

Digital Evidence

Criminal Justice

How devices and accounts are imaged, verified and examined without altering them.

Work on a verified copy, never on the original.

1

Identify and isolate

Locate devices and prevent remote wiping or further writes.

2

Acquire

Take a forensic image rather than examining the original device.

3

Verify

Hash the image and source to show the copy is faithful.

4

Analyse

Examine the copy, recording tools, versions and every action taken.

5

Report

State what was found, what was inferred and what remains unknown.

Educational reference. Attributing activity to a person is an inference about who was using a device, not a direct reading.