

Digital Forensics Fundamentals (STW109SE)

VIVA Coursework (Activity Led Learning)

Handling Digital Evidence

MODULE LEADER: Dipesh Maskey

Student Name:

Roll No:

I can confirm that all work submitted is my own: Yes ☐

Question 1 (100 Marks)

The suspected file (hero.txt) in your hard drive which you feel has been compromised to harm your computer system. File hero.txt can be your great source of investigation. How do you proceed ahead to handle the file so that file will be ready for the Investigative purpose.

- a) Submit the word-processed document detailing;
 - i. Different techniques used to handle digital evidences.
 - ii. Different techniques used to preserve the integrity of the Digital Evidences.
 - iii. Explain the steps, process and techniques you will follow to make file “hero.txt” ready for the Investigation. Improper handling of evidences may change, modify or damage the attributes of the evidences.
- b) Submit the contemporaneous notes which will record of ‘exactly’ what you did to handle the “hero.txt” file. This should be included as appendix A. It is acceptable to provide contemporaneous notes as scanned handwritten notes, a screenshot, or any other forensic note taking software that you can acquire and use (providing you are adhering to any license agreements that may be required).

Plagiarism Note

As with all assessed work, both the research and written submission should be your own work. When submitting this work you are explicitly indicating that you have read the rules on plagiarism as defined in the University regulations and that all work is, in fact, your own, except where explicitly referenced using the accepted referencing style.

NOTES:

1. Try and limit your answer to between 1000 and 1200 Words.

Marking Scheme

Your work will be marked out of 100 with the breakdown as follows:

Assessable Item		Mark
Handling Digital Evidence		
a	Discussion on different techniques used to handle digital evidences.	20
b	Discussion different techniques used to preserve the integrity of the Digital Evidences.	20
c	Explaining steps and techniques for Handling “hero.txt”	40
d	Contemporaneous Note	10
e	References	5
f	Formatting and Cleanliness	5
General Comments		
Total		100