

The Role of Digital Evidence in Legal Proceedings

From discovery to court, how digital evidence is gathered, preserved, and used in South Africa.



Why do we need Digital Forensics?

This presentation delves into the Digital Forensic Standard within South Africa, emphasizing the interplay between the legal framework, pertinent international standards, and the vital functions performed by digital forensic practitioners. Understanding these components is crucial for ensuring the integrity and admissibility of digital evidence in legal proceedings.



Data Vs Fingerprints & DNA

2000

ACPO Principles in Digital Forensics



No actions taken by investigators should change the data which may be subsequently relied upon in court.

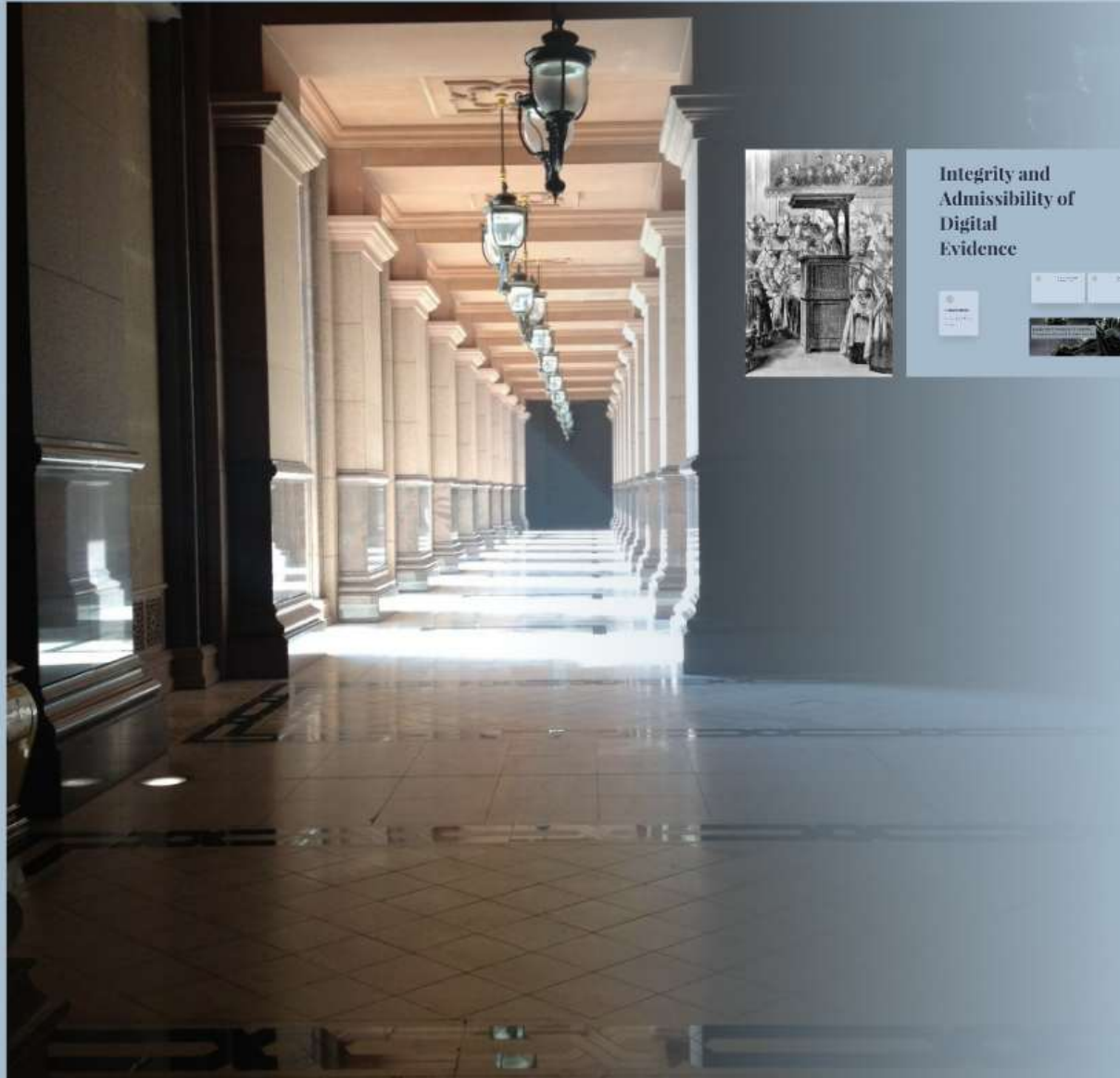


Only in exceptional situations should investigators work with or access the original data and only if they are competent to do so



All processes applied to the digital evidence by investigators should be fully recorded to enable independent third-party review





Legal Requirements for digital evidence

Integrity and Admissibility of Digital Evidence



Constitution

Privacy - Search & Seizure

Fair trial



Section 14: Originality and Integrity of Evidence

14. (1) Where a party produces evidence in a proceeding in reliance on the originality and integrity of the evidence, the court shall, in determining whether to admit the evidence, consider the following factors:

- (a) the reliability of the evidence;
- (b) the reliability of the person who provided the evidence;
- (c) the reliability of the process by which the evidence was obtained;
- (d) the reliability of the evidence as presented to the court.



Section 15: Admissibility of Digital Evidence

15. (1) Where a party produces evidence in a proceeding in reliance on the originality and integrity of the evidence, the court shall, in determining whether to admit the evidence, consider the following factors:

- (a) the reliability of the evidence;
- (b) the reliability of the person who provided the evidence;
- (c) the reliability of the process by which the evidence was obtained;
- (d) the reliability of the evidence as presented to the court.

Regulatory Framework: Electronic Communication and Transaction Act



Constitution

Privacy - Search & Seizure

Fair trial



Section 14: Originality and Integrity of Evidence

14. (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if:

- a. the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and
- b. that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1(a), the integrity must be assessed:

- a. by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
- b. in the light of the purpose for which the information was generated; and
- c. having regard to all other relevant circumstances.



Section 15: Admissibility of Digital Evidence


15. (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence:

- a. on the mere grounds that it is constituted by a data message; or
- b. if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to:

- a. the reliability of the manner in which the data message was generated, stored or communicated;
- b. the reliability of the manner in which the integrity of the data message was maintained;
- c. the manner in which its originator was identified; and
- d. any other relevant factor.



Regulatory Framework: Electronic Communication and Transaction Act



Section 14: Originality and Integrity of Evidence

14. (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if-
- a. the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and
 - b. that information is capable of being displayed or produced to the person to whom it is to be presented.
- (2) For the purposes of subsection 1(a), the integrity must be assessed-
- a. by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
 - b. in the light of the purpose for which the information was generated; and
 - c. having regard to all other relevant circumstances.



Section 15: Admissibility of Digital Evidence

15. (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence-
- a. on the mere grounds that it is constituted by a data message; or
 - b. if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
- (2) Information in the form of a data message must be given due evidential weight.
- (3) In assessing the evidential weight of a data message, regard must be had to-
- a. the reliability of the manner in which the data message was generated, stored or communicated;
 - b. the reliability of the manner in which the integrity of the data message was maintained;
 - c. the manner in which its originator was identified; and
 - d. any other relevant factor.

Creation of Forensic Copies and Data Processing

Write Blocker
Hash value

Adherence to Legal and Ethical Standards

Filter Team
Exonerating evidence

Support for Judicial Processes

Expert Opinion



Role of Digital Forensic Practitioners

Creation of Forensic Copies and Data Processing

Write Blocker
Hash value

Adherence to Legal and Ethical Standards

Filter Team

Exonerating evidence

Support for Judicial Processes

Expert Opinion

Overview of International Standards



ISO 27041

Information Security Management System (ISMS) Requirements for Cloud Computing

ISO 27037

Information Security Management System (ISMS) Requirements for Cloud Computing

ISO 27042

Information Security Management System (ISMS) Requirements for Cloud Computing

International
Organisation of
Standardization
Standards

ISO 27043

13 Phases Model

Parallel Processes

- Authorisation
- Chain of Custody

ISO 27037

Primary Principles

- Relevance
- Reliability
- Sufficiency

Auditable
Repeatable

- When the same procedures and methods are used.
 - When the same equipment under the same conditions is used.
- Reproducibility:
- When the same method is used.
 - When different equipment is used under different conditions.
 - When the same results can be reproduced at any time after the original test.
- Justifiable

ISO 27042

Report findings as fully and impartially as possible. In order to achieve this, adopt a structured approach to investigation, carried out by competent and proficient investigator

ISO 27043:2016 Information security -- Incident response -- Guidelines for the investigation and analysis of information security incidents
ISO 27037:2016 Information security -- Incident response -- Guidelines for the investigation and analysis of information security incidents
ISO 27042:2016 Information security -- Incident response -- Guidelines for the investigation and analysis of information security incidents

International Organisation of Standardization Standards

ISO 27043

13 Phases Model

Parallel Processes

- Authorisation
- Chain of Custody

ISO 27037

Primary Principles

- Relevance
- Reliability
- Sufficiency

Auditable

Repeatable

- When the same procedures and methods are used.
- When the same equipment under the same conditions is used.

