Organization for Security and Co-operation in Europe

Global Program

- Presentation, handling electronic evidence
- The Standard Operating Procedures introduction
- The workshops
  - SOP's your inputs
  - Computer Forensics
  - Cryptocurrencies

Organization for Security and Co-operation in Europe

HANDLING DIGITAL EVIDENCE

« preserve integrity, not only a technical matter»

Organization for Security and Co-operation in Europe

Presentation Program

- Overview of Internet use in Albania
- Criminal Legal framework, French, Budapest convention, Albanian CPC
- Evidence preservation period
- Seizing and examination, International standards, C-PROC, ISO 27032/NIST SP 800-86
- Court presentation

OSCE
Organization for Security and Co-operation in Europe

Goals

Understand the legal framework

- At national Level
- International cooperation
- Fundamental rights
- Cybercrime

Use international standards

- C-PROC Cybercrime Programme Office of the Council of Europe
- ISO 27037
- Nist SP 800-86

Knowing what is digital forensics

- Definition
- Methodology

OSCE
Organization for Security and Co-operation in Europe

Internet in Albania

DATAREPORTAL

OSCE
Organization for Security and Co-operation in Europe

Internet in Albania

FEB 2025

ALBANIA

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

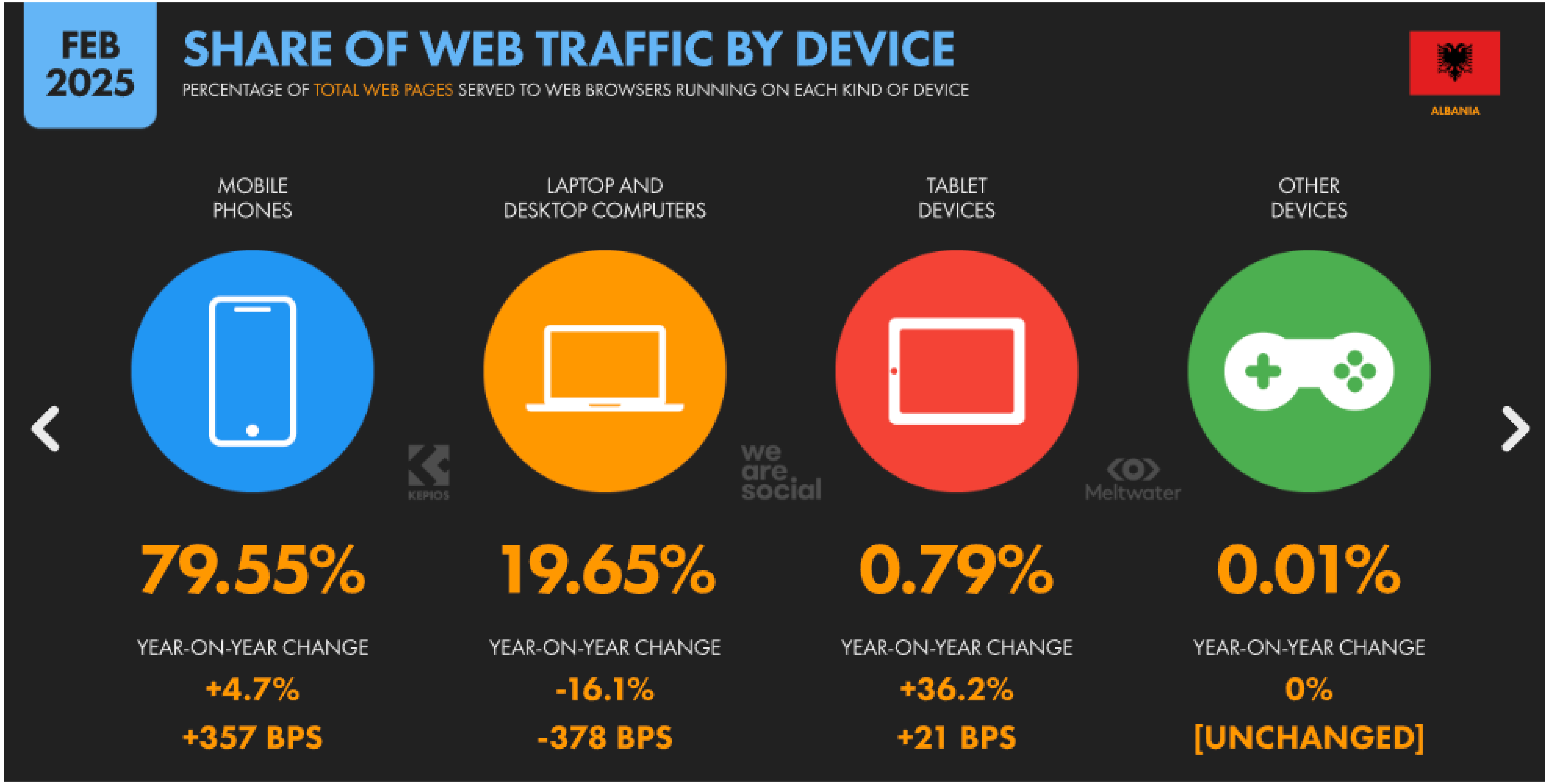
NOTE: SIGNIFICANT REVISIONS TO SOURCE DATA MEAN THAT FIGURES SHOWN HERE ARE NOT COMPARABLE WITH PREVIOUS REPORTS. SEE THE IMPORTANT NOTES AT THE START OF THIS REPORT FOR DETAILS.

