# Abstract

The rapid development of information technology has significantly impacted social media platforms, including Twitter, which is often misused for crimes such as the distribution of pornography. This research focuses on analyzing digital evidence related to pornography crimes on Twitter using static forensics and the National Institute of Standards and Technology (NIST) framework for computer forensics, adapted to the researcher's workflow. The research process involved forensic tools FTK Imager and Autopsy. The results demonstrate that the static forensic method is ef ective with 100% accuracy in uncovering and collecting evidence, including files deleted by the suspect using the Twitter account @Kai_jon75364 on their laptop through standard deletion methods. The analysis identified deleted image files and successfully recovered critical data, such as photo files that were originally in .jpeg format and converted to .png, along with other files that remained in the Pictures folder. This research also evaluated advanced deletion methods, including Shift+Delete and wipe, revealing that although files deleted by these methods can be recognized, static forensics cannot ef ectively recover them. Additionally, the research successfully traced the origins of the images owned by the suspect, showing that some images were screenshots from the internet, while others were transferred from another device to the suspect's laptop via an external device. This research highlights the limitations of static forensics in detecting data deleted using advanced deletion methods.
**Keyword**: static forensic, Twitter, social media, digital evidence, Digital forensic, NIST.