

### *Abstract*

*In digital forensic activities, efforts to maintain the integrity of digital evidence are important concern. One of effort to maintain the integrity of digital evidence is to ensure that secondary storage is used to store duplicate results of digital evidence are completely empty, so that digital evidence is not contaminated. How to empty secondary storage can be done through a removal technique that is in accordance with forensic rules.*

*In this study, manual removal techniques were carried out on secondary storage (using shift delete and format techniques) and using wiping techniques with NTFS file systems. In testing the removal deletion technique use the one zero pass method with the Active Kill Disk tool. Testing is done through data recovery testing using Disk Drill Pro software. The test results aim to compare three data deletion techniques that are suitable for emptying secondary storage based on whether or not the data has been successfully restored. After analyzing the test results, the author made a visualization of the deletion technique in the form of an animated storyboard that served to explain the comparison of deletion techniques to people with non-IT backgrounds. Based on the results of research, the shift delete and format deletion techniques do not completely empty the secondary storage, while the wiping deletion technique can empty the secondary storage in accordance with the rules of digital forensics.*

*Keywords: Forensik Digital, Secondary Storage, Wiping.*