TOTAL POPULATION	CELLULAR MOBILE CONNECTIONS	INDIVIDUALS USING THE INTERNET	SOCIAL MEDIA USER IDENTITIES
2.78 MILLION	3.97 MILLION	2.38 MILLION	1.41 MILLION
YEAR-ON-YEAR CHANGE	YEAR-ON-YEAR CHANGE	YEAR-ON-YEAR CHANGE	YEAR-ON-YEAR CHANGE
-0.7%	+2.8%	-0.7%	[N/A]
-20 THOUSAND	+107 THOUSAND	-17 THOUSAND	[BASE REVISIONS]
URBANISATION	TOTAL vs. POPULATION	TOTAL vs. POPULATION	TOTAL vs. POPULATION
65.7%	143%	85.6%	50.7%

we are social
Meltwater

osce
Organization for Security and Co-operation in Europe

Internet in Albania



OSCE
Organization for Security and Co-operation in Europe

The legal framework

France

Hybrid Inquisitorial process 1808, national

Phases: Investigations, inquiry, Trial

Investigations: Preliminary, Rogatory Letter

Actors: The Judge, The Prosecutor, The Lawyer

- Complaint not mandatory
- The victim can impose investigations
- The investigations are secret
- Written process
- Prosecution is the head of investigations
- General search warrant document
- The trial is public and contradictory
- Digital Evidence First Responder, Digital Evidence Specialist, the Lab

Albania

Hybrid Accusatory process, Federal

Phases: Investigations, pretrial, Trial

Investigations: Preliminary, Rogatory Letter

Actors: The Judge, The Prosecutor, The Lawyer

- Search warrant
- Art.34&34 a,b Rights
- Art. 37 self incrimination
- Art. 248 questioning of arrested person
- Art. 255 Duties of Judicial Police officer
- Art. 256 Questioning of the arrested or detained person
- Digital Evidence First Responder, MISSING BODY, the Lab

Organization for Security and Co-operation in Europe

The legal framework

Budapest Convention

Art. 16 and 17, preservation of stored data and traffic data

Art. 18, production order, allowing to request identification from a private company Offering a service in a foreign country

Art. 19 Search and Seizure, to be able to find electronic evidence and seize it legally.

Art.26 Spontaneous information, under condition, sharing information is possible

Art. 29 Preservation request

Art. 32 Trans-border access to stored computer data with consent or where publicly available

Art. 35 The Point of Contact, H24/7 must be created

OSCE
Organization for Security and Co-operation in Europe

The legal framework

Budapest convention 1st addendum protocol

The main goal is to criminalize online racism and xenophobia :

Criminal offenses	Art.3 to Art.5
Approval, justification genocide	Art.6

Budapest convention 2nd addendum protocol

The main goal is to allow direct request to foreign private company for:

Identification	Art.7
Traffic data	Art.8
Urgency	Art.9

Agreement for Joint Investigation Teams	Art. 12

Organization for Security and Co-operation in Europe

Compare The legal framework

2 BUDAPEST CONVENTION PROCEDURAL LAW	ART	Criminal Procedure Code	ART	Comments
Scope of procedural provisions, traffic and Interception capabilities	14	Content Limits of autorisation 7 years imprisonment or threats harassment 0 year The penalty is 5 years more with article 334 when 3 and more suspects are involved	221/275 CPC 334 CC	It's limited to 7 years minimum for wiretapping threats and harassment if data app are used, an issue is identified here
Conditions and safeguards protecting human rights	15	Constitution of Albania		Article 3, part II , chapter 2, 3, 4
Expedited preservation of stored computer data	16	The court, the Prosecutor if its' urgent, or the victim can request data	191/a/1	
Expedited preservation and partial disclosure of traffic data	17	The court, the Prosecutor if its' urgent, or the victim can request any information on subscriber The prosecutor can disclose data with a Court notification	191/a/2 191/a/3	Duration 15 day + 15 days Prosecutor but as an evidence, 90 days + 90 days
Production order	18	Obligation to disclose computer data	191/a	Data retention period
Search and seizure of stored computer data	19	Computer data seizure is possible with a court order, from a local or remote access This warrant is request by the Public Prosecutor Police Officers can preserve computer data in flagrante delicto	208/a 298	Search and Seizure, Botnet Cleaning and identification ENDGAME Only with MLA official request except urgent requests life in danger and terrorism. Some answers with MLA are back in 3 months, or sometimes never, in telegram exemple At national level, cloud access was not done during investigations
Real-time collection of traffic data	20	SECTION IV INTERCEPTIONS, not specified as Traffic, it's an interception, a Court Order is mandatory	221-223	Technical limitation yes with critical infrastructure identified and listed on a list approved by prime minister
Interception of content data	21	SECTION IV INTERCEPTIONS, can be done with a Court Order, 15 days+15 days For preventing crimes, the Public Prosecutor can intercept communication without a Court Order, but it will not be admissible at Court, art 221/5	221-223	Technical limitation, no content on cybersecurity for cybercrime, possible in state police

Compare The legal framework

3 BUDAPEST CONVENTION INTERNATIONAL COOPERATION	ART	Criminal Procedure Code	ART	Comments
Extradition	24	SECTION I EXTRADITION ABROAD	488	
Spontaneous information sharing	26	Prosecutor functions for cooperation with foreign authorities The prosecutor can disclose data with a Court notification	24 191/a/3	
Expedited preservation of stored computer data	29	Expedited preservation and maintenance of the computer data	299/a	
Expedited disclosure of preserved traffic data	30	Expedited preservation and partial disclosure of computer data	299/b	
Mutual assistance regarding accessing of stored computer data	31	INTERNATIONAL ROGATORY LETTERS	519	
Trans-border access to stored computer data with consent or where publicly available	32	Computer data seizure is possible with a court order, from a local or remote access This warrant is request by the Public Prosecutor Police Officers can preserve computer data in flagrante delicto	208/a	Search and Seizure, Botnet Cleaning and identification ENDGAME Never done before
Mutual assistance regarding the real-time collection of traffic data	33	SECTION IV INTERCEPTIONS There is no definition on Traffic in tis article, it's real time interception for traffic	221	Possible with MLA
Mutual assistance regarding the interception of content data	34	SECTION IV INTERCEPTIONS 5. Preventive interceptions shall be regulated by special law. The results of preventive interceptions cannot be used as evidence.	221	Not possible because technical limitation
H24 point of contact	35	Albanian State Police Cybercrime Directorate	Present	
Budapest Convention 1st protocol Racism Xenophobia	ETS 189 – Cybercrime	Signed in 2003 entry into force 2006 Criminal Code ALBANIA	84/a 119/A 119/b	
Budapest Convention 2nd protocol Disclosure E-Evidence and cross-border access NO MLA	CETS No. 224	Signed in 2023 to be ratified	Ongoing process under discussion	Data disclosure without MLA after an H24 request from EU member state

OSCE
Organization for Security and Co-operation in Europe

E-Evidence

⚖️ Critical Legal Requirements for E-Evidence

- **Section 1 - Legal Authorization:** Consent (written), warrant, or expert appointment REQUIRED
- **Section 2 - Contradictory Process:** Owner/witnesses MUST be present during on-site operations (search, live acquisition, sealing)
- **Section 2 - Article 37 (Albanian Law):** IF person makes self-incriminating statement, IMMEDIATELY interrupt, warn of rights (lawyer), suspend if requested. Statements BEFORE warning = INADMISSIBLE
- **Section 4 - Training Check:** Live acquisition ONLY by trained personnel with proper tools (FTK Imager or equivalent)
- **Section 5 - On-Site Copying:** FTK Imager mandatory, E01 format mandatory, contradictory process mandatory
- **Section 6 - Sealing:** ALL parties MUST sign (owner, witnesses, police, expert) in contradictory process
- **Section 9 - E01 Format:** Mandatory for evidence (READ-ONLY, embedded hash, cannot be modified)
- **Section 9 - Double Hash:** SHA-256 (primary) + SHA-1/MD5 (secondary) - both documented and RFC3161 timestamp
- **Section 9 - SSD/Flash:** TRIM modifications MUST be documented (technical, unavoidable, does NOT affect validity)
- **Section 9 - Hash Verification:** E01 hash failure = FILE corruption (storage/transfer), NOT source problem
- **Section 9 - Hash Failure Response:** Restore from backup OR report to court - DO NOT re-image
- **Section 10 - Expert Neutrality:** Report ALL findings (incriminating + exculpatory)

Organization for Security and Co-operation in Europe

E-Evidence

⚠️ **E-Evidence May Be Inadmissible If:**

❌ **Section 1:** No legal authorization (consent/warrant/expert appointment)
❌ **Section 2:** Contradictory process violated (owner/witnesses not present during on-site operations)
❌ **Section 2 - Article 37:** Self-incriminating statements used without proper warning, OR questioning continued after lawyer requested
❌ **Section 4:** Live acquisition attempted by untrained personnel without proper tools
❌ **Section 5:** On-site copying NOT using forensic tools (used Windows copy, xcopy, etc.)
❌ **Section 5:** On-site copying NOT in E01 format
❌ **Section 5:** On-site copy report NOT signed by all parties
❌ **Section 6:** Sealing NOT done with all parties present and signing
❌ **Section 7:** Chain of custody broken
❌ **Section 9:** Evidence NOT imaged in E01 format
❌ **Section 9:** SSD/Flash TRIM modifications not disclosed in report
❌ **Section 9:** E01 hash failure and evidence "re-imaged" without contradictory process
❌ **Section 10:** Expert not independent/neutral
❌ **Section 10:** Expert only reported incriminating evidence, (the legal report too)

Organization for Security and Co-operation in Europe

E-Evidence

⚖️ THREE LEGAL PATHWAYS FOR CLOUD DATA ACCESS

🔴 **FUNDAMENTAL PRINCIPLE:**

Cloud data stored by foreign providers requires international legal cooperation

THREE POSSIBILITIES ONLY
(Budapest Convention on Cybercrime)

PATHWAY 1: FREE, FAIR & LEGAL CONSENT - REMOTE ACCESS

Budapest Article 32.b

Account holder provides written voluntary consent
Suspect MUST be present for remote access
NO request to cloud provider

⏱ **Timeline:** Immediate / Same day
✅ **Result:** Full data access (remote download)
🔑 **Key:** NO foreign authorization, NO provider delay

PATHWAY 2: IMPOSSIBLE TO LOCATE

Search Warrant + Contradictory Procedure

Data found during live computer search
User agreement with live search
⏱ **Timeline:** Immediate
⚠️ **Limitation:** Live demo only
🔑 **Key:** Cannot compel credentials

PATHWAY 3: PRESERVATION + MLAT

Budapest Article 16

Preservation (16.1) + MLAT production (16.2)

⏱ **Timeline:** Months to Years
✅ **Result:** Full data access
🔑 **Key:** Foreign authorization required

Organization for Security and Co-operation in Europe

E-Evidence preservation period

	Text	Topic	Quality	Comments
National data retention	Duration	Telecommunication	2years	telecommunication law 54-2024 source dest
	Duration and quality	Data	2 years	IP source dest and timestamps, receiving and IP identification without the Port number a list of cistomers will be provided locally
	Text	Topic	Quality	Comments
National request	Identification	Phone number and call history	Yes 2 years	
		Internet Access Provider customer	2 years	
		IP with or without source port number	2 years	
		Webhosting customer	2 years	Telecommunication regulation 54-2024 atr 160
		Domain Name	2 years	
		Email	2years	
	traffic	Call list	2 years	
		ISP customer history traffic	2 years	
		CCTV	2 months	tell regulation
		WebHosting logs	Not included	
	data copy	Storage Device	Yes on site	
		Phone	Noy for CERT	
		Server	Yes on site	

Organization for Security and Co-operation in Europe

International Standards

Cybercrime Programme Office of the Council of Europe (C-PROC)

ISO 27037

NIST 800-86

OSCE
Organization for Security and Co-operation in Europe

International Standards

Standard Operating Procedures

for the collection, analysis and presentation of

electronic evidence

Prepared by

Cybercrime Programme Office of the Council of Europe (C-PROC)

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

OSCE
Organization for Security and Co-operation in Europe

International Standards

Cybercrime Programme Office of the Council of Europe (C-PROC)

- Onsite retrieval
- Securing
- Transport and handling
- Analysis
- Presentation

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented by the Council of Europe

International Standards

