General Principles for Digital Evidence

PREAMBLE

The Conference of International Investigators (CII) has endorsed the Uniform Principles and Guidelines for Investigations (the "Investigation Guidelines").[1] These General Principles for Digital Evidence supplement the Investigation Guidelines and were endorsed by the CII at its 21st Conference in May 2021.

The purpose of these General Principles is to define common principles for the proper handling of digital evidence by investigators, external service providers, or other functions within an Organisation handling digital evidence on behalf of, or in collaboration with, Investigative Offices.[2]

The most crucial aspect of digital investigations is to ensure the reliability of digital evidence. In a digital age, most (if not all) investigations involve digital evidence, and all investigators should be familiar with current best practices for handling digital evidence. These principles will focus on the integrity, confidentiality and authenticity of digital evidence.

The General Principles for Digital Evidence synthesize recommendations from practitioners who are knowledgeable about the subject matter, scientific research and best practices. Because of the complex issues associated with digital evidence, these recommendations may not be feasible in all situations. The principles do not offer the only possible correct course of action but present the most widely accepted recommendations and practices.

These General Principles do not, and are not intended to, bind any Organisation, its Investigative Office, or its personnel; confer, impose, or imply any duties, obligations, or rights on them or on any third parties; or affect their rights and obligations under applicable rules, policies, and procedures (their "Policies"), including any privileges and immunities afforded to them by international treaty, customary international law, or the laws of any respective member state. These General Principles are to be utilized within the framework of each Organisation's Policies and the exercise of an Investigative Office's professional judgment and expertise.

GENERAL CONSIDERATIONS

1. Digital evidence is defined as information and data of potential value to an investigation that is stored or transmitted in digital form. Digital evidence differs from traditional evidence in multiple ways:

    a. It is often highly complex, frequently scattered among different physical or virtual locations, and requires expertise and tools to collect.

    b. It can easily be altered, accidentally or intentionally, possibly without leaving any trace.

    c. It can easily be copied and distributed, presenting challenges to preserving confidentiality.

    d. It can be temporary in nature: network logs, Internet browsing history, social media posts, instant messages, cached data and deleted data can be lost if not preserved in a timely manner.

---

[1] The Investigation Guidelines were endorsed by the Fourth CII in 2003. The second edition was endorsed by the Tenth CII in 2009.

[2] Consistent with the Investigation Guidelines, "Organisation" includes all institutions participating in the CII, and "Investigative Office" refers to the units or functions of an Organisation mandated to investigate allegations of wrongdoing—as defined by the Organisation—within the Organisation or associated with its projects and activities.

2. As a result, special consideration is necessary to establish authenticity, protect integrity and maintain the confidentiality of digital evidence. These considerations include:

    a. Ensuring that collection of digital evidence is properly authorized and conducted in compliance with Organisational policies.

    b. Documenting the collection and preserving the documentation for later review.

    c. Not altering the digital evidence, unless it is necessary, and only by a trained person.

    d. Documenting all interactions with the evidence.

    e. Establishing a Chain of Custody as soon as possible.

    f. Backing up the digital evidence and only working with copies.

    g. Ensuring that evidence and all copies are securely stored, transported and disposed of.

IDENTIFICATION

3. At the beginning of an investigation, all possible sources of digital evidence potentially relevant to the investigation should be identified and preserved. Digital evidence can be of a temporary nature and time is of the essence!

4. Possible sources of digital evidence include computers, mobile devices, external storage media, network servers, cloud storage and the Internet.

5. To limit data volumes and to reduce the possibility of collateral intrusion, the proportionality and relevance of digital evidence should be carefully considered. The collection of digital evidence and/or the scope of digital forensic examination should reflect this.

COLLECTION

6. To ensure the reliability of digital evidence, it is crucial not to modify the evidence. Any action that could potentially modify evidence should only be undertaken by a person specifically trained to do so, and all steps should be documented.

7. Interactions with live (powered on) devices should be kept to a minimum, as they are likely to modify and overwrite potentially relevant data. Mobile devices should be disconnected from all networks to prevent remote wipe.

8. If the device is powered on, it should be turned off as soon as possible. If live data could be of interest, encryption is enabled, or a passcode to unlock a mobile device cannot be obtained, the device should be kept powered on and a digital forensic expert should be consulted.

