

ASSIGNMENT BRIEF

HTU Course No: 10203361	HTU Course Name: Forensics
BTEC Unit Code: F/615/1658	BTEC UNIT Name: Forensics

Version: 3



Student Name/ID Number/Section	
HTU Course Number and Title	10203361 Forensics
BTEC Unit Code and Title	F/615/1658 Forensics
Academic Year	2023-2024 Spring
Assignment Author	Safaa Hriez
Course Tutor	Safaa Hriez
Assignment Title	Unraveling Truth
Assignment Ref No	1
Issue Date	01/04/2024
Formative Assessment dates	From 01/04/2024 to 30/05/2024
Submission Date	11/06/2024
IV Name & Date	Sami AlMashaqbeh 31/03/2024
Submission Format	
<p>The submission for this assignment is an individual written reports that discribed in the <i>Assignment Brief and Guidance</i> section. The students have to submit a declaration form with their reports.</p> <p>An oral discussion or its equivalent will be hold. Instructions, date, and time for the discussion will be provided later. A witness statement or observation record is considered as evidence for this part.</p> <p>In your report, you should make use of headings, paragraphs, and subsections as appropriate. Your report should be in docx format and written in a formal business style using Times New Roman, and font size 12.</p>	
Unit Learning Outcomes	
<p>LO1 Examine the processes and procedures for carrying out digital Forensic Investigation</p> <p>LO2 Discuss the legal and professional guidelines and procedures for carrying out digital Forensic Investigation</p> <p>LO3 Use a tool or tools to conduct digital Forensic Investigation on devices or networks or cyberattacks</p> <p>LO4 Develop a Test Plan and make some recommendations for use in digital Forensic Investigation</p>	
Assignment Brief and Guidance	
<p>The capital city has been gripped by a series of high-profile kidnappings, starting with the kidnapping of the daughter of the CEO of the city's largest investment firm. The organized crime group, known as the BlackEAgle, managed to extort a \$1 million ransom for her release, setting a precedent for subsequent incidents. In each kidnapping that followed, the BlackEAgle demanded substantial sums of money in exchange for the hostages' freedom. They publicly challenged law enforcement, promising that their next crime would be the most daring yet.</p> <p>In a recent breakthrough, the Metropolitan Police arrested a key member of the criminal organization known as Eagle's Eye and began interrogation procedures. Despite thorough questioning, investigators hit a dead end and failed to obtain any information about the location or timing of the next crime. However, a ray of hope appeared when the police confiscated the criminal's device along with the USB drive. With the assistance of a digital forensics expert who was present at the arrest, images of both items were obtained. As a member of the investigation team, you have received these images. Now, It is your turn to unravel the truth, examine these digital artifacts, and uncover any clues that might reveal the time and location of the next crime.</p>	

I. Provide digital forensic report contains screenshots for each step, the report should follow the template and presents the time and location of the next crime for the BlackEAgle organization.

II. Provide separate report that contains the following information:

- a. Discuss what is meant by digital forensics.
- b. Did you use Rodney McKemmish model? If yes, explain it. If no, illustrate the used model and explain it.
- c. What is the importance of following the model presented in the previous question?
- d. Evaluate the advantages and disadvantages of conducting digital forensic investigation to improve system security.
- e. What are the law enforcement guidelines that you used when conducting the investigation?
- f. Discuss legal and ethical requirements that you have considered when conducting the investigation.
- g. Eagle's Eye is an individual in the city and has legal rights. In reference to these rights, assess how ethical you were when conducting the investigation.
- h. Evaluate the impact of both following and not following guidelines in a legal case, with regard to digital forensic evidence.
- i. What was your forensic examination plan for conducting the analysis before starting the analysis.
- j. Based on your journey in the analysis, what improvement recommendations do you suggest?
- k. Are your recommendations help in this investigation only or can be used as best practices for conducting digital forensic investigation in general? Discuss your thoughts.
- l. Critically evaluate your investigation, suggesting improvements to the current digital forensic investigation guidelines, processes and procedures.
- m. Compare between Autopsy and FTK-imager as tools that can be used in digital forensic investigation.

Learning Outcomes and Assessment Criteria			
Learning Outcome	Pass	Merit	Distinction
LO1 Examine the processes and procedures for carrying out digital Forensic Investigation	P1 Discuss what is meant by Digital Forensics with the aid of diagrams/pictures.	M1 Discuss the importance of following a process or procedure when conducting digital Forensic Investigation.	D1 Investigate the advantages and disadvantages of conducting digital Forensic Investigation.
	P2 Examine the processes and procedures for conducting digital Forensic investigation.		
	P4 Discuss several legal and ethical requirements for conducting digital Forensic Investigations		
LO2 Discuss the legal and professional guidelines and procedures for carrying out digital Forensic Investigation	P3 Examine several law enforcement guidelines for conducting digital Forensic Investigations	M2 Assess how ethical it is to conduct digital Forensic Investigations on a suspected individual with reference to their legal rights.	D2 Discuss why NOT following guidelines might jeopardise a legal case with regards to digital Forensic evidence.
LO3 Use a tool or tools to conduct digital Forensic Investigation on devices or networks or cyberattacks	P5 Determine hardware and software tools that can be used to conduct digital Forensic Investigation.	M3 Compare two tools that can be used to conduct digital Forensic Investigation. M4 Conduct a digital Forensic Investigation on a device or network or cyberattack.	D3 Critically evaluate your work and suggest improvements to the current digital Forensic Investigation guidelines, processes and procedures.
	P6 Examine the file system structure of several Operating Systems e.g. MS-DOS, Windows, UNIX, Linux, MacOS, Android, etc		
LO4 Develop a Test Plan and make some recommendations for use in digital Forensic Investigation	P7 Develop a Test Plan for conducting a test on digital devices or networks or cyberattacks. P8 Suggest recommendations for best practices for conducting digital Forensics.		