Community operational security guidelines for consensual forensic practicioners

This section consolidates operational security guidance for acquisition frontliners and forensic analysts using AQF and MVT.

Workstation preparation

`Dedicated acquisition device.` Use a single purpose device for acquisition (such as a dedicated laptop, Raspberry Pi or similar). Never use a personal or work machine that holds other sensitive data or credentials to organizational infrastructure.

`Full disk encryption.` Mandatory on both acquisition and analysis workstations. This is the primary defense against a Physical Seizure scenario. Use LUKS on Linux, FileVault on macOS or BitLocker on Windows. Ensure the machine is powered off (not just suspended) when not in use.

Per-case isolation

`Fresh working directory per case.` Never reuse output directories across cases. Verify the output directory is empty before starting acquisition or analysis.

`Manual bundle verification.` After acquisition, verify the bundle contains expected artifacts (`packages.json`, `getprop.txt`, `bugreport.zip`, `files.json`, `dumpsys.txt`, etc.). A missing or empty file could mean the collection failed silently.
Note that if the acquisition output was encrypted using a third party's public key, it is not possible to decrypt the bundle to perform this verification.

Encryption and key management

`Always encrypt during acquisition.` Place a valid age public key in `key.txt` alongside the AQF binary. Never transport plaintext bundles between acquisition and analysis stages. If encryption is unavailable, treat the plaintext bundle as highly sensitive and transfer it to the analyst via an encrypted channel, then securely delete the local copy.

`Verify encryption is active.` Use AQF with the `-v` verbose flag to verify that encryption is enabled and working correctly.

`Key separation.` Store the private key (the counterpart to the public key used as `key.txt` during acquisition) on a different physical medium than the bundle (different USB stick, different device). Never store the private key on the

acquisition workstation. If the workstation is seized, the encrypted bundle is useless without the key.
If no access to plaintext logs is needed at the acquisition stage, consider using the analyst's public key for encryption to avoid holding unnecessary decryption capability. Note that this prevents the frontliner from verifying bundle contents, so collection errors may go undetected until analysis.

Acquisition hygiene

`Disable Developer Options after acquisition.` Immediately disable Developer Options on the HRD device after acquisition is complete. AQF already displays this reminder, but it is easy to overlook under time pressure.

`ADB authorization key hygiene.` When the device prompts "Allow USB debugging?", do not check "Always allow from this computer." Opting in to persistent trust stores the acquisition workstation's ADB RSA public key on the HRD device. The tradeoff is that the operator may need to be attentive to additional authorization popups on the phone during acquisition.

Sample transfer and handoff

`Encrypted transfer channel.` Transfer samples only over encrypted channels. For example, an age encrypted file sent via Signal, OnionShare or trusted third-party platforms with end-to-end encryption.

Sample integrity

`Use the -H flag.` Run MVT with `--hashes` (`-H`) to compute SHA256 hashes of the input bundle and record them in `info.json`. This creates an independent record of exactly what was analyzed.

Post-analysis data handling

`Securely delete plaintext material.` After findings are communicated, securely delete plaintext bundles, decrypted samples, and analysis output from the analysis workstation. Use `shred` on Linux or equivalent secure deletion tools. On SSDs, be sure to enable full disk encryption as secure deletion is unreliable at the file level.

`Retain only encrypted copies.` If long-term storage is needed, retain only the encrypted bundle. The analyst may not need to keep the raw bundle after producing findings.

`Document a data retention policy.` Per engagement, define: what is kept, for how long, where it is stored, and who has access. Communicate this policy to the HRD whose device was acquired for consent.

Physical seizure preparedness

`Assume seizure is possible.` The question is not "will it happen" but "what will they find." Design your operational setup so that a seized workstation yields nothing usable.

`Full disk encryption.` Mandatory on both acquisition and analysis workstations. This is the primary defense against a Physical Seizure scenario. Use LUKS on Linux, FileVault on macOS or BitLocker on Windows. Ensure the machine is powered off (not just suspended) when not in use.

Leverage age encryption of samples. If the bundle is age-encrypted and the private key is stored elsewhere (different USB stick, different device, with a different person), a seized workstation contains only opaque encrypted data.

Additional operational practices

Verify AQF binary integrity before use. AQF is distributed as a standalone binary from GitHub releases. The frontliner should verify the binary's SHA256 checksum against the published release hashes before use.

Compartmentalize acquisition and analysis workstations. If possible, use separate physical machines for acquisition and analysis. The acquisition workstation connects to potentially compromised devices via USB/ADB, while the analysis workstation operates only on bundle files.