## Aromatawai tuarua | Assessment 2 – Outline INFO702

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | Forensic Investigation | **Total Possible Mark** | 100 |
| **Type** | Forensic investigation and report | **Weighting** | 35% |
| **Learning Outcome(s)** | 1. Investigate OS, application, website and network threats and vulnerabilities 2. Investigate and implement OS, application, website and network security and testing techniques 3. Research tools and methods used in the IT industry related to cyber-attacks or cyber-security | | |

### Task / Aim

### In this assessment, your task is to conduct a digital forensics investigation using open-source tools. You will examine the provided digital evidence, analyse it using appropriate techniques, and answer specific questions related to the assigned investigation aspect. Your aim is to compile a comprehensive report summarising your findings and conclusions. This assessment assesses your ability to apply forensic analysis skills, think critically, and document your process effectively while upholding legal and ethical standards.

### Conditions/Guidelines

* Work will be completed in groups.
* The scenario and evidence files will be provided part way through the semester.
* Each group must conduct an independent analysis and interpretation of the findings, ensuring to avoid direct copying or plagiarism.
* Properly document and cite any external sources used in your investigation, including the open-source tools employed.

### Task Details / Instructions / Steps

1. Examine the provided digital evidence, including but not limited to disk images, RAM dumps, and any associated digital devices.
2. Research appropriate open-source forensic analysis tools to extract, analyse, and interpret digital evidence.
3. Document your forensic analysis methodology, including the tools, techniques, and rationale behind your approach. Properly document and cite any external sources used in your investigation, including the open-source tools employed.
4. Conduct independent analysis and interpretation of the findings to solve the case.
5. Answer the specific questions for your assigned aspect of the case (questions and scenarios will be provided during the semester).
6. Compile a comprehensive report summarising your findings, analysis, and conclusions. Include any supporting artifacts, timestamps, or significant discoveries.
7. Submit the report that includes your findings, analysis, methodology, and conclusions.

### Aromatawai tuarua | Assessment 2 - Marking Rubric

| **Criteria** | **Exemplary**  **100-75%** | **Proficient**  **74-50%** | **Needs Improvement**  **49-0%** |
| --- | --- | --- | --- |
| Executive Summary  5% | Provides a comprehensive and concise summary that includes a background, clearly states the objective, summarises the investigation's key findings, and effectively sets the context. The summary is insightful and highlights the relevance of the findings to the overall investigation. | Provides a sufficient background and states the objective. Summarises the key findings of the investigation and sets the context adequately. It may lack depth or minor details. | Lacks clarity in providing the background and/or does not clearly state the objective. The summary of findings is incomplete, unclear, or missing and fails to set the context for the investigation effectively. |
| Digital Evidence Examination  10% | Thoroughly examines and describes the digital evidence, clearly understanding its significance. Applies appropriate tools and techniques effectively, following a recognised forensic framework such as the NIST framework. The examination is systematic, logical, and well-documented. | Clearly examines and describes the digital evidence, demonstrating a reasonable understanding. Applies appropriate tools and techniques effectively, following a recognised forensic framework. The examination is generally systematic and logical, with minor gaps in documentation. | The examination and description of the digital evidence are incomplete or unclear. There may be inconsistencies in understanding, tool application, or methodology. Fails to follow a recognised forensic framework effectively. |
| Analysis and Findings  35% | Provides thorough, accurate, and well-supported findings for the assigned investigation aspect, with extensive use of supporting artifacts, timestamps, or significant discoveries, and demonstrates a deep understanding of their significance in the context of the investigation. | Provides clear and adequately supported findings for the assigned investigation aspect, with sufficient use of supporting artifacts, timestamps, or significant discoveries, and demonstrates a reasonable understanding of their significance in the context of the investigation. | Findings may lack clarity or coherence, with minimal use of supporting artifacts, timestamps, or significant discoveries, and interpretation may lack depth or fail to address their significance in the context of the investigation adequately. |
| Full and Correct Solution  35% | Presents a complete and accurate solution to the assigned investigation aspect, demonstrating a comprehensive understanding of the case, applying appropriate forensic analysis techniques effectively, and providing clear justification for the solution. | Presents a mostly complete and accurate solution to the assigned investigation aspect, demonstrating a reasonable understanding of the case, applying appropriate forensic analysis techniques effectively, and providing adequate justification for the solution. | The solution may lack completeness or accuracy, with limited understanding of the case, inconsistencies in applying forensic analysis techniques, or insufficient justification for the solution. |
| Conclusion  10% | Concisely summarises key findings, emphasises their relevance to the assigned investigation aspect, and provides an insightful reflection on the investigation. | Summarises key findings highlights their relevance to the assigned investigation aspect and provides a reasonable reflection on the investigation. | The conclusion may lack clarity or completeness in summarising the key findings or their relevance to the assigned investigation aspect, and reflection may lack depth or fail to provide meaningful insights. |
| Documentation and Presentation  5% | The report is well-organised, with a clear structure and logical flow. The language used is highly professional, precise, and effectively conveys the information. Proper citation and referencing are consistently applied. | The report is organised, with a clear structure and mostly logical flow. The language used is professional and conveys the information adequately. Proper citation and referencing are mostly applied. | The report may lack organisation or coherence in its structure and flow. The language used may be inconsistent or imprecise. Citation and referencing may be inconsistent or inadequate. |