Instructions for Digital Forensic Process

1. Get a fresh flash drive 4GB to 8GB in size without contents.
2. Copy the contents of the google drive /digital forensic software/doc to your flash drive.
3. Delete the following files:
   - SAD Ebook - shelly Rosenblatt folder
   - myfile.doc
   - IMG_5198
   - initial config

Problem:
A new wave of bitcoin extortion scams is making its way to educational institutions. Written in Filipino, it contains a threatening message depicting how the scammer was able to hack the victim's computer and webcam through malware that can remain hidden against the victim's antivirus software. It also claims to have the ability to purportedly get illicit videos of the victim. What follows is a threat to release those videos online if the victim does not transfer funds to the scammer's bitcoin wallet address. The scammer ends the letter with a 48-hour ultimatum with the consequence of releasing and sharing the claimed video to the victim's contact.

Threatening schemes such as these are the go-to for scammers to shock readers and eventually make them pay. We recommend never interact with unknown senders to avoid being scammed.

You are the first responder of the crime scene:

1. What procedure are you going to perform in this instance?

As a Forensic Investigator, perform the steps in digital forensic.
Explain the procedure on how did you come up with the conviction of the scammer basing on the flash drive you secured as your evidence.

Write a report based on your Analysis to be submitted to the court of law.

Rubric for checking:

1. Identification - 15pts
2. Acquisition/Imaging - 30pts
3. Analysis - 40pts
4. Reporting - 15 pts

Digital Forensics Report on Bitcoin Sextortion Scam

1. Identification

Based on the information provided to me, as a first responder, from the victim of the scam – the evidence available is mainly revolving around the victim's computer, which contains persistent data and volatile data.

Victim was also sent a threatening message about how the scammer was able to infiltrate the said victim's computer and webcam. Evidence regarding such claims is essential in knowing what approach to take. As this information is available on the victim's computer, it is best to not tamper with the computer for data imaging and analysis.

Before any processing begins, it is important that I, as a responder, have legal authorization to collect evidence. Double check the equipment I have brought as to not tamper with any evidence that may be crucial to solving this case and also to secure the scene by removing all unauthorized personnel from the scene and documenting the surroundings as well as the device used.

The room where the victim's computing device is stored should be considered as the boundaries of the crime scene. It is crucial that we document the computer's surroundings. It is important to take note of the specifications of the computer as well as the camera being used – it is best to question the victim regarding such as tampering of the device is off limits.

A USB has also been found, it's important to take a picture of such evidence for documentation before acquiring and proper labeling is significant. Gloves is necessary before touching evidence and must be placed inside a sealed anti-static bag.

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: 001
Evidence Number: 001
Unique description: Bitcoin Sextortion Scam
Examiner: Christian Stewart
Notes:
```

2. Acquisition / Preservation

As the first responder, it is important to identify, seize and secure all digital evidence at the scene. Documentation is essential as well. The course of action I would take is to leave the computer powered on. Evidence that is volatile may be lost when the system is turned off. Take photos of the scammer's message to the victim as evidence – label the picture accordingly.

The threatening message from the scammer is digital evidence and requires imaging to be analyzed as the case furthers. The investigator takes 2 disk-to-disk images of the evidence available on the computer using Access-Data FTK Imager. The first image as the backup image from which a second image is created to be used on analysis. Additional images will be made as

necessity arises. An image is created of the USB as evidence. The first image is a backup image and a 2nd image is created from the first one.

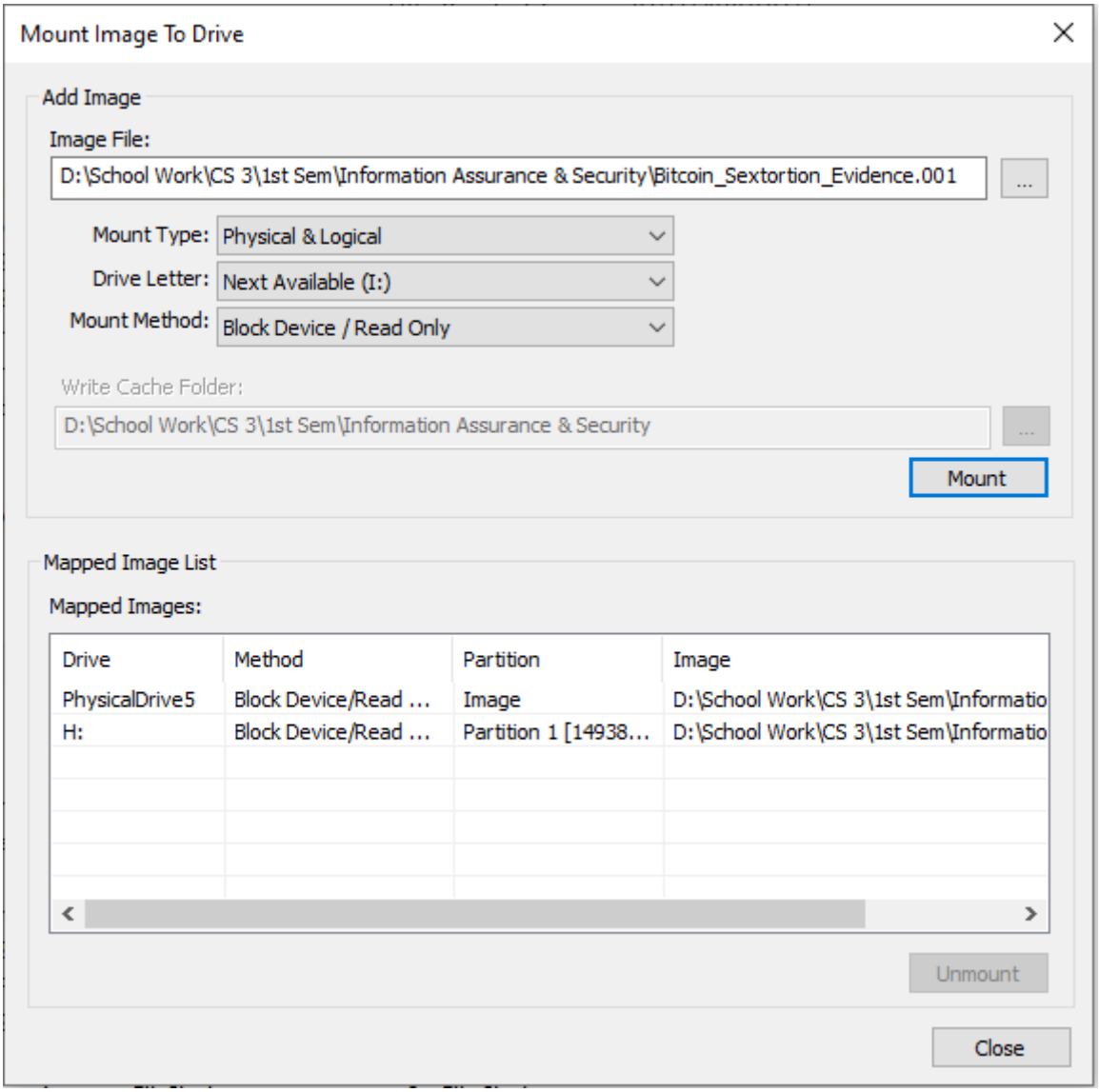
Authentication

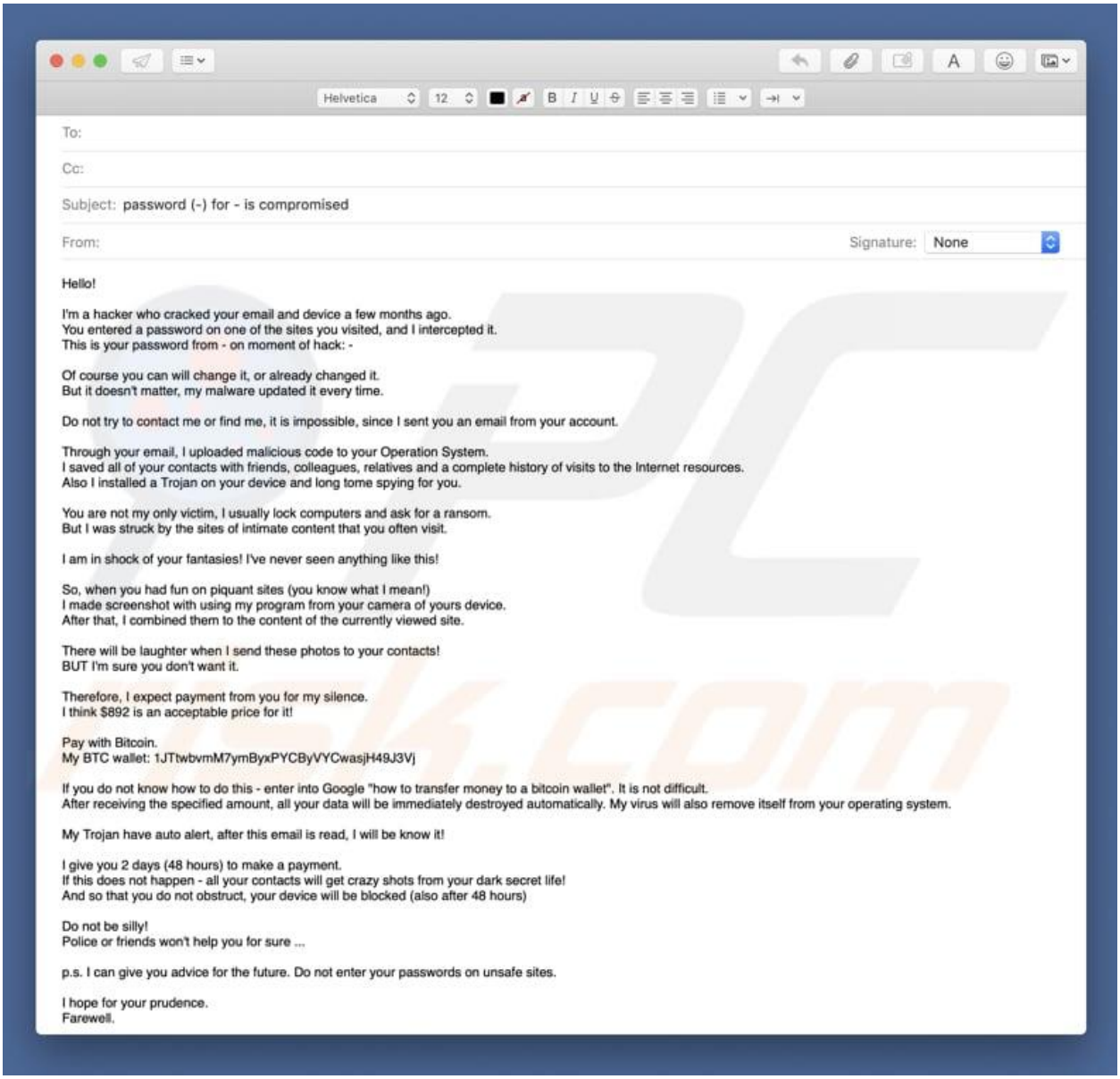
Once these images are made, cryptographic hash values of the evidence files were calculated to further prove that evidence has not been tampered with or modified in any way. Documentation also helps in ensuring evidence was not manipulated which I, as the first responder, have proactively done. Hash values are also compared as to see that evidence has not been tampered with upon acquisition.

```
[Computed Hashes]
 MD5 checksum:    8573d37d56e001b524522ea0b62b53ff
 SHA1 checksum:   9fa934a64580831fef63c06d12f37a90a9b0cc58

Image Information:
 Acquisition started:   Tue Sep 27 21:11:15 2022
 Acquisition finished:  Tue Sep 27 21:18:10 2022
 Segment list:
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Bitcoin_Sextortion_Evidence.001
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Bitcoin_Sextortion_Evidence.002
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Bitcoin_Sextortion_Evidence.003
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Bitcoin_Sextortion_Evidence.004
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Bitcoin_Sextortion_Evidence.005
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Bitcoin_Sextortion_Evidence.006
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Bitcoin_Sextortion_Evidence.007
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Bitcoin_Sextortion_Evidence.008
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Bitcoin_Sextortion_Evidence.009
  D:\School Work\CS 3\1st Sem\Information Assurance & Security\Bitcoin_Sextortion_Evidence.010

Image Verification Results:
 Verification started:  Tue Sep 27 21:18:10 2022
 Verification finished: Tue Sep 27 21:20:29 2022
 MD5 checksum:    8573d37d56e001b524522ea0b62b53ff : verified
 SHA1 checksum:   9fa934a64580831fef63c06d12f37a90a9b0cc58 : verified
```

3. Analysis

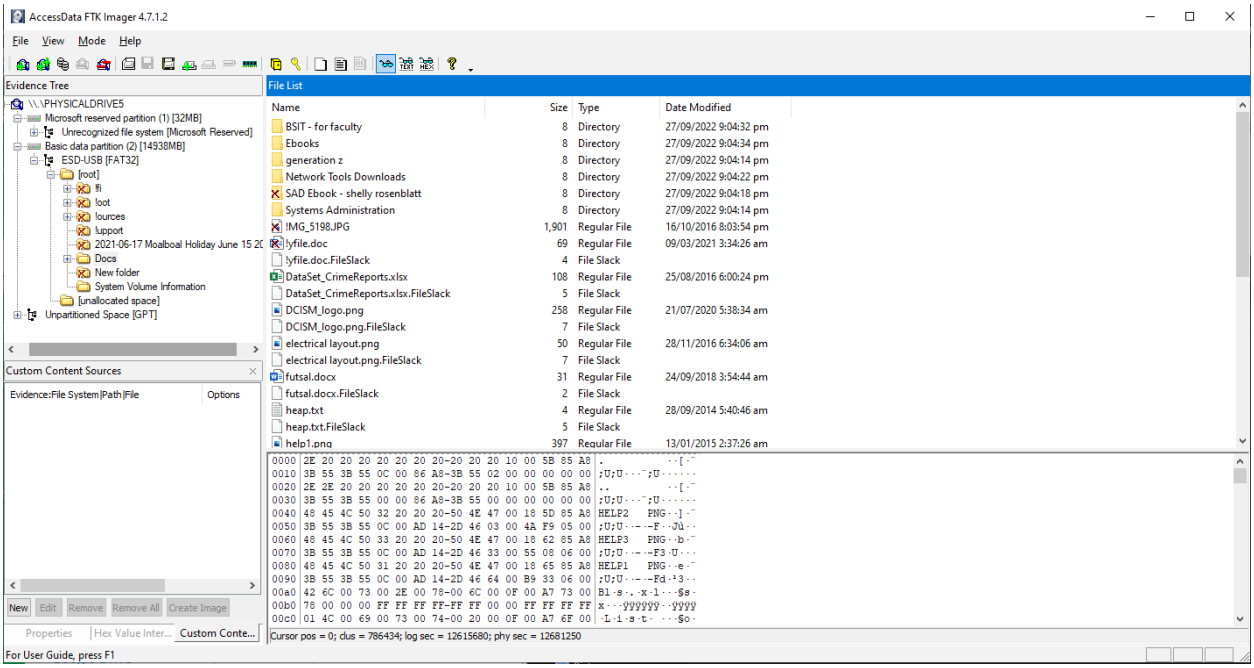
To verify the contents of the USB, a software tool is used – AccessData FTK Imager – to image the device and check for deleted files if there are any. As shown in the image below, the attacker has deleted evidence from the USB. “myfile.doc” on the surface seems like it is merely a document but when you open it – it appears quite unreadable filled with gibberish. This is because it’s not meant to be a document file. After assuming that it wasn’t a document file, I altered it’s file type to png for image and lo and behold, evidence of the bitcoin sextortion scam.





Reporting

Based on the obtained analyzed information from previous steps in the process, there is obvious evidence that certain files from the USB have been deleted. Thus, this leads us to conclude that the person who tampered with the USB has attempted to remove such files from it. This USB is evidence and the tampering of evidence is unjust and unlawful. This is proof enough for a criminal act. Additionally, one of the files deleted has been tampered with – specifically “myfile.doc” to appear as if it was a document.



Court Representation

As a digital forensic examiner, I have performed the necessary steps in obtaining and analyzing information. In the file attached below is evidence of sextortion on bitcoin scams and a USB has been manipulated by deletion of certain files to hide the actual evidence whose filetype has been altered.

Therefore, the accused of the crime should be convicted for the bitcoin sextortion scam he/she has laid upon the victim. The contents of the USB have undergone the digital forensic process of identification, acquisition, analysis and reporting and evidence suggests that no tampering of the evidence has been done which leads us to the decision of conviction of attempted sextortion.

Bitcoin_Sextortion_Evidence.001.txt