Reproducibility:

- When the same method is used.
- When different equipment is used under different conditions.
- When the same results can be reproduced at any time after the original test.

Justifiable

ISO 27042

Report findings as fully and impartially as possible. In order to achieve this, adopt a structured approach to investigation, carried out by competent and proficient investigator

To ensure that the outcome of an investigation is reliable, it should be performed by a "competent investigators using examinations which are composed of validated analytical processes, in which they are proficient, and ensuring that every item of digital evidence produced can be traced back to the source of potential digital evidence from which it is derived"

Competence:
"sufficiently familiar with, and experienced in, the tools, methods and techniques which he will use to be able to carry them out with minimal supervision and should also be able to recognise the limits of their own abilities".

Proficiency:
If he is given a sample set of evidence, he produces equivalent results to another competent Digital Forensic Practitioner, using a similar analysis.

A Digital Forensic Practitioner should:

- Consider sufficient evidence;
- Be competent to carry out the investigation;
- Follow a validated process;
- Use a process that does not change the evidence or follow a process that minimises the impact on the evidence. Where there is an impact on the evidence, the Digital Forensic Practitioner should be competent to explain the effect and reason for the change;
- Be impartial and if evidence is located disproving the premise or supporting a counter-premise it should be reported.

In interpreting digital evidence, a Digital Forensic Practitioner should:

- Derive meaning from the evidence by analysing it in context of the circumstances;
- Find facts and in some cases, augmenting facts with opinion;
- Provide a fair and accurate interpretation of the facts;
- Differentiate between established opinions, facts and information inferred - the distinction needs to be stated in a report and the logical process that was followed in reaching an opinion and making an inference must be clear and repeatable;
- Where information is received from a person, care should be taken to test the reliability of such information and to ensure that assigned probative value reflects that reliability.

To ensure that the outcome of an investigation is reliable, it should be performed by a “competent investigators using examinations which are composed of validated analytical processes, in which they are proficient, and ensuring that every item of digital evidence produced can be traced back to the source of potential digital evidence from which it is derived”

Competence:

“sufficiently familiar with, and experienced in, the tools, methods and techniques which he will use to be able to carry them out with minimal supervision and should also be able to recognise the limits of their own abilities”.

Proficiency:

If he is given a sample set of evidence, he produces equivalent results to another competent Digital Forensic Practitioner, using a similar analysis.

A Digital Forensic Practitioner should:

- Consider sufficient evidence;
- Be competent to carry out the investigation;
- Follow a validated process;
- Use a process that does not change the evidence or follow a process that minimises the impact on the evidence. Where there is an impact on the evidence, the Digital Forensic Practitioner should be competent to explain the effect and reason for the change;
- Be impartial and if evidence is located disproving the premise or supporting a counter-premise it should be reported.

In interpreting digital evidence, a Digital Forensic Practitioner should:

- Derive meaning from the evidence by analysing it in context of the circumstances;
- Find facts and in some cases, augmenting facts with opinion;
- Provide a fair and accurate interpretation of the facts;
- Differentiate between established opinions, facts and information inferred - the distinction needs to be stated in a report and the logical process that was followed in reaching an opinion and making an inference must be clear and repeatable;
- Where information is received from a person, care should be taken to test the reliability of such information and to ensure that assigned probative value reflects that reliability.

ISO/IEC 27042 Report



Reports should contain, at a minimum:

- a clear statement of the writer's qualifications or competence to participate in the investigation and produce the report;
- a clear statement of the information provided to the investigative team prior to the investigation commencing (including the nature of the report to be produced);
- the nature of the incident under investigation;
- the time and duration of the incident;
- the location of the incident;
- the objective of the investigation;
- the members of the investigative team, and their roles and actions;
- the time and duration of the investigation;
- the location of the investigation;
- factual details of the digital evidence found during the investigation;
- any damage to potential digital evidence that has been observed during the investigation and its impact on the further investigative steps;
- limitations of any analysis undertaken (e.g. incomplete data sets, operational/time constraints); and
- a list of processes used including, where appropriate, any tools used.

Digital Forensic Standard for South Africa ACFE



The Role of Digital Evidence in Legal Proceedings

From discovery to court, how digital evidence is gathered, preserved, and used in South Africa.