9. Performing a proper shutdown typically commits multiple writes to the internal storage device. To prevent this, a device can be powered off by removing the power cord and/or batteries.

10. As internal storage drives are increasingly difficult to remove, it can be more practical to collect the device and the power cord instead.

11. In circumstances where physical collection is not feasible, a computer can be acquired via a network using remote collection tools.

CHAIN OF CUSTODY

12. The Chain of Custody for digital evidence is the chronological documentation of its handling from the time of collection until its disposal. The Chain of Custody can consist of signed paper forms, photographs, investigator's notes, examination reports, automatically generated logs and forensic hashes.

13. The Chain of Custody should uniquely identify the evidence. Computers, phones and other storage media can be identified by recording the manufacturer's name, model number and serial number. If no unique identifier exists, evidence can be tagged, labelled or bar coded for that specific purpose.

14. Digital evidence such as emails, digital documents, multimedia files or website captures can be identified by how, when and from whom it was received; or by how, when and from where it was collected.

15. As a minimum, the Chain of Custody should document the following:

    a. The person collecting or receiving the evidence.

    b. The source of the evidence.

    c. Date and time, including time zone information where applicable.

    d. Unique identifiers.

    e. How the evidence was collected, including the tools and methods used.

    f. Any additional documentation as required by the Organisation.

FORENSIC HASHES

16. Forensic hashes, sometimes referred to as digital fingerprints, are values that uniquely identify digital evidence. Forensic hashes are used to verify the integrity of all types of digital evidence and to verify that copies are identical to the original.

17. Forensic hashes are computed using mathematical functions, most commonly the Message Digest (MD5) and Secure Hash (SHA) algorithms. Forensic hashes should be computed immediately when the evidence is collected or received and should be stored securely together with the original evidence.

EXAMINATION

18. Examination of digital evidence should only be performed on work copies.

19. Computers, mobile devices and original external storage media should only be examined by trained digital forensic examiners. Browsing a computer/mobile device or connecting an external storage device to preview its content could compromise the integrity of digital evidence and should be avoided.

20. When using analysis tools that use keyword searches, care should be taken that either an Optical Character Recognition (OCR) tool was used to convert all non-searchable content before indexing, or non-searchable documents such as document scans are manually reviewed.

21. For data and network security reasons, it is recommended that digital evidence is examined on a dedicated computer isolated from all networks.

22. Using personal computers or storage media to store or view digital evidence and using personal accounts to search for or download information from the Internet should be avoided.

23. All tools and methods used for the examination of digital evidence should be documented.

AUTHENTICATION

24. Investigators should be aware that digital evidence can easily be manipulated without leaving any trace.

25. It is recommended that digital evidence provided by third parties, e.g., subjects, complainants or witnesses is authenticated. Evidence should preferably be collected directly from its native environment, e.g., a computer, a mobile device, a social media account or a website.

26. If collection from the source is not possible (e.g., a witness is not willing to submit their personal device for digital forensic acquisition), the investigator should attempt to verify the evidence by confirming its existence on the original device or the online account.

27. Document metadata that is not examined in its native environment (the device used to create or modify the document) should not be taken at face value.

STORAGE, TRANSPORT AND DISPOSAL

28. To maintain confidentiality, access to all digital evidence (including work copies) should be limited to authorized personnel only.

29. If evidence is stored on networked servers, or is being transmitted through networks, strict access control and encrypted transmissions should be used. Portable storage devices used to transport evidence should be encrypted.

30. Digital evidence should be transported in appropriate packaging and protected from extreme temperatures, humidity, physical shock, static electricity and magnetic fields.

31. Every computer and storage device used to store or view digital evidence should be properly sanitized before it is transferred to another user or recycled.

PUBLICATION AND IMPLEMENTING GUIDELINES

32. These General Principles have been endorsed by the CII. Any Organisation may refer to these General Principles in its own Policies or may publish them itself in accordance with its Policies. In addition to these General Principles, in July 2020 the Inter-Agency Digital Investigations Working Group (DIG) published *Digital Evidence Guidelines* which may be used for further non-binding guidance.