



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

MOBILE APP TO ANALYSE APK FILES BASED ON YARA RULE

B DETAILS OF STUDENT | BUTIRAN PELAJAR

Name	MUHAMMAD IZHAM BIN NORHAMADI	Program: BITC <input type="checkbox"/> BITD <input type="checkbox"/> BITI <input type="checkbox"/> BITE <input type="checkbox"/> BITM <input type="checkbox"/> BITS <input type="checkbox"/> BITZ <input checked="" type="checkbox"/>			
Matric No.	B032020039				
Handphone No.	019-670 2850				
Semester	2	Session	2021/2022	Email Address	izhamhamadi@gmail.com

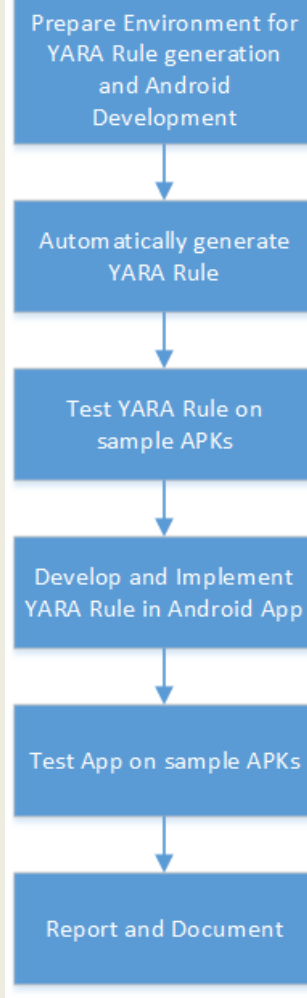
C PROJECT INFORMATION | MAKLUMAT PROJEK

(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)

Android Operating System is one of the most popular and widely used open-source mobile platforms and has the highest mobile market share until this day, making it the most widely used operating system in the world. This fact makes Android users the biggest target group for malware developers as trend analyses show large increase in mobile malware targeting the Android platform which leads to privacy thefts of Android users. The security and privacy of Android apps are very critical, especially that over 6000 apps are added to the Google Play Store every day. Thus, various mobile malware detection systems are proposed in the recent years to address this issue. The objective of this project is to develop a mobile application that can analyse APK files by utilizing YARA Rule. By the end of this project it is expected to produce a functional mobile app that can analyse malware from APK files using certain YARA Rules.

(ii)	Detailed Proposal of the Project
	(a) Introduction <i>(Project Background and Problem Statements)</i>
	<p><i>1.1 Malware Detection and Analysis on Android</i></p> <p>There are two approaches of detecting malwares in Android operating system. The first is the signature based approach in which the derived signature of any application is checked against the malware database, and the other is behavioral detection, where the behavior of the application is checked at runtime with the malicious and normal behavioral profiles. DREBIN is an example of malware detection system that performs a broad static analysis on different sources to excerpt various features such as restricted API calls, utilized permissions, suspicious API calls and network address to detect malicious activity. The dynamic analysis approach for detection of Android malware uses the features that are obtained dynamically at runtime or compile time, features like system call traces and API calls were excerpted and then a machine learning algorithm is used to dynamically detect whether the application is benign application or malicious application. [5]</p> <p><i>1.2 Problem Statement and YARA Rule</i></p> <p>The accelerating rate of malware incidents indicates the magnitude of problem in malware analysis. While malware analysts detect many malware attacks and incidents, keeping pace with the number and different types of attacks poses a significant challenge to malware analysts. There is no true detection solution to malware, as there is no single malware analysis technique with the capability to treat all malware incidents [10]. Known malware signatures in databases have to be actively maintained and updated to be effective [1], as a result analysts select the most suitable malware analysis technique for the specific security incident. This is where YARA rules came handy, YARA rules has emerged as a widely accepted technique for malware analysis due to its flexible and customizable nature, allowing malware analysts to develop YARA rules according to their specific requirements in targeting specific threats [10]. YARA rules can be generated either manually or automatically, both with their pros and cons.</p> <p><i>1.3 App Development framework</i></p> <p>In this project, we will focus on developing the app using open source tools</p>

