

## ABSTRACT

Instant Messaging software application is a messaging application that is widely used by all levels of society. As a medium for exchanging messages among users of the application without being hindered by time and distance limits, *Telegram* is a cloud-based multiplatform instant messenger application that is widely used around the world. This application is being used today because it is free and can be used via smartphones and computer devices. Users can exchange messages, photos, videos, audios, stickers, and other types of files. *Telegram* also provides end-to-end message exchange. This technology can be misused for crimes such as the spread of pornography or cybercrime cases. Currently, the solution is to conduct digital forensics on cybercrime cases that have been occurred. In the case of a terrorist group in Indonesian, it was found using the *Telegram* application as a means of communicating among members. this final project conducts forensic investigation on *Telegram* instant messaging application and an Android device In conducting an investigation, investigators create a model to analyze forensic results on Android that contain artifacts or what are often called Data Remnants. Data Remnant is a package generated from storage media obtained from *Telegram* after carrying out digital forensic activities on digital evidence in the form of these artifacts. In this final project, to carry out this investigation carried out are looking for artifacts or Data Remnants generated from *Telegram* on Android during the investigation process using the data crawling method or often called the data collection method. This final project aims to obtain digital evidence from cybercrime cases and become reference material for forensic science.

*Keywords : Cybercrime, Telegram, Digital Forensic, Data Remnant*