# ABSTRACT

## *ANALYSIS OF THE IMPACT OF MALWARE ON NETWORK TRAFFIC WITH BEHAVIOR-BASED DETECTION TECHNIQUES*

**By**

**ADIB FAKHRI MUHTADI**

**1202154192**

*Malware is a software or computer program that is used to run malicious activity. Malware is created with the aim of harming users because it can spend even a portion of all bandwidth on network traffic. Therefore, research is needed to analyze the impact of malware on network traffic with behavior-based detection techniques. This study aims to determine how the impact of malware on network traffic. This technique analyzes malware by running malware samples into an environment to monitor activities caused by malware samples. To obtain accurate results, the analysis is done by retrieving API call network information and network traffic activities. From the analysis of the malware call network API, the information will be generated about the order of the call network API used by malware. Then from the network traffic, malware activities are obtained by analyzing the network traffic behavior of the infected malware, payload, and traffic bandwidth. Furthermore, from the results of the API call network sequence used by malware and the results of its network traffic analysis, it is analyzed so that it can know what the impact of malware on network traffic and the causes of these impacts.*

***Keywords****: malware, dynamic analysis, behavior-based, network traffic,* API *call network.*