|  |  |
| --- | --- |
| **Project Code** |*Kod Projek* | **BITU 3973** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | UNIVERSITI TEKNIKAL MALAYSIA MELAKA  FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY | | | | | | | | | | | | | | | |
| PROJEK SARJANA MUDA 1: PROPOSAL FORM | | | | | | | | | | | | | | | | | | | |
| **A** | **TITLE OF PROPOSED PROJECT** |*TAJUK PROJEK YANG DICADANGKAN* | | | | | | | | | | | | | | | | | | |
| IMPROVEMENT OF MEMORY ANALYSIS TOOLS FOR DIGITAL FORENSIC INVESTIGATION | | | | | | | | | | | | | | | | | | | |
| **B** | **DETAILS OF STUDENT** |*BUTIRAN PELAJAR* | | | | | | | | | | | | | | | | | | |
| Name | | NUR AFIQAH BINTI SHAHRULNIZAM | | | | | **Program:** | |  | |  | |  | |  | |  | |  |
| **BITC** |  | | **BITD** | |  | | **BITI** | |  |  |
|  | |  | |  |
| **Matric No.** | | B032020023 | | | | | **BITE** |  | | **BITM** | |  | |  | | |  |
|  | |  | |  | | |
| **Handphone No.** | | 01156686418 | | | | | **BITS** |  | | **BITZ** | | x | |  | | |  |
|  | |  | |
|  |  | |  | |  | |  | | |  |
| **Semester** | | 2 | **Session** | | 2021/2022 | **Email Address** | | afiqahsnizam@gmail.com | | | | | | | | | | | |
| **C** | **PROJECT INFORMATION** | MAKLUMAT PROJEK | | | | | | | | | | | | | | | | | | |
| **(i)** | **Executive Summary of Project Proposal [Maximum 300 words]** | | | | | | | | | | | | | | | | | | |
| *(Please include the background of the project, problem statements, objectives, and expected outcomes/ proposed solution from the project)*  *Digital forensic contains five steps which are the identification, preservation, analysis, documentation and presentation. Memory analysis or also known as memory forensic describes the volatile data analysis in a computer’s memory dump. Memory analysis tools are used to retrieve data that are hard to be extracted or volatile data when the computer is switched on. The problem of the current tools is that the processing time is slow. The objective of this project is to find the flaw in the processing time that make it slows. This project will later improve it by improving the tool to make it processes faster. Method to do this project is by running all three tools and analyse it to find the processing time and then later improve it by looking up from the free source. From this project, we expect that the small prototype will be able to produce the result of the prototype in which produces faster collection phase result.* | | | | | | | | | | | | | | | | | | | |
| **(ii)** | **Detailed Proposal of the Project** | | | | | | | | | | | | | | | | | | |
| **(a) Introduction** *(Project Background and Problem Statements)* | | | | | | | | | | | | | | | | | | |
| * 1. *Digital Forensics Investigation*   *Digital forensics is the usage of scientifically proven methods towards preservation, collection, validation, identification, analysis, interpretation, documentation and presentation (Reith, M., Carr, C., & Gunsch, G., 2002, p.2). Computer forensic is devided into two steps, which is forensic in the occurrence area and laboratory forensic analysis (Kamal, K. M. A., Alfadel, M., & Munia, M. S., 2016, p.1). Forensic tools are also divided into two parts which are the hardware and software. To complete an investigation, forensic tools are required to capture the data. In this case, memory analysis tools are required in order to get the wanted data.*   * 1. *Problem with Current Memory Analysis Tools*   *With memory analysis tools, there are problems where business commercial software tools are failed in which leads to dependency towards open source tools (Kamal, K. M. A., Alfadel, M., & Munia, M. S., 2016, p.2). There are also problem where the processing time are slow. Windbg tool has a disadvantage where it is isolated from each other (Garcia, G. L., 2007, pg.4)*     * 1. *Steps*   *In this project, we will be focusing on processing time of the 3 tools from open source at collection phase. To achieve the project, we will be following the steps that can be seen as shown in the diagram below.* | | | | | | | | | | | | | | | | | | |
| **(b) Objectives of the Project** | | | | | | | | | | | | | | | | | | |
| *This project embarks on the following objectives*   1. *To analyse the advantage and disadvantage between 3 memory analysis tools.* 2. *To investigate the flaw in the memory forensic tools.* 3. *To test the weakness that is found in the tools.* | | | | | | | | | | | | | | | | | | |
| **(c) Scope of the Project** | | | | | | | | | | | | | | | | | | |
| 1. *Comparing 3 memory analysis tools to find the weakness of the tools from open source.* 2. *Find the weakness or flaw in the forensic tools and analyse it.* 3. *Improving the weakness found from the tools to make it suits the project.* | | | | | | | | | | | | | | | | | | |
| **(d) Expected Outcome/ Proposed Solution** | | | | | | | | | | | | | | | | | | |
| *The expected outcome of this project is to analyse the processing time of memory analysis tools and improvise it to make it faster.* | | | | | | | | | | | | | | | | | | |
| **D** | **REFERENCES** | *RUJUKAN* | | | | | | | | | | | | | | | | | | |
| *State your references (Minimum 10 references)* | | | | | | | | | | | | | | | | | | | |
| **1** | *Gaur, S., & Chhikara, R. (2016). Memory forensics: tools and techniques. Indian J. Sci. Technol, 9(48), 1-12.* | | | | | | | | | | | | | | | | | | |
| **2** | *Garcia, G. L. (2007, October). Forensic physical memory analysis: an overview of tools and techniques. In TKK T-110.5290 Seminar on Network Security (Vol. 207, pp. 305-320). Helsinki: TKK.* | | | | | | | | | | | | | | | | | | |
| **3** | *Case, A., & Richard III, G. G. (2017). Memory forensics: The path forward. Digital Investigation, 20, 23-33.*  [*https://www.sciencedirect.com/science/article/pii/S1742287616301529*](https://www.sciencedirect.com/science/article/pii/S1742287616301529) | | | | | | | | | | | | | | | | | | |
| **4** | *Schramp, R. (2017). Live transportation and RAM acquisition proficiency test. Digital Investigation, 20, 44-53.*  [*https://www.sciencedirect.com/science/article/pii/S1742287617300609*](https://www.sciencedirect.com/science/article/pii/S1742287617300609) | | | | | | | | | | | | | | | | | | |
| **5** | *Arfeen, A., Asim Khan, M., Zafar, O., & Ahsan, U. (2022). Process based volatile memory forensics for ransomware detection. Concurrency and Computation: Practice and Experience, 34(4), e6672.*  [*https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.6672*](https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.6672) | | | | | | | | | | | | | | | | | | |
| **6** | *Thomas, T., Piscitelli, M., Nahar, B. A., & Baggili, I. (2021). Duck Hunt: Memory forensics of USB attack platforms. Forensic Science International: Digital Investigation, 37, 301190.*  [*https://www.sciencedirect.com/science/article/pii/S2666281721000986*](https://www.sciencedirect.com/science/article/pii/S2666281721000986) | | | | | | | | | | | | | | | | | | |
| **7** | *Ahmed, W., & Aslam, B. (2015, October). A comparison of windows physical memory acquisition tools. In MILCOM 2015-2015 IEEE Military Communications Conference (pp. 1292-1297). IEEE.*  [*https://ieeexplore.ieee.org.libproxy.utem.edu.my/document/7357623*](https://ieeexplore.ieee.org.libproxy.utem.edu.my/document/7357623) | | | | | | | | | | | | | | | | | | |
| **8** | *Graziano, M., Lanzi, A., & Balzarotti, D. (2013, October). Hypervisor memory forensics. In International Workshop on Recent Advances in Intrusion Detection (pp. 21-40). Springer, Berlin, Heidelberg.*  [*https://link.springer.com/chapter/10.1007/978-3-642-41284-4\_2*](https://link.springer.com/chapter/10.1007/978-3-642-41284-4_2) | | | | | | | | | | | | | | | | | | |
| **9** | *Varshney, G., Iyer, P., Atrey, P., & Misra, M. (2021, January). Evading DoH via Live Memory Forensics for Phishing Detection and Content Filtering. In 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS) (pp. 1-4). IEEE.*  [*https://ieeexplore.ieee.org.libproxy.utem.edu.my/document/9352935*](https://ieeexplore.ieee.org.libproxy.utem.edu.my/document/9352935) | | | | | | | | | | | | | | | | | | |
| **10** | *Maggio, R. D. (2021). Improving Memory Forensics Through Emulation and Program Analysis.*  [*https://digitalcommons.lsu.edu/gradschool\_dissertations/5528/*](https://digitalcommons.lsu.edu/gradschool_dissertations/5528/) | | | | | | | | | | | | | | | | | | |
| **11** | *Kamal, K. M. A., Alfadel, M., & Munia, M. S. (2016, December). Memory forensics tools: Comparing processing time and left artifacts on volatile memory. In 2016 International Workshop on Computational Intelligence (IWCI) (pp. 84-90). IEEE.*  [*https://ieeexplore.ieee.org.libproxy.utem.edu.my/stamp/stamp.jsp?tp=&arnumber=7860344*](https://ieeexplore.ieee.org.libproxy.utem.edu.my/stamp/stamp.jsp?tp=&arnumber=7860344) | | | | | | | | | | | | | | | | | | |
| **12** | *Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1-12.*  [*http://www.just.edu.jo/~Tawalbeh/nyit/incs712/digital\_forensic.pdf*](http://www.just.edu.jo/~Tawalbeh/nyit/incs712/digital_forensic.pdf) | | | | | | | | | | | | | | | | | | |
|  |  | | | | | | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **E** | **Declaration by student** |*Akuan pelajar* | | | | | | | | | | | | | | | | | | | |
| **(i)** | **Date:** | |  | | **Student’s Signature:** | | | | | | |  | | | | | | | | |
| 9/3/2022 | |  | | | | | | |  | |
|  | |  | | | | | | |  | | | | | | |  | |
| **E** | **RECOMMENDED BY SUPERVISOR**  *PERAKUAN OLEH PENYELIA* | | | | | | | | | | **Recommendation by the Committee**  *Perakuan oleh Jawatankuasa* | | | | | | | | | |
| **(ii)** |  | | | | |  |  | |  | |  | | | |  |  |  | | | |
| **Recommended** | | | | |  | x | |  | | **Accepted** | | | |  | x |  | | | |
|  | | | | |  |  | |  | |  | | | |  |  |  | | | |
|  | | | | |  |  | |  | |  | | | |  |  |  | | | |
| **Not Recommended** | | | | |  |  | |  | | **Not Accepted** | | | |  |  |  | | | |
|  | | | | |  |  | |  | |  | | | |  |  |  | | | |
| **Comments:** | | | | | | | | | | **Comments:** | | | | | | | | | |
|  | | | | | | | | | |  | | | | | | | | | |
| **Supervisor’s Name:** | | | | | | | | | | **Committee’s Name:** | | | | | | | | | |
|  | | | | | | | | | |  | | | | | | | | | |
| **Signature & Stamp:** | | | | | | | | | | **Signature & Stamp:** | | | | | | | | | |
|  |  | | | | | |  | | |  | |  | | | | |  | | |
|  | | | | | | | | | |  | | | | | | | | | |
|  | | | | | | | | | |  | | | | | | | | | |
| **Date:** | | |  | | | | | |  | **Date:** | | |  | | | | | |  |
|  | | | | | | | | | |  | | | | | | | | | |
|  | | | | | | | | | |  | | | | | | | | | |