



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Computer Forensics (ACCD5000)

Digital Evidences



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

Lab Activities are based on

TryHackMe, EC Council – CHFI, Digital Forensics Workbook and other Industry Digital Forensic Curriculum

[illegible]

ICONS Used in this document:

Find out the outcome/ Answers/ Solution and record your reflection



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.



Recommended Screenshot (with Timestamp) for your Coursework.



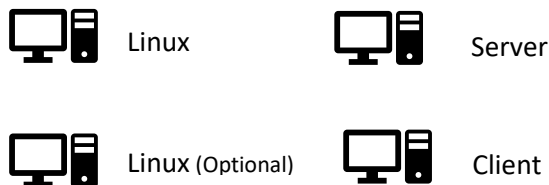
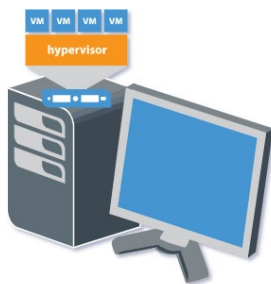
Recommended to address this part in your Coursework.

Note: For this activity and other upcoming activities, you shall use any relevant screenshots or discussions to your coursework according to your judgement. I will not be recommending Screenshots/ Recommended part to address in the coursework.

Task 1: Lab Setup

For your Computer Forensics (ACCD5000) Module, you need a Server and Multiple Clients. It is recommended to setup a virtual environment with the following machines.

1. Windows Server 2022/2019
2. Windows Client (10)
(Lecturer's Note: Download a Microsoft Evaluation Copy – It works for 180 Days – Alternatively, download from Microsoft Azure – Talk to Lee Cobley for any support with Microsoft Azure)
3. Any Linux Machine (Ubuntu/ Debian/ CentOS/ Kali Linux)



4. Open Virtual Box (Recommended – Already installed in the Lab PC's) and download the above recommended OS and install them in the same network.
5. Use \\192.168.135.50\FTKToolsShare\$ to download the required tools for your Labs

