CT109-3-M E-Investigation

Individual Assignment (70%)

Learning Outcomes:

CLO2: Defend the use of selected investigative skills in regard to investigation in specific scenarios to demonstrate strategic thinking (A4, PLO5).

CLO3: Integrate the use of criminal profiling and machine learning techniques in digital evidence gathering and analysis (A4, PLO6).

This assignment will contribute 70% towards the total course marks

Assignment Details:

Digital investigators are facing new challenges due to the expansion of digital evidence to be handled. At the same time, rapid development in computer science and information technology provides innovative techniques for digital investigations. Machine learning as an application of artificial intelligence can be used to analyze large amounts of diverse datasets. The use of behavioral profiling in an investigation also has significant potential to aid digital investigators.

For the assignment, choose one of the following cybercrimes (or similar):

1. Data breach
2. Fraudulent transactions
3. RAT *(Remote Access Trojan)*
4. Account hijack

and complete the tasks as follows (with suggested titles*):

- **Task 1 (CLO2) – 20%:** IoCs and Relevant PDE to Collect from Internal and External Sources for *[Chosen Cybercrime]* Investigations*
    - (*IoCs : Indicators of Compromise PDE : Potential Digital Evidence)*
- **Task 2 (CLO3) – 50%:** A Proposed Framework Incorporating Behavioural Profiling and AI / ML Technologies for *[Chosen Cybercrime]* Investigations*

Documentation Guidelines

You are required to submit documentation for both Task 1 and 2, as well as a presentation (PowerPoint slides) for Task 1. Document your work in a **professional and systematic** manner.

For Task 1, your presentation material should be approximately 12-15 (not 20 or more) slides to present within 10-15 minutes, with the following minimum requirements:

1. Title Slide
2. Agenda
3. Contents:
    a. OSINT and IoCs
    b. Specific types of digital evidence that can be used to prove this case, and where they are most likely to be found
4. Conclusions
5. References

For the report the expectation is an approximate length of 2500 words (excluding diagrams, appendixes, and references).

The report should meet the following minimum requirements:

1. Well-presented with Times New Roman font size 12, 1.5-line spacing, page numbers.
2. Cover Page with the following details:
    a) APU Logo
    b) Assignment Title: E-Investigation Individual Assignment
    c) Student Name, TP Number, and Intake Code
    d) Module Name and Code
    e) Lecturer Name
3. Table of Contents
    1. List of Figures / List of Tables (if applicable)
    2. Introduction
    3. Contents (numbered section and sub-sections)
        3.1. Task 1

3.2.1. Sub-sections

3.2. Task 2

3.2.1. Sub-sections

4. Conclusion
5. References
6. Appendices

Citations and references:

a) All information, figures, and diagrams obtained from external sources must be cited in the text and referenced using the APA referencing system.
b) All citations must have references, and all references must be cited. The reference list must be in alphabetical order, by author.
c) You are expected to have at least 8 references from authoritative sources, such as academic publications, research websites, and vendor whitepapers; avoid Wikipedia or About.com or the like as sources or references for your work, they will not count toward the total of authoritative references.

Content Notes:

1. You must use enough of your own words to convince that you understand your own assignment. Evidence of originality in your writing reflected by the effort of paraphrasing and use of own personal expression in your individual analysis and evaluation.
2. You should not submit a "copy and paste" work as you will only be awarded at most a **PASS** even though a proper citations and referencing are given.
3. You must ensure that your writing is clear and concise as quantity does not always guarantee quality. Therefore, you should not expect by writing more will enable to get a high mark unless the information is presented with clarity and relevance with high degree of analysis and evaluation.

Assessment Criteria (Marks Breakdown)

Student Name:	**Marks Allocation (%)**
Identification and Collection of Digital Evidence (~700 words)	
Evaluation of IoCs and OSINT	25
Evaluation of PDE	25
Evaluation of Sources	25
Presentation, Communication and Style	25
Total Marks	100
Proposed Framework (~1800 words)	
Framework Design - justification and discussion of the proposed design	25
Profiling Techniques - incorporation of behavioural profiling	25
Application of AI / ML - explanation of selected AI / ML tools	25
Written Communication - report format, citations, references, Turnitin	25
Total Marks	100

Marking Rubrics

Task 1 (CLO2 – 20%):

	0 to 12 (Fail)	13 to 15 (Pass)	16 to 18 (Credit)	19 to 25 (Distinction)
Cybercrimes Cases Evaluation (25)	Not able to evaluate cybercrime cases clearly.	Able to evaluate cybercrime cases with limited clarity; Requires significant improvements.	Able to evaluate cybercrime cases fairly and clearly but requires minor improvements.	Able to evaluate cybercrime cases with excellent clarity and justification.
Evidence and Admissibility (25)	Not able to explain / discuss relevance of evidence and legal aspects in collection properly.	Able to explain / discuss relevance of evidence and legal aspects in collection with minimal depth and detail.	Able to explain / discuss relevance of evidence and legal aspects in collection with a good level of depth and detail.	Able to explain / discuss relevance of evidence and legal aspects in collection with excellent clarity and justification.
Presentation, Communication and Style (25)	No or poor presentation and style. Unable to provide answers during Q&A.	Average presentation and style. Able to manage Q&A but not that confident.	Good presentation and style. Appropriate answers during Q&A with good confidence.	Excellent presentation and style. Excellent answers during Q&A with high confidence.
Ethics and Professionalism (25)	Does not perform tasks within the scope of work. Does not demonstrate professionalism in completing the task.	Able to perform tasks within the scope of work to fulfil basic requirements. Demonstrated minimal professionalism in completing the task.	Able to perform tasks within the scope of work and meets expectation. Demonstrated good professionalism in completing the task.	Able to perform tasks within the scope of work and exceeds expectation. Demonstrated excellent professionalism in completing the task.

Task 2 (CLO3 – 50%):

	0 to 12 (Fail)	13 to 15 (Pass)	16 to 18 (Credit)	19 to 25 (Distinction)
Proposed Framework Design (25)	Missing or poor design of the framework. Missing or inaccurate justification and discussion No diagram.	Acceptable design of the framework, with limited justification and discussion. Diagram provided.	Good design of the framework, with adequate justification and discussion. Diagram provided.	Excellent design of the framework. Well elaborated justification and discussion. Diagram provided.
Behavioural Profiling (25)	Missing or poor elaboration on applying behavioural profiling techniques.	Minimal or very general elaboration on applying behavioural profiling techniques	Good elaboration on applying behavioural profiling techniques in the chosen context	Extensive elaboration on applying behavioural profiling techniques in the chosen context
Application of AI / ML Tools (25)	Missing or poor explanation of the application of AI / ML tools.	Satisfactory general explanation of the application of selected AI / ML tools	Good explanation of the application of selected AI / ML tools in the chosen context	Excellent explanation of the application of selected AI / ML tools in the chosen context.
Written Communication (25)	Serious deficiencies in report format. Poor grammar, spelling, or sentence structure. Missing or poor citations / references.	Noticeable deficiencies in report format, grammar, spelling, or sentence structure. Minimal or improperly formatted citations / references.	Minor deficiencies in report format, grammar, spelling, or sentence structure. Relevant citations / references in the required format	Trivial deficiencies in report format, grammar, spelling, or sentence structure. Extensive citations / references. in the required format