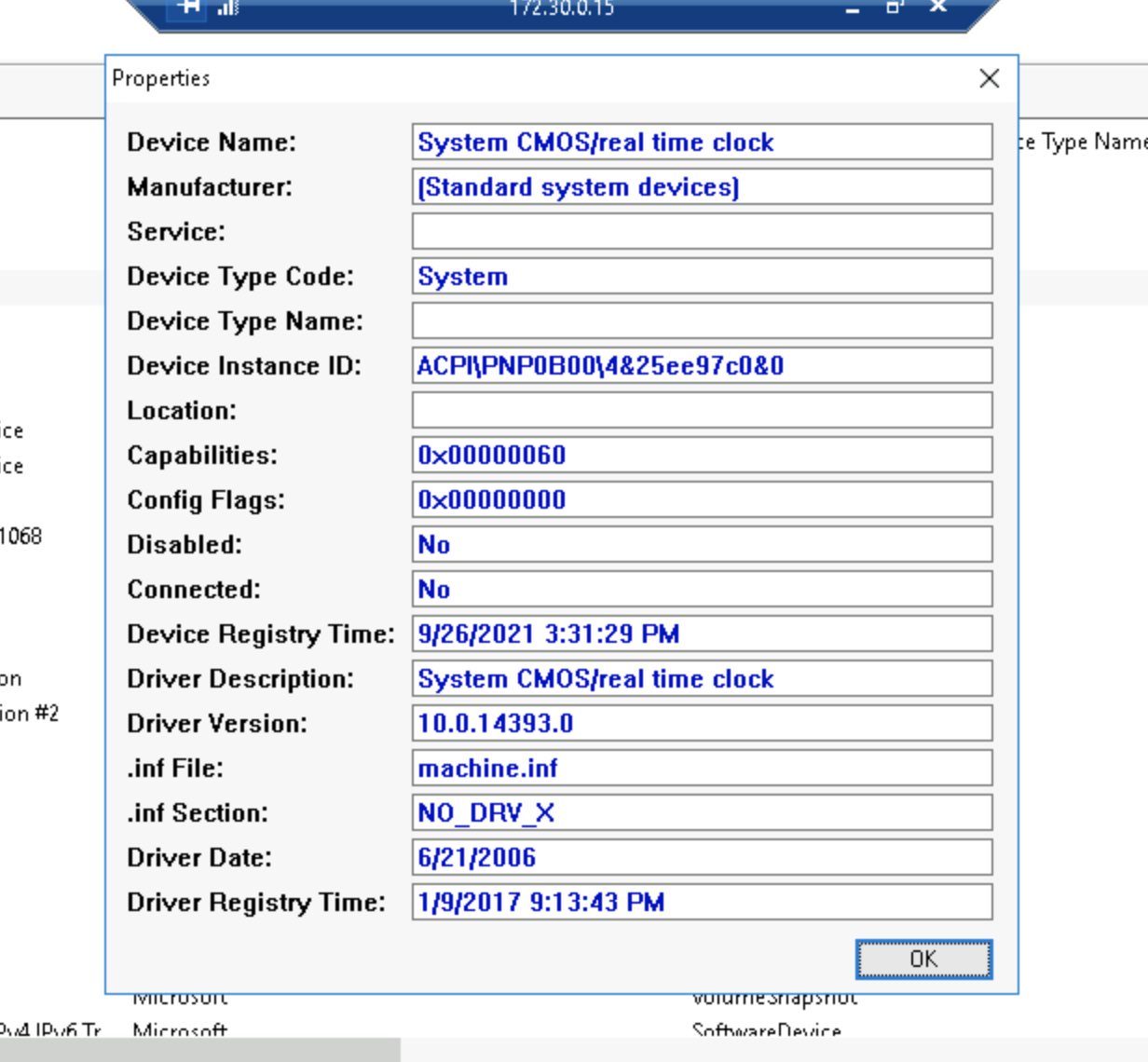


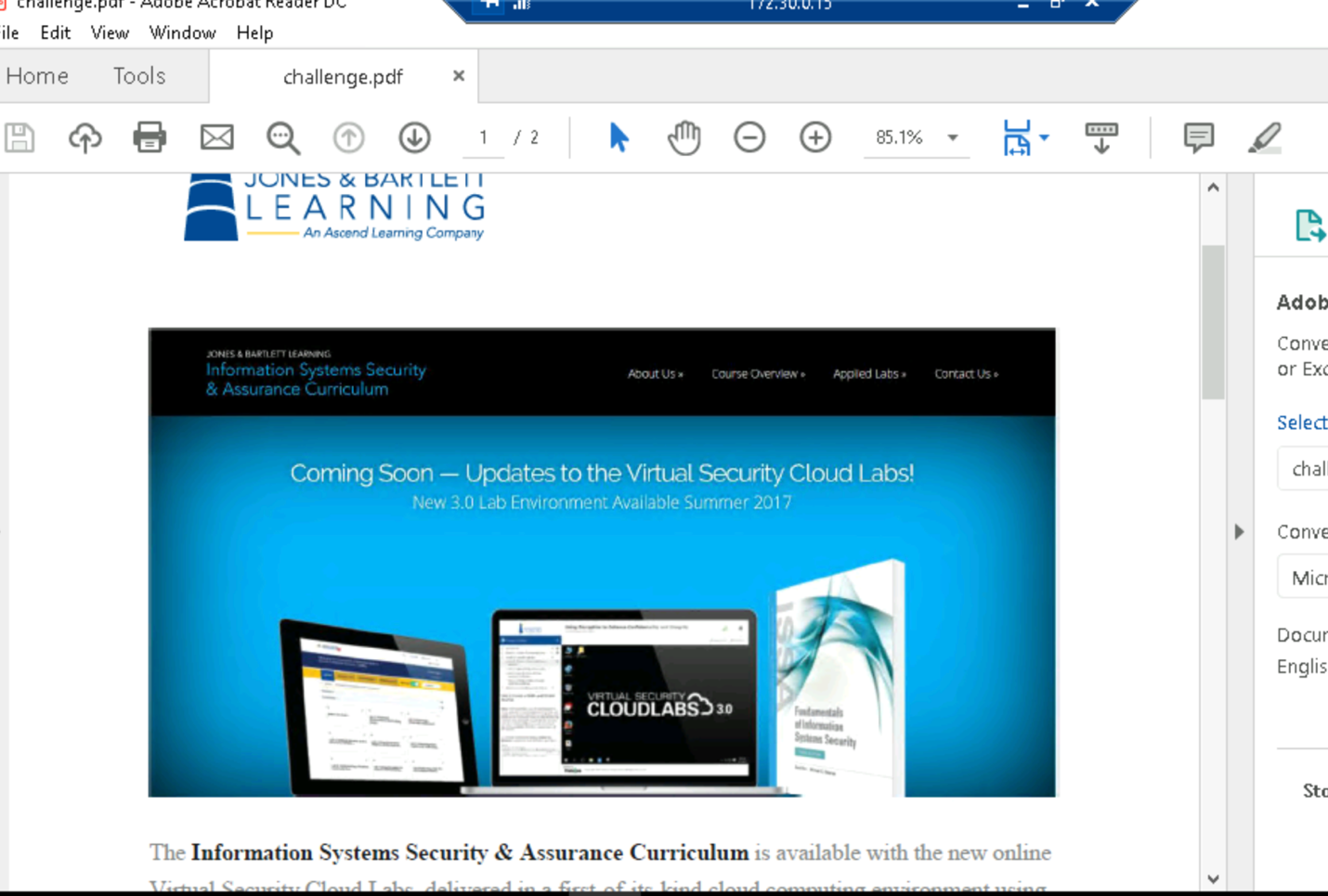


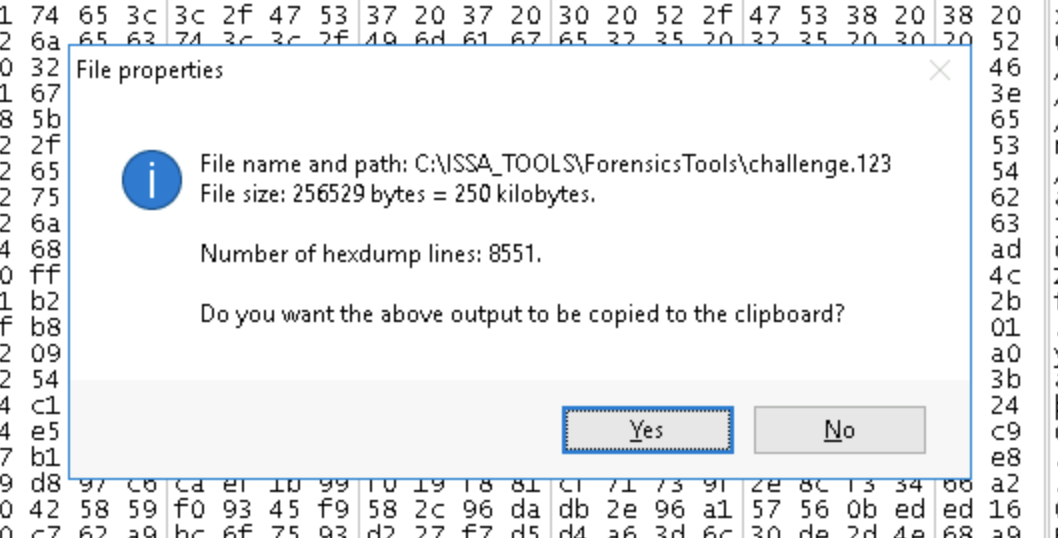


