

Goal:

Learn how to
delete sensitive
electronic data



Security Threats

Digital information everywhere!

“Deleting” a file doesn’t really delete it

File versions are constantly created and *insecurely* deleted

Files are recoverable until they are written over

SOLUTION: *Wiping* data

Eraser

Free, open source tool for permanently wiping data

Permanently wipes:

- Deleted files
- Contents of Recycle bin
- Free (unallocated) disk space

NO recovery option



CCleaner

Free tool for permanently wiping data

Permanently wipes

- Temporary files
- Free disk space

NO recovery option



Tips

Before:

- Create an encrypted backup of important files
- Delete all unnecessary files and empty recycle bin

When Wiping:

- Wipe temporary files with Ccleaner
- Wipe all unallocated (free) space with Eraser
- Wipe Windows swap file with Eraser

Long-Term:

- Wipe sensitive files AND wipe periodically