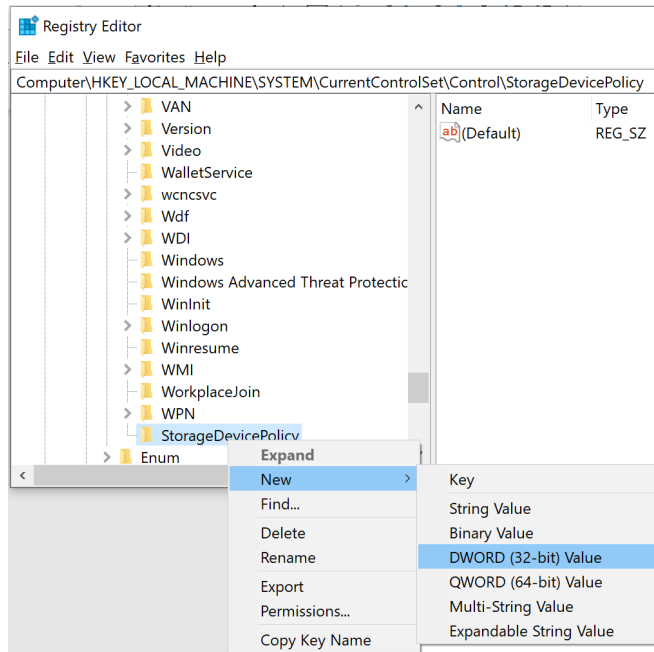
Scenario

Task 2: Ensuring Integrity

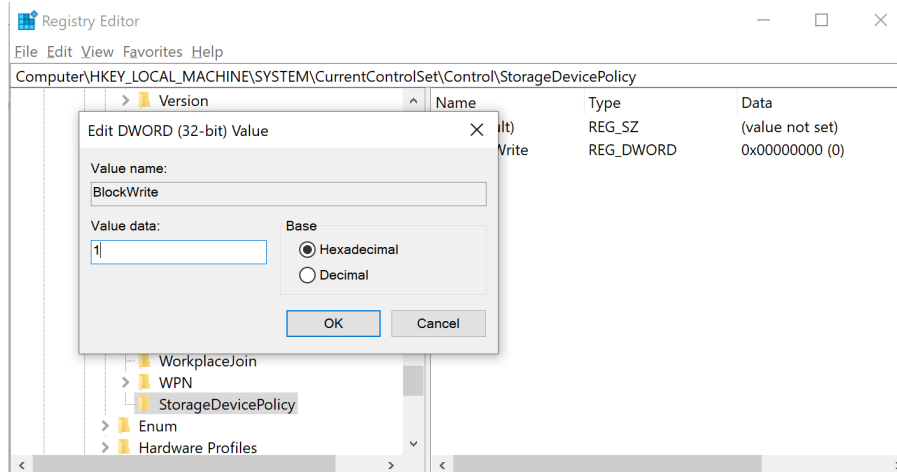


1. Discuss with your Lecturer and Classmates on what are the necessary steps to take in ensuring the integrity of the data.
 - a. Document your reflection in Moodle – Discussion Forum.
2. Do you know that using Windows Registry, you can prevent data from being written to any other external storage/ device?
Login to your Virtual Lab → Windows Client: Make sure your Windows Client in your Virtual Lab could access USB Port.
3. Review the options available in Windows Registry to accomplish the task to protect the data from being written to a USB storage/ device.
4. Open Reg Edit
 - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
 - Review the available Control Sets.
 - Create a New Key under Control and name it appropriately. I named it as StorageDevicePolicy.

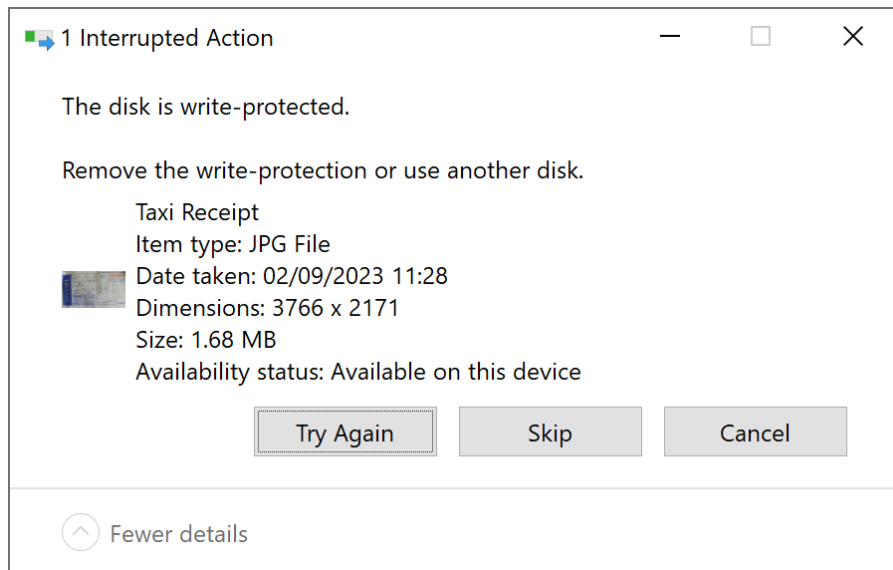
- Click New: What are those options? Research and discuss with your Team



- Create a DWORD and name it appropriately. Change the value to 1.



- Check the outcome by connecting a Flash Drive/ HDD and copying data to it. (Note: This activity requires a pre-setup in your virtual box to allow Flash Drive/ External HDD to be connected/ recognised in your virtual environment. – Research/ Discuss and enable Flash Drive/ External HDD to be accessible in your virtual environment)
- You can try this in your Host Machine as well. However, note that you have to reset the configuration if you try in your Host Machine.
- Record your outcome: (All recordings must have a time stamp on it) – The outcome will be similar to the one below.



Overall Reflection

Record your reflection via Moodle – Group Discussion.

1. Understanding of the concepts discussed in the lecture and its relation to the activity done.
2. Understanding setting up the Virtual Lab Environment and making adequate customization (Allowing Flash Drives etc).
3. Understanding and implementing Data Integrity and its need.
4. Rate yourself (1 very low – 5 exceptional): Understanding the Basics

-----End of Activity-----