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

***Abstract*— The decision between forced shutdown and normal shutdown is crucial regarding memory artifact recovery in computer forensics. For stand-alone and network-connected client computers, a forced shutdown is usually performed by abruptly unplugging the power supply, often recommended as it efficiently retrieves temporary data, namely pagefile.sys. While computer forensic experts typically advise forced shutdowns for forensic purposes, there is insufficient data to validate this procedure unequivocally. This research aims to fill that gap by providing empirical evidence on the effectiveness of forced shutdowns compared to normal shutdowns on Windows 10. Our findings indicate that forced shutdowns capture complete artifact data, whereas normal shutdowns lose two critical artifact data points. By providing evidence-based results on optimal shutdown procedures, this research could significantly give confident, solid justification to standardized protocols that ensure data integrity and reliability of digital evidence.**

Keywords—force shutdown, normal shutdown, computer forensics, memory artifact, operation system, pagefile.sys