Muhammad Izham Bin Norhamadi
B032020039
S2G1

Class Activity

2) a) State the information need to be extracted to be used as evidence of the case investigated.

- The metadata including a file's created, modified, and accessed dates.

b) Explain how to ensure the integrity of the evidence is not tempered during the acquisition process.

- Avoid accessing or modifying the evidence before imaging to preserve the metadata originality

3) a) Explain the purpose of dd command.

- A bitwise copy of any input source such as disk drive, file or any input device.

b) Identify the dd problem and how it can be solved.

- dd creates raw format file that does not compress the data if it was too big. This can be solved with the split command to split the output segments into separate volumes.

c) Briefly explain the difference between dd and dcfldd command.

- dd command is intended as a data management tool while dcfldd worked the same as dd but with additional functions for forensic purposes such as hashing.