



Multimedia Section
Technical Procedure for Wiping Media
Digital and Multimedia Evidence Division



1. TECHNICAL PROCEDURE FOR WIPING MEDIA

1.1. Purpose

- 1.1.1. The purpose of this procedure is to completely wipe digital media from destination drive, when applicable, in order to restore a source forensic image to that drive.
- 1.1.2. The intent is to ensure that the destination drive contains no remnant files that may contaminate the source files copied to the destination media. The destination drive can then be inserted into the original device for native examination of the source content, if needed.
- 1.1.3. This process prevents contamination or deleterious changes to the original source media by using a substitute drive for the examination.

1.2. Scope

- 1.2.1. This procedure describes the steps taken for the secure wiping of data on target drives by Multimedia Section analysts.

1.3. Equipment

- Forensic workstation, or external stand-alone media wiping device
- Approved software or hardware device(s) for wiping data
- Device to be wiped

1.4. Procedure

- 1.4.1. Select an appropriate forensic target drive of suitable size and characteristics to be wiped.
- 1.4.2. Attach the forensic target drive to be wiped to the appropriate forensic workstation.
- 1.4.3. Use an approved hardware wiping device or wiping software to remove all information from the target drive.
 - 1.4.3.1. Note that EnCase will wipe a target hard drive prior to restoring a forensic image as part of the process.
- 1.4.4. The following information should be documented in the technical case record:
 - Date and time the forensic wiping was initiated
 - Hardware and software (include version) used to wipe the target device
 - Unique identifier for the forensically wiped media (i.e. drive characteristics, make, model, serial number or lab designator written in indelible marker on the label)
 - Record if the wipe fails.

1.5. Limitations

- 1.5.1. Due to media architecture limitations, software wiping utilities likely will not be successful or possible on tape drives, CDs/DVD, Blu-ray or other media. Reuse of this media for forensic purposes is not recommended.



1.5.2. Wiping is generally only performed on hard drives.

1.5.3. Damaged hard drives that cannot be completely or successfully wiped should be physically destroyed. Absent a successful wiping process, data overlap contamination may occur. Wiping must be properly completed to safeguard the process.

1.6. References

- EnCase Forensic User Manual
- EnCase Intermediate Analysis and Reporting Course Guide
- EnCase Advanced Computer Forensics Course Guide
- Tableau User Guide for TDW1 and TD2