MACQUARIE University

ACCG8076 Foundations of Forensic and Data Analytics

Assessment 4

Critical Essay

Learning Objectives

- Examine issues and key principles of professional digital forensic practice, including chain of custody and best practice procedures
- Diagnose and appraise mechanisms to uncover or recover evidence from digital devices to support litigation and investigations

MACQUARIE University

ASSESSMENT 4: QUESTION

Critical Essay

Rob is a forensic computer specialist employed by BTS Pty Ltd, an investigative firm hired by ABC Pty Ltd to investigate potentially fraudulent activities by employees of ABC Pty Ltd. Rob attends the premises of ABC Pty Ltd and undertakes a physical review of the workplace. After a walk through of the premises, Rob decides to seize laptops and other electronic devices to collect evidence. There are over 80 laptops at ABC Pty Ltd distributed over three floors. Rob and his team immediately get to work and start by placing each laptop in individual boxes to transport them back to the forensic laboratory for further review. Each member of Rob's team is assigned a floor to collect and box laptops.

BTS Pty Ltd have hired an independent courier service to assist with the transportation of evidence back to their premises. As each laptop is secured in a box, the IT employees of ABC Pty Ltd assist Rob and his team by carrying the laptops to the trucks for transportation. One of the truck drivers asks why they are so many boxes, Rob replies "well we need to collect every single laptop as we don't know which one will have the smoking gun for this fraud investigation."

Critical Essay

After three hours of boxing the laptops, it becomes clear there are not enough boxes to seal the remaining seven laptops. Brett, the head of IT at ABC Pty Ltd offers to assist by preserving the remaining laptops and extracting all relevant documents and data to Rob for his investigation. As Rob is satisfied that Brett will maintain integrity and understands the process, he accepts Brett's offer of assistance. However, before he leaves, Rob quickly does a copy and paste of all the documents saved on the laptops on to his secure memory card as a precaution. Rob then tells the couriers to drive direct to BTS Pty Ltd and leave the boxes at the basement for his team to access.

Rob returns to BTS Pty Ltd and immediately carries the boxes into his forensic laboratory—which is a large room at the end of a corridor that can be accessed by any member of BTS Pty Ltd. Rob commences the extraction of the data from the seized laptops by using his preferred forensic software and makes one copy and labels them 1 through to 73 for all laptops. He places all the copies created into a folder and returns the laptops into the boxes to be returned to ABC Pty Ltd.

Critical Essay

Required:

Critically review the above facts, particularly the actions of Rob, and identify and examine all issues relevant to a consideration of whether there is any failure to comply with the standards applicable to forensic digital practice including chain of custody and best practice processes.

Analyse the issues identified, clearly specify the impact each issue may have on both the investigation and potential litigation and explain what should have been done to counter or mitigate the identified risks.

Maximum Word count: 2,500 (include a word count – references not included)

Due Date: Wednesday, 28th October 2020 (2 PM)

MACQUARIE University

ASSESSMENT 4: MARKING RUBRIC

Marking Rubric

MACQUARIE University

Criteria (50 MARKS TOTAL)	Fail	Pass	Credit	Distinction	High Distinction
Contextualise and examine issues and key principles of professional digital forensic practice, including chain of custody and best practice procedures **(30 marks)**	Inappropriate critique of issues and key principles of professional digital forensic practice, including chain of custody and best practice procedures	Appropriate critique of issues and key principles of professional digital forensic practice, including chain of custody and best practice procedures	Substantially appropriate critique of issues and key principles of professional digital forensic practice, including chain of custody and best practice procedures	Good critique of issues and key principles of professional digital forensic practice, including chain of custody and best practice procedures	Excellent critique of issues and key principles of professional digital forensic practice, including chain of custody and best practice procedures
Diagnose and appraise mechanisms to uncover or recover evidence from digital devices to support litigation and investigations **(15 marks)**	Little or no evidence of understanding the mechanisms to uncover or recover evidence from digital devices to support litigation and investigations	Some evidence of understanding the mechanisms to uncover or recover evidence from digital devices to support litigation and investigations	Evidence of substantial understanding the mechanisms to uncover or recover evidence from digital devices to support litigation and investigations	Strong and clear evidence of understanding the mechanisms to uncover or recover evidence from digital devices to support litigation and investigations	Comprehensive and high-level critical evidence of understanding the mechanisms to uncover or recover evidence from digital devices to support litigation and investigations
Clear, ordered, precise and appropriately referenced. **(5 marks)**	Little or no appropriate referencing. Language is frequently too informal for academic purposes. Errors in grammar make overall meaning unclear.	Predominantly appropriate use of referencing. Language is occasionally informal. Errors in grammar make meaning unclear in places.	Appropriate use of referencing. Language is generally appropriate for an academic assignment, with only occasional minor errors in grammar, spelling or presentation.	Accurate use of referencing. Writing style and presentation are of a high academic standard.	Accurate use of referencing. Writing style is exemplary and compelling, and is of a publishable academic standard.