Analysis of the Effective Turning-Off Methods for Computer Forensics

1st Muhammad Naufal
School of Computing
Telkom University
Bandung, Indonesia
zachfal@student.telkomuniversity.ac.id

2nd Niken Dwi Wahyu Cahyani
School of Computing
Telkom University
Bandung, Indonesia
nikencahyani@telkomuniversity.ac.id

3rd Erwid Musthofa Jadied
School of Computing
Telkom University
Bandung, Indonesia
jadied@telkomuniversity.ac.id

A consistent protocol for collecting and analyzing digital evidence can solve this problem. This protocol will include guidelines for identifying and protecting critical system artifacts and instructions for proper computer shutdown. By following this protocol, forensic investigators can ensure the accuracy and reliability of the evidence collected, regardless of the shutdown method used.

I. Background

The scientific process of obtaining, analyzing, and preserving data contained in electronic media that can be used as evidence in court is known as digital forensics [1]. This process involves examining various system artifacts to discover user actions, system logs, and other relevant information. As more and more criminal activities are carried out using digital devices, digital forensics is becoming increasingly important in today's world.

A study from the National Institute of Standards and Technology (NIST) found that traditional techniques for shutting down a computer, such as giving a shutdown command or pressing the power button, may not shut down the computer completely, leaving data vulnerable to tampering or theft. According to this study, understanding how various kill techniques affect digital evidence collected during forensic investigations [2]. It is recommended that this problem be avoided more safely, such as by turning off the power source or removing the laptop battery [3].

Forensic investigators face significant problems when using non-standard shutdown methods, as they can produce incomplete or inaccurate results, which can jeopardize the integrity of the investigation. Therefore, it is essential to examine how various shutdown techniques affect digital evidence. Controlled experiments using shutdown methods such as shutdown commands, power buttons, and cutting off the power supply can be used to measure their effects on system artifacts and evidence reliability.