**Digital Forensics**

**Assignment 2 – Windows Encrypting File System (EFS)**

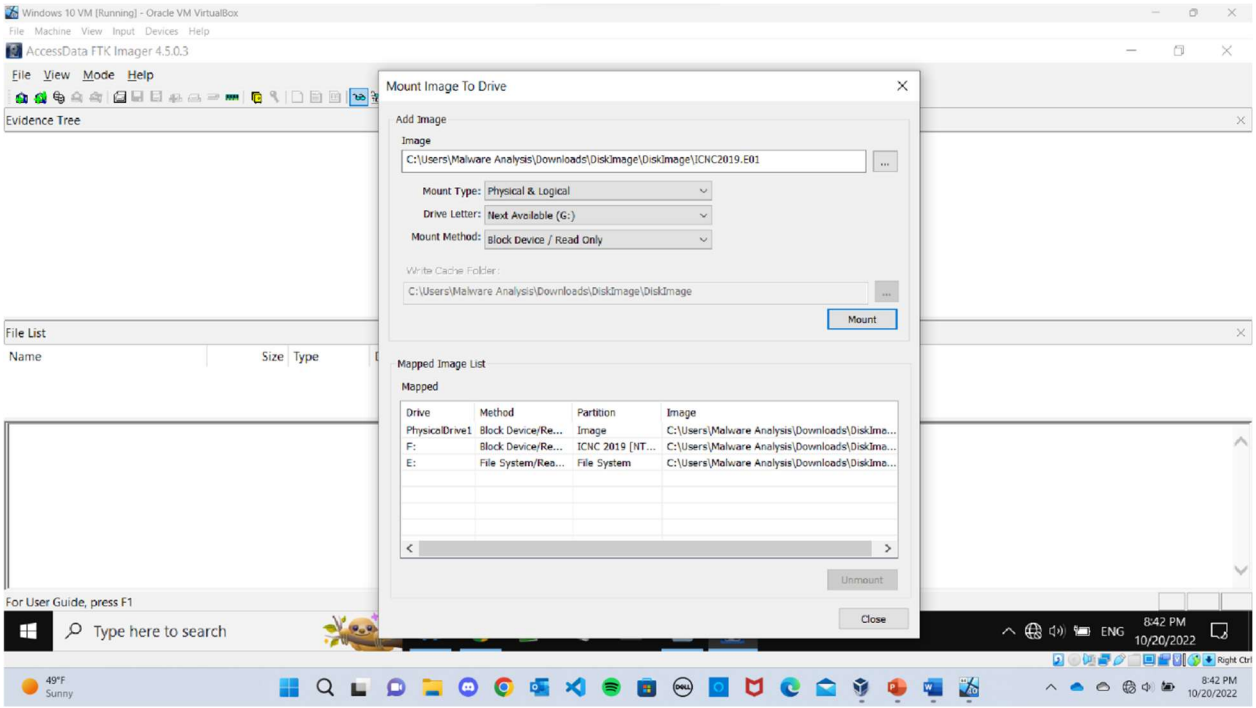
**10 points**

Kush Patel

## QUESTIONS

This assignment will be performed under the Kali Linux VM.

1. Please download the image of a USB drive at https://studentuml-my.sharepoint.com/:f:/g/personal/xinwen_fu_uml_edu/EjHyzTjhJ0RIgQ3uNxgnjfcBIKaLWTftAPjjGrI38RlGWw?e=HCWsgz to your Windows VM. Note: if clicking the link does not work, please copy and paste the link to a browser. *ICNC2019.E01* is the compressed image file in the E01 format. Please use FTK Imager to mount the image.
    a. Please provide a screenshot of the mounted image below. Note the mounted image will appear as a drive. (2 points)



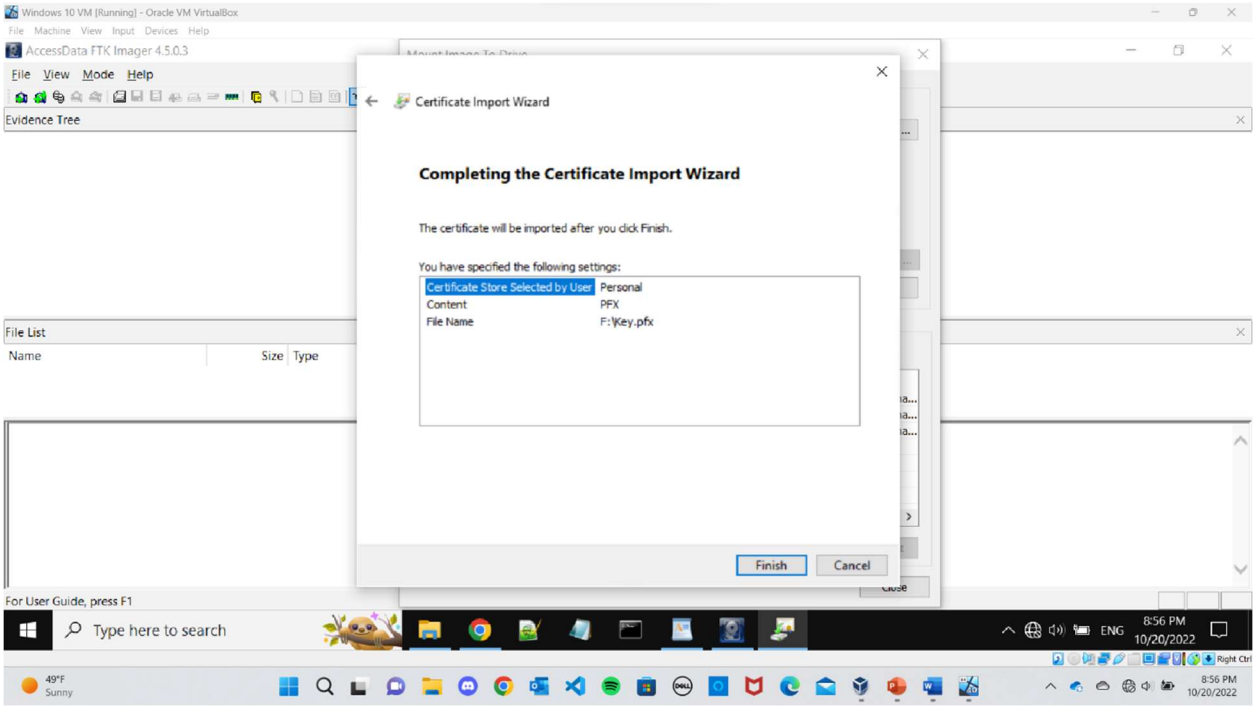

    b. Within the mounted image, there is a folder called *Secret*. There is a png image in the folder. When you double click the file, can you view the image? Why? (2 points)

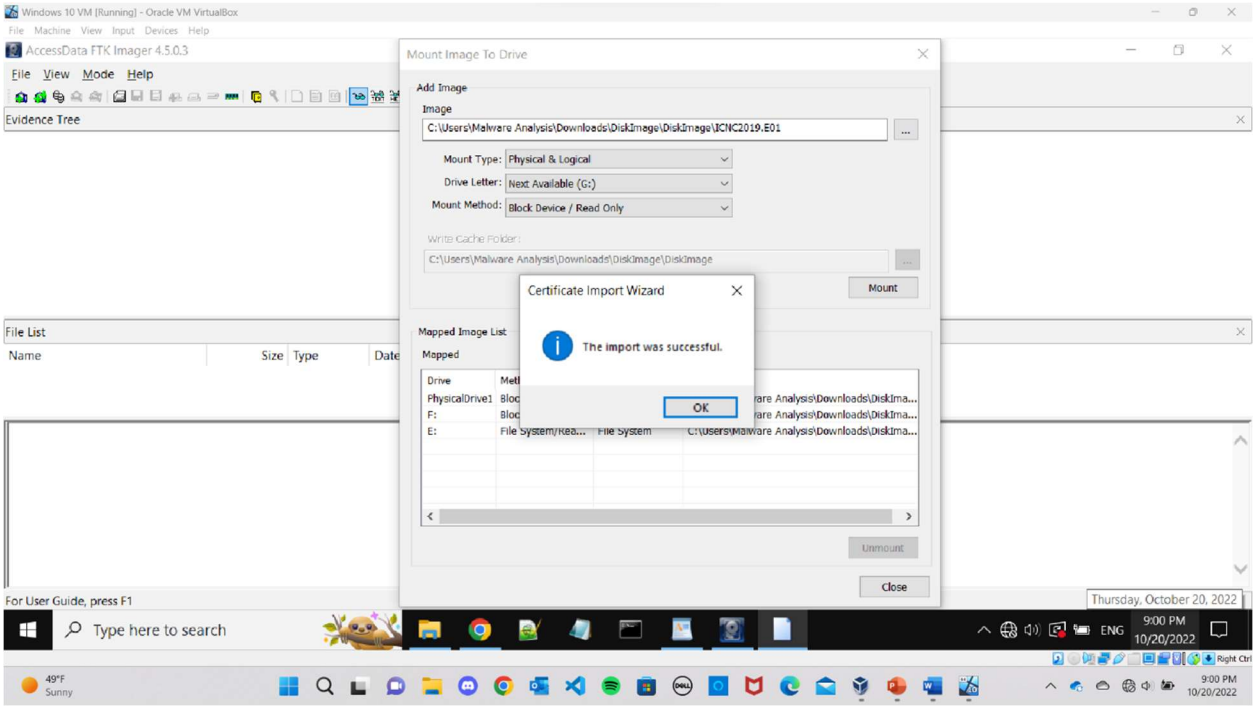
        No, because I don't have permission to view the file.

    c. Within the mounted image, there is a file called *Key.pfx*. Double click it and import the keys (private key and public key) into the Windows certificate store. Note: the

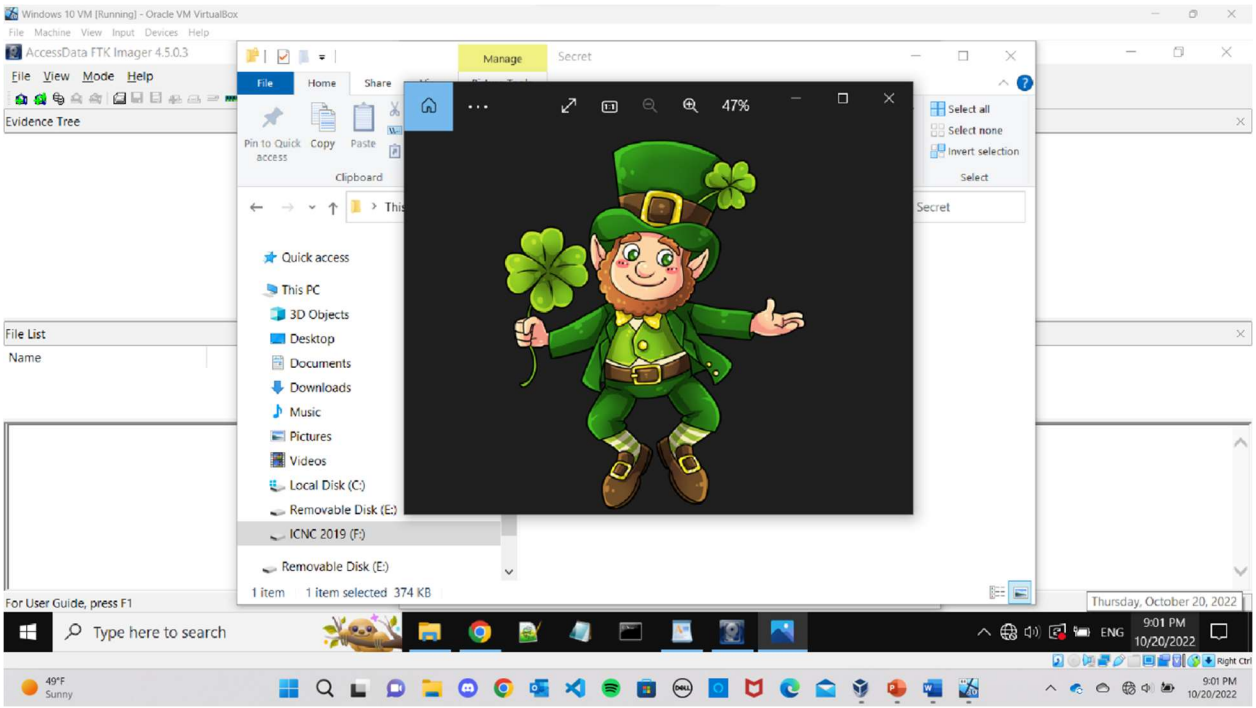
password protecting the private key is *Malware*. Please provide a screenshot of the imported certificate in the Windows certificate store. (2 points)

i. Please read [1] on how the EFS certificate is backed up and [2] on how to view a pfx file if necessary.



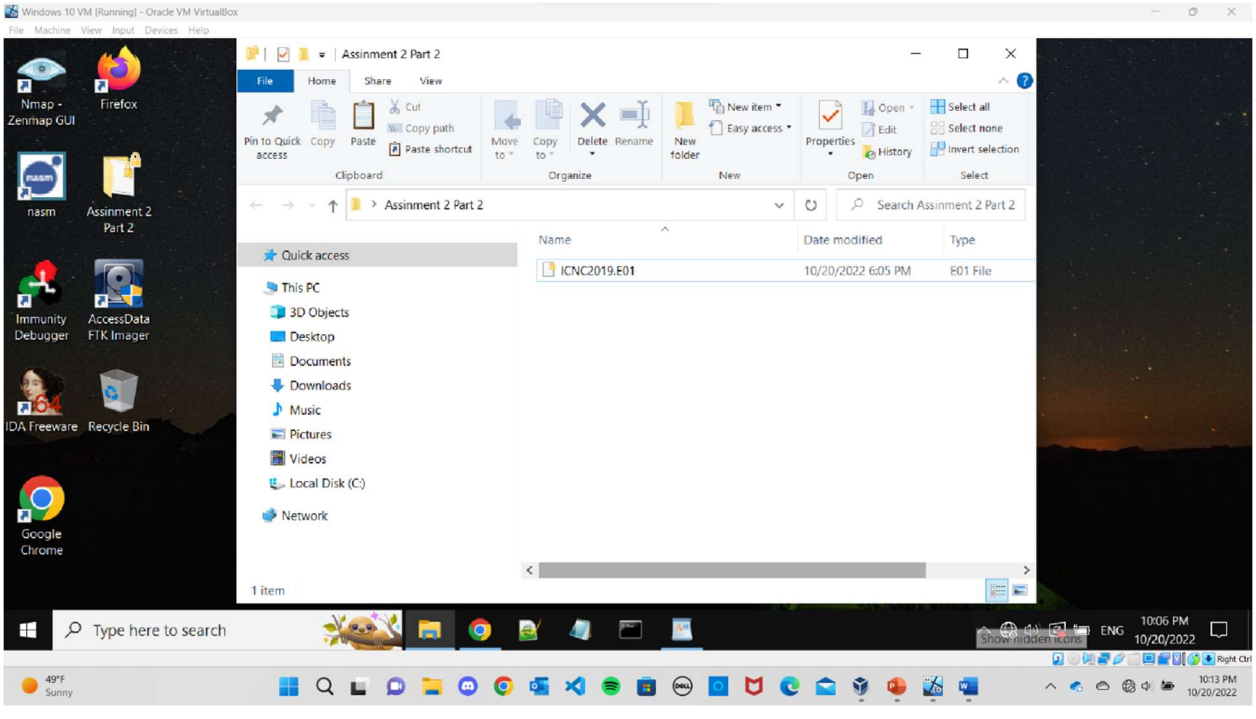



d. Please double click the image in the Secret folder again and the png image shall open. Please insert the image below. (1 point)




2. After *Key.pfx* is imported into the Windows certificate store, the key can be used to encrypt other files. Please choose a file, encrypt it and provide a screenshot of the encrypted file below. (1 point)

The encrypted folder is on the desktop as well.



3. Please discuss if a criminal encrypts his files, what can a forensics investigator do to open the encrypted files? (2 points)

Forensics investigators can use forensic analysis tools. Pro Discover basic is one tool they can use. They can copy the data and analyze it. Copying it allowed them to view the encrypted file on another device.

**References**

[1] Admin, 2 Ways to Backup or Export EFS Certificate in Windows 10 / 8 / 7, October 16th, 2017.
[2] Simon A. Eugster, How do I view the contents of a PFX file on Windows?, Apr 10 '13