National Forensics Agency

Standard Operating Procedures

NATIONAL FORENSICS AGENCY

H-11/4 Islamabad Capital Territory Pakistan

1. Introduction

The National Forensics Agency (NFA) provides comprehensive digital and conventional forensic services. Established to combat modern crimes such as digital terrorism, and white-collar offenses, the NFA ensures the integrity, legality, and admissibility of digital evidence in court. This document outlines the SOPs for handling, submitting, and analyzing digital evidence to assist the public.

2. Guidelines for Handling Digital Evidence

2.1. Precautions and Care

- Secure the scene and ensure no unauthorized access to evidence.
- Avoid touching or moving items unless necessary. Use gloves (latex or anti-static) and document all actions.
- Record the state of devices (e.g., powered on/off) and take photographs of the scene.

2.2. Preservation of Evidence

Handle devices carefully to avoid data loss or corruption:

I. Computers

- Power off safely; capture/dump RAM if volatile data is critical.
- Document device details (model, serial numbers) and handle components with anti-static precautions.

II. Mobile Phones

- Put in airplane mode, disconnect from the network (e.g., turn off Wi-Fi, mobile data, and Bluetooth) or Place in Faraday bags.
- Photograph the device and record visible details (e.g., lock screens, damage).

III. Storage Devices

- Handle HDDs, SSDs, USB drives, and RAID systems with care.
- Use anti-static bags and avoid physical damage
- Avoid powering on devices unless necessary.

IV. Drones

- Safely powered down, secure storage devices and any logs
- Document model, serial number, and current status (e.g., powered on/off).

V. DVR/NVR/Video Systems

- Properly powered, secure any connected cameras or audio devices and store DVR/NVR/Storage devices in anti-static packaging.
- Document the date and time

VI. Audio/Video and Image files

- The original audio, video and Images files (not compressed) along with the source device should be sent for forensic analysis.

VII. Digital Wallets

- Secure hardware wallets in anti-static/Faraday bags.
- Document software wallet files and credentials without accessing them.

VIII. Gaming Consoles

- Power off and document details (model, serial number).
- Maintain chain of custody for integrity.

Label and seal all evidence with essential details (e.g., case number, date, officer's name).

2.3. Documentation and Chain of Custody

Maintain a detailed log of:

- Date, time, and location of seizure.
- Identity of officers involved.
- Observations and condition of evidence.
- Use a Chain of Custody Form (Annexure-B) to track possession and ensure continuity.

2.4. Transportation

Use secure packaging (e.g., Faraday bags, anti-static bags, shockproof containers).

Avoid exposure to magnetic fields, extreme temperatures, or humidity.

3. Submission of Evidence to NFA

3.1. Requirements for Submission

- Complete the Digital Forensic Request Form (DFRF) with case details (refer to Annexure A).
- Include:
    - Seizure memo and Chain of Custody documents.
    - Case summary justifying forensic analysis.

3.2. Packaging and Transport

Package evidence securely to prevent contamination:

- Use Faraday bags for mobile phones and drones.
- Use anti-static strips and anti-static bags for storage devices.
- Label packages clearly with case details and seal them.

4. Post-Analysis Steps

4.1. Reporting

NFA provides a detailed forensic report outlining findings and conclusions.

4.2. Evidence Return

Evidence is returned to the submitting party with a signed receipt.

4.3. Legal Admissibility

Ensure all procedures comply with legal standards to maintain admissibility in court.

5. Conclusion

The NFA's SOPs for digital forensics are to ensure the precision, integrity, legality, and admissibility of evidence in investigations. The LEAs are requested to follow the above SOPs to effectively combat digital crimes and other offenses in the digital domain.

Annexures

Annexure B: Digital Forensic Analysis Form (DFAF).

Annexure C: Chain of Custody Form.

Note: For Further Details Visit (www.nfa.gov.pk)