**(b) Objectives of the Project**

This project embarks on the following objectives:

1. To investigate YARA Rule and its application on malware investigation
2. To develop a suitable YARA Rule and mobile app
3. To assess mobile app using sample APKs

(c) Scope of the Project

1. Automatically generate YARA Rule using open source tools
2. Develop mobile app using Flutter Framework
3. Assess YARA Rule and mobile app

(d) Expected Outcome/ Proposed Solution

The expected outcome in this project is an accessible mobile app that analyses mobile APKs for malware based on YARA Rule

D REFERENCES | RUJUKAN

State your references (Minimum 10 references)

1	Khalid, M., Ismail, M., Hussain, M., & Durad, M. H. (2020, October). Automatic YARA Rule Generation. In <i>2020 International Conference on Cyber Warfare and Security (ICCWS)</i> (pp. 1-5). IEEE.
2	Bayer, U., Moser, A., Kruegel, C., & Kirda, E. (2006). Dynamic Analysis of Malicious Code. <i>Journal in Computer Virology</i> , 2(1), 67–77. doi:10.1007/s11416-006-0012-2
3	Park, J., Chun, H., & Jung, S. (2018, January). API and permission-based classification system for Android malware analysis. In <i>2018 International Conference on Information Networking (ICOIN)</i> (pp. 930-935). IEEE.
4	Talukder, S., & Talukder, Z. (2020). A survey on malware detection and analysis tools. <i>International Journal of Network Security & Its Applications (IJNSA)</i> Vol, 12.
5	Z. D. Patel, "Malware Detection in Android Operating System," <i>2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)</i> , 2018, pp. 366-370, doi: 10.1109/ICACCCN.2018.8748512.
6	Talha, K. A., Alper, D. I., & Aydin, C. (2015). APK Auditor: Permission-based Android malware detection system. <i>Digital Investigation</i> , 13, 1-14.
7	Culling, C. S. Which YARA Rules Rule: Basic or Advanced?.
8	VirusTotal Revision (2021). Welcome to YARA's documentation!. https://yara.readthedocs.io/en/stable
9	Raff, E., Zak, R., Lopez Munoz, G., Fleming, W., Anderson, H. S., Filar, B., ... & Holt, J. (2020, November). Automatic YARA rule generation using biclustering. In <i>Proceedings of the 13th ACM Workshop on Artificial Intelligence and Security</i> (pp. 71-82).
10	N. Naik, P. Jenkins, R. Cooke, J. Gillett and Y. Jin, "Evaluating Automatically Generated YARA Rules and Enhancing Their Effectiveness," <i>2020 IEEE Symposium Series on Computational Intelligence (SSCI)</i> , 2020, pp. 1146-1153, doi: 10.1109/SSCI47803.2020.9308179.
11	Cohen, M. (2017). Scanning memory with Yara. <i>Digital Investigation</i> , 20, 34-43.


E DECLARATION BY STUDENT | AKUAN PELAJAR

(i)	Date: <div style="border: 1px solid black; padding: 2px; display: inline-block;">12/3/2022</div>	Student's Signature: 
-----	--	--

E RECOMMENDED BY SUPERVISOR PERAKUAN OLEH PENYELIA

RECOMMENDATION BY THE COMMITTEE PERAKUAN OLEH JAWATANKUASA

(ii)	<div style="display: flex; justify-content: space-around;"> <div> Recommended <input type="checkbox"/> </div> <div> Accepted <input type="checkbox"/> </div> </div> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div> Not Recommended <input type="checkbox"/> </div> <div> Not Accepted <input type="checkbox"/> </div> </div>
------	---

	Comments: 	Comments:
	Supervisor's Name: 	Committee's Name:
	Mohd Zaki Bin Mas'ud	
Signature & Stamp:  DR. MOHD ZAKI BIN MAS'UD Pensyarah Kanan Jabatan Sistem dan Komunikasi Komputer Fakulti Teknologi Maklumat dan Komunikasi Universiti Teknikal Malaysia Melaka (UTeM)	Signature & Stamp: 	
Date:		Date: