

Chris Fullerton

Github ethics and law

My First hour priorities

First thing to do is get the system and network logs and establish a timeline

Volatile memory snapshots capture running processes and connections and potential malware in ram before its gone.

Get the copies of important documents to see if they were changed and check if anything was leaked.

Avoid

Make sure to stay legal and careful to not get any personal information when getting into a device.

All captured evidence is hashed (e.g., **SHA-256**) at the time of collection to verify integrity during the investigation. Files are stored in a **secured evidence repository** with access logged and restricted to authorized personnel only. A **redaction policy** is applied to remove or mask unnecessary PII, credentials, or unrelated user data, ensuring only the minimum necessary information is retained for analysis while protecting privacy.