I. INTRODUCTION

In the last decade, communication technology has been rapidly evolving. These advances are followed by the increase in technology users, one of which is the massive use of smartphones which have become a major influence on the significant development of various social media and instant messenger applications. Instant messenger applications can be used for free to communicate with other users in real-time either through text, audio, or video calls. It can also be useful to share location information, documents of any type, or other convenient features.

Among various instant messaging applications, WhatsApp and Telegram Messenger are two of the most widely used applications. Based on the data in 2022, WhatsApp has gained more than two billion monthly active users worldwide [1] while Telegram Messenger has reached around 500 million monthly active users per April 2022 [2]. WhatsApp and Telegram Messenger have a feature that can be accessed according to the user's wishes. The use of these instant messenger applications is not only a medium for exchanging messages but also for carrying out unlawful actions such as online fraud, identity theft, selling illegal goods, etc. by taking advantage of access to this feature. Violation of the law that utilizes computer technology or by using internet access is referred to as cybercrime [3].

In the case of cybercrimes, law enforcement should conduct digital forensics which is a method used for finding evidence left behind from a cybercrime. This study examines digital forensic analysis on android-based instant messenger applications, especially WhatsApp and Telegram. The forensic analysis approach is used for describing the evidence or artifacts obtained during digital forensics and explanation are provided regarding the information associated with digital evidence data. The followings are the steps taken in this study to obtain valid digital forensic analysis results:

1) Conducting cybercrime simulations of fraudulent online buying and selling of goods between victims and perpetrators by using WhatsApp and Telegram as the conversation medium.
2) Discussing the evidence collection process and the validation of the evidence obtained from WhatsApp and Telegram.
3) Explaining the contents of the conversation data obtained from the cybercrime simulation, such as evidence of the conversation chronology, user ID, contact info, the sent messages (text, image, video, or sound), the incoming and outgoing message scenarios, and the evidence of message deletion.

Section II of this paper reviews the literature and references used for this study while section III describes the methodology used in the analysis process. Meanwhile, section IV explains the process of forensic analysis carried out and, lastly, section V presents the conclusion of this study.