DevManView Devices: 78 Devices

Disabled “Connected Devices”: 121 Devices



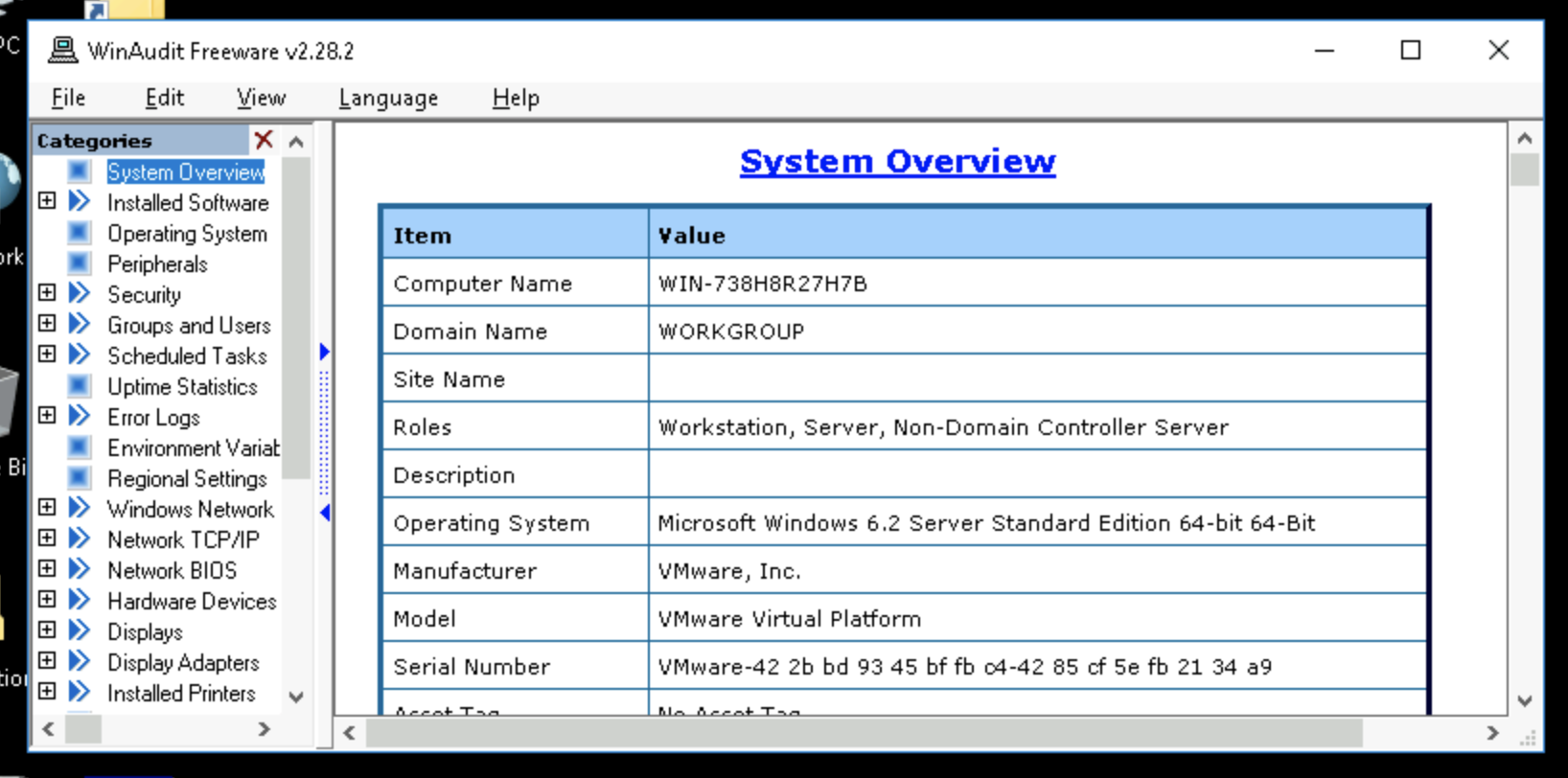


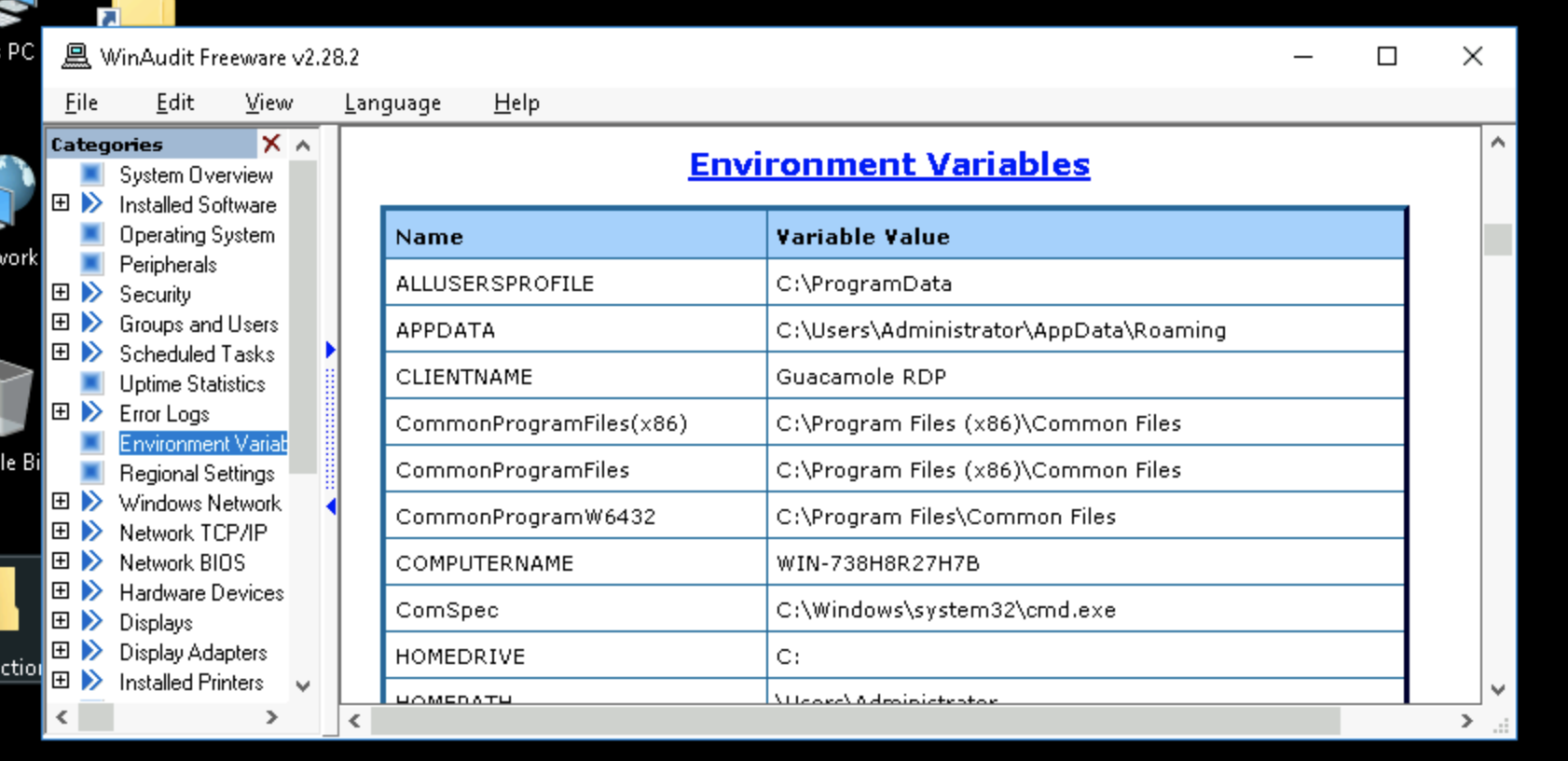


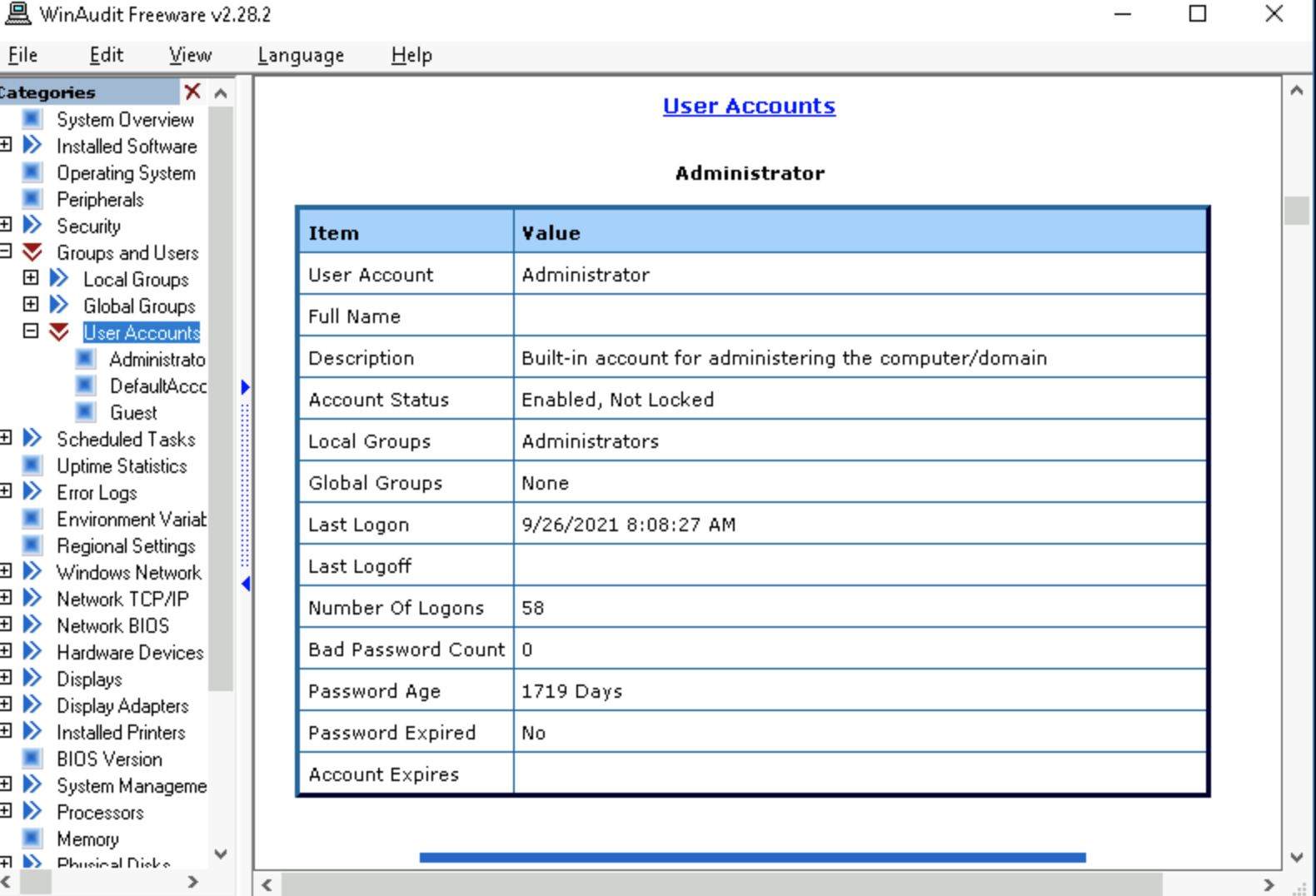
Section 1 Report:

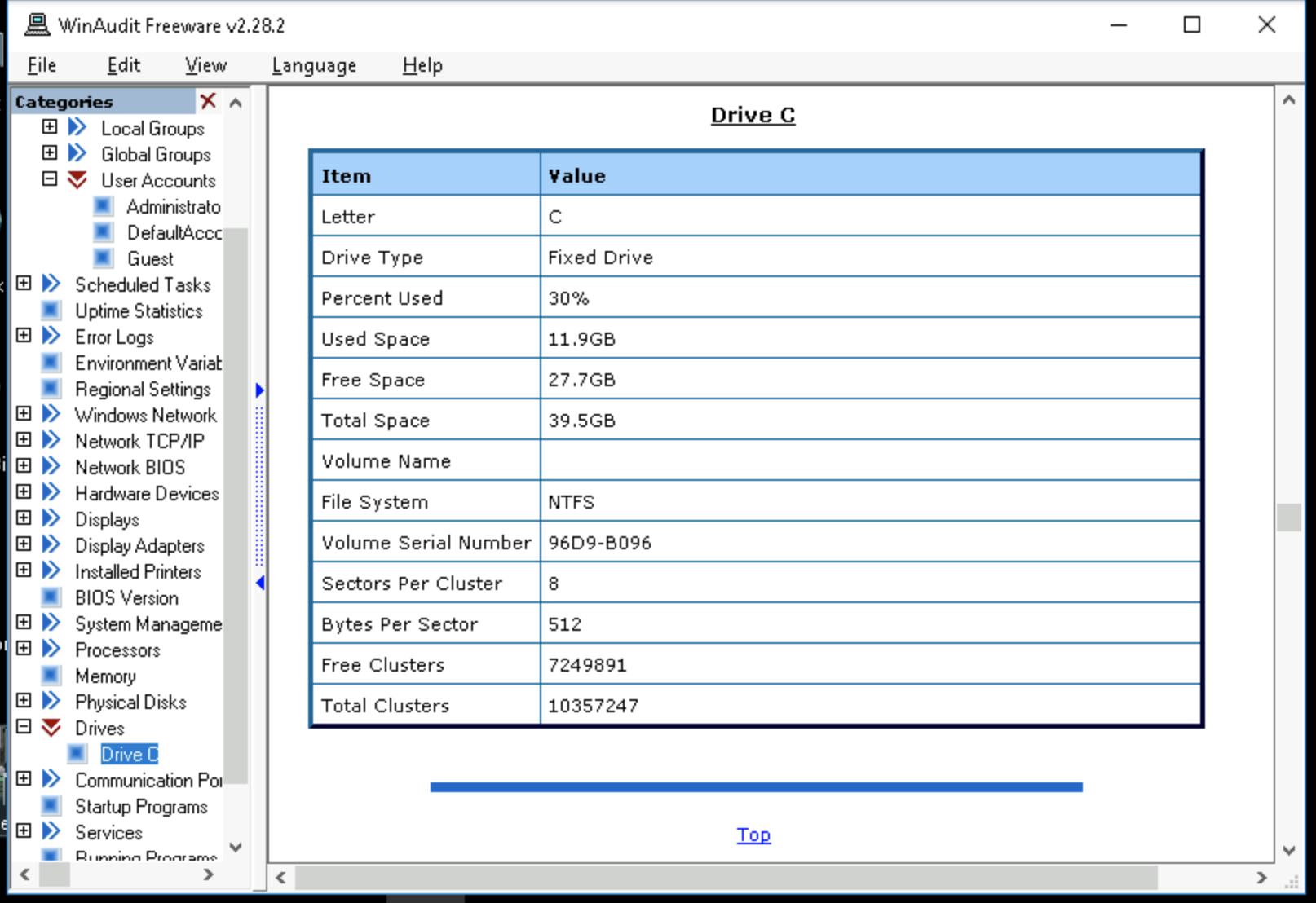
So, since we have to write a lab report for both 1 and 2, and the steps basically mirror each other, I decided to only do it for section 2 since that one was more independent. The steps and the report would be exactly the same, except we find the unknown file to be a pdf instead of a png.

Section 2:









DevManView Devices: 115

DevManView Connected Devices: 77

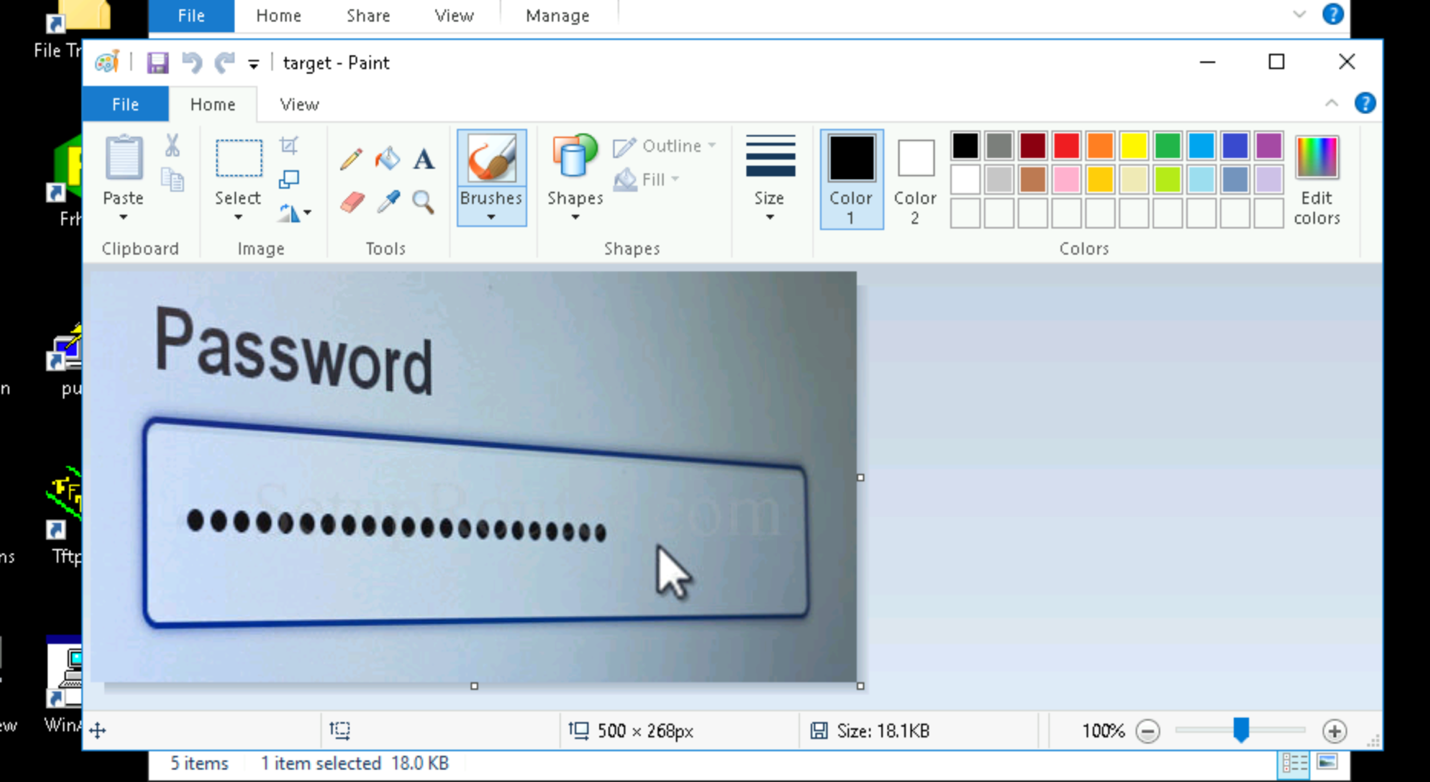


Device Instance ID: ROOT\NdisVirtualBus\0000

Inf. File: nidsvirtualbus.inf



I honestly didn’t see what would give away what this file type is. I’m seeing a lot on adobe things though so I’m assuming it’s a png.

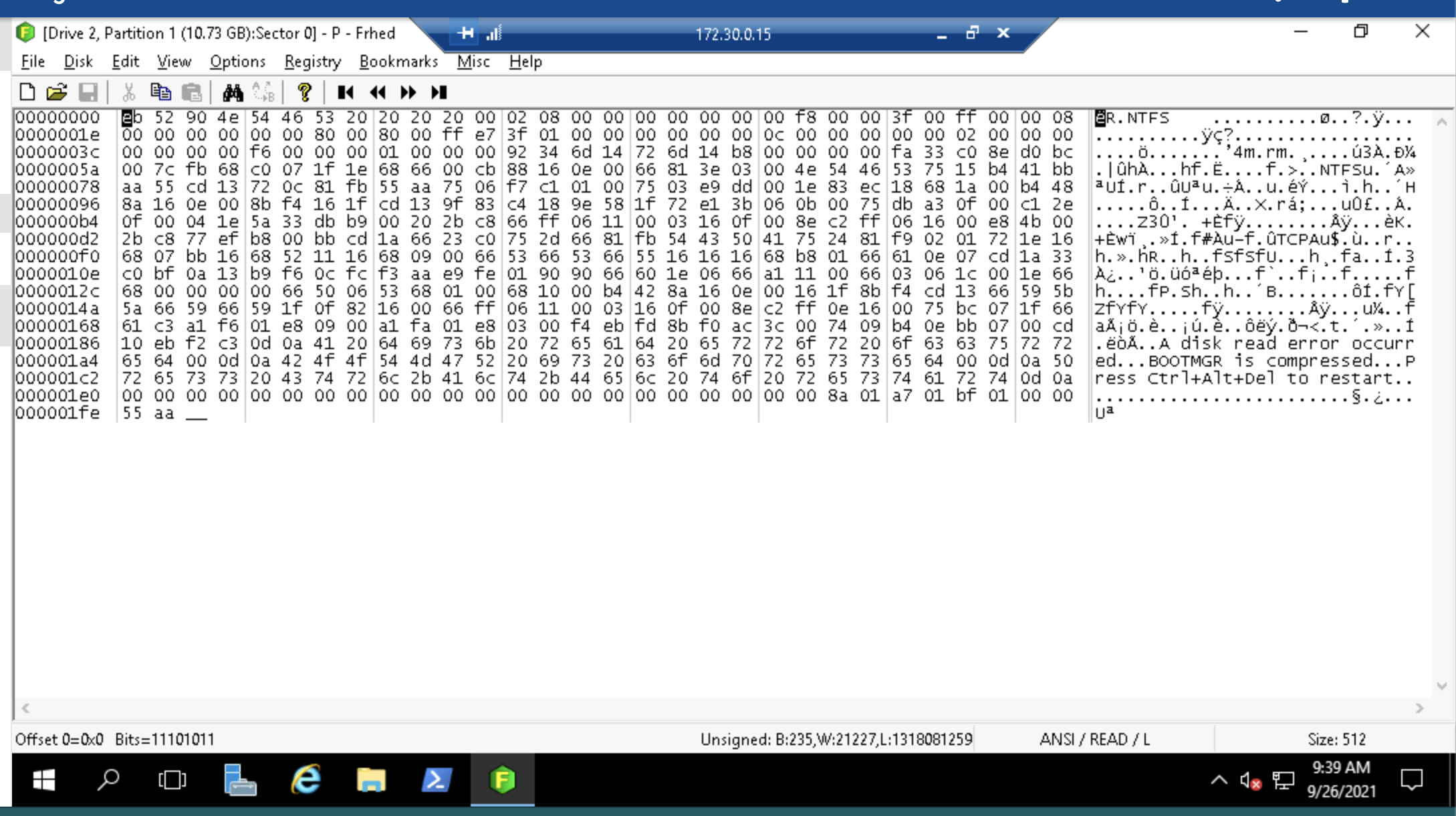


Section 2 Report:

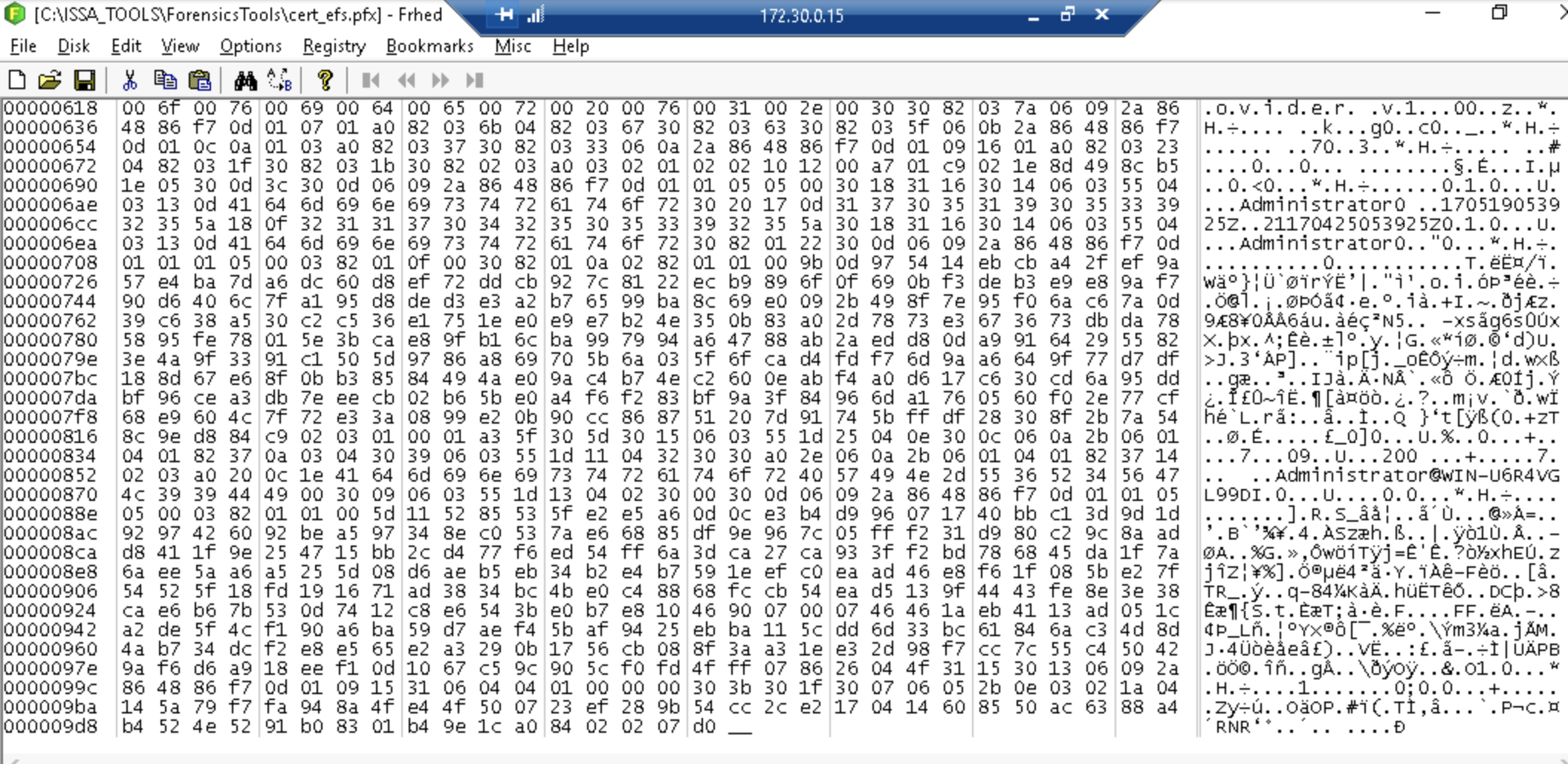
As we go through your system, we definitely get a better look at your system and its structure using our WinAudit program. It appears nothing out of the ordinary, or any malicious software were identified at this point. Then, using DevManView, we get a better look at all the connected devices, as well as the unconnected devices related to your system, as well as the information associated with those devices such as their ID’s. If there were any foreign devices, DevManView would’ve helped here. Lastly, we use Frhed to analyze specific files for corruptions or anything out of the ordinary. We analyzed the unknown file type, finding it was a png photo of a password. This no doubt poses a threat and must be addressed as to how this photo was captured.

Section 3:

All of these are important skills for simply understanding your system. Knowing where files are and how they are stored, their size, parents/children, when these files were edited, if the files are corrupt, etc. It is a skill, and things like Frhed definitely require more practice, but it is helpful to know so that you can be responsible with your files and understand the intricacies of your device.



After some researching, it looks that “1e” is a partition label, meaning that second line on the left signifies it’s a partition. Quite frankly, still pretty unsure on how to decipher this. I assume most of it is knowing the code and their combinations meanings. I am still unsure on how to read this though since I feel the lab didn’t really show us what to look for to find those answers.



I am seeing some stuff on the right about an admin, so my guess would be that user. Not quite sure about the type of encryption though. Maybe that “RNR”?

I tried finding an app similar for macs to look at drive info, but macs are picky. This is really the best info I could find, even after trying a few different apps.

