

Capture & Cease – Disk Forensics Recovery Report

Summary

This report documents a simulated digital forensic investigation focused on recovering deleted image files from a suspect disk partition using industry-standard tools.

Objectives

- Recover deleted image files using forensic tools. - Validate recovered file integrity using hash analysis. - Generate clear documentation for potential legal or internal use.

Tools Used

Tools Utilized: • FTK Imager – For disk image mounting and sector-level inspection. • Autopsy – For deleted file recovery and EXIF metadata extraction. • HashMyFiles – For SHA256 hash comparison and validation.

Findings

Three deleted image files were successfully recovered from the provided disk image. All recovered files were verified using SHA256 hashes and found to be intact, with no evidence of tampering. Metadata analysis provided timestamp and device information for chain-of-custody purposes.

Conclusion

The simulated forensic recovery was successful. The integrity of recovered files was validated and documented. This process demonstrates fundamental disk forensics procedures applicable to real-world investigations.