UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN PERTENGAHAN SEMESTER 2
MID TERM EXAMINATION SEMESTER 2
SESI 2020/2021
SESSION 2020/2021
FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

KOD MATAPELAJARAN ***SUBJECT CODE***	**:**	**BITS 3443** ***BITS 3443***
MATAPELAJARAN ***SUBJECT***	**:**	**FORENSIK DIGITAL** ***DIGITAL FORENSICS***
PENYELARAS ***COORDINATOR***	**:**	**SITI RAHAYU SELAMAT**
KURSUS ***COURSE***	**:**	**2 BITZ**
MASA ***TIME***	**:**	**1 JAM DAN 30 MINIT** ***1 HOUR AND 30 MINUTES***
TARIKH ***DATE***	**:**	**10th MEI 2021**
TEMPAT ***VENUE***	**:**	**ONLINE**

NAMA PELAJAR : Muhammad Izham Bin Norhamadi
MATRIC NO : B032020039

ARAHAN KEPADA CALON
INSTRUCTION TO CANDIDATES

1. **Kertas soalan ini mengandungi DUA (2) soalan:**
   This question booklet contains TWO (2) questions:
2. **Sila jawab SEMUA soalan**
   Please answer ALL questions
3. **Jawapan hendaklah ditulis menggunakan tulisan tangan.**
   Answers should in handwritten form

KERTAS SOALAN INI TERDIRI DARIPADA (5) MUKA SURAT SAHAJA
(TERMASUK MUKA SURAT HADAPAN)
THIS QUESTION PAPER CONTAINS (5) PAGES INCLUSIVE OF FRONT PAGE

Muhammad Izham Bin Norharadi

No.: B032020039 Date:

Question 1

1a) Identification - Identify the nature of the case so that the appropiate steps can be taken. Then, identify all the potential containers of evidence on the scene.

Preservation - Secure the crime and make sure only authorized member of the investigation team were allowed access to the scene.

Collection - Collect and seize the digital evidence. Capture live data such as RAM and copy it to a removable drive. Collect all the digital containers and seal them in antistotic bag. Write the chain of custody form and send the evidence to forensic lab.

Analysis - Create an image for the evidence and perform investigation on the image. Use forensic tools to analyse the image and replication of the findings.

2a) Not really, forensic examination may involves other electronics on the crime scene too such cameras, ATM machines, and so on as they may be tampered too.

b) - In order to get the full picture of the crime a thorough examination of the files and folders must be made including missing, tampered, or encrypted files. Thus, these files need to be restored or unlocked first.

- The evidence devices involved and it's location may compromised how much evidence can be acquired before breaching sensitive data. A proper clearance from the court or organization was needed to collect sufficient data.

No.: Date:

Question 2

First, we identify the nature of the case which is theft of company's assets. Then, secure the crime scene and the evidence in the account manager's room. Identify and collect any digital containers such as the flash drive and seal them in antistatic bag. If the computer was turned on, attach a write blocker to the device and collect the data on RAM using portable software such as MoonSols DumpIt and seal it in antistatic bag. Then, file a chain of custody form and send the evidence to forensic lab. In the lab, create an image copy of the evidence using FTK imager. Perform an investigation on the image ProDiscover Basic to find the appropiate evidence on the case and write them on a report. Perform further tests on the image using different tool such as Forensic Toolkit. Present the evidence to the higher-ups and make a conclusion on the case. Finally, make the decision on whether the employee is guilty or not in the court and show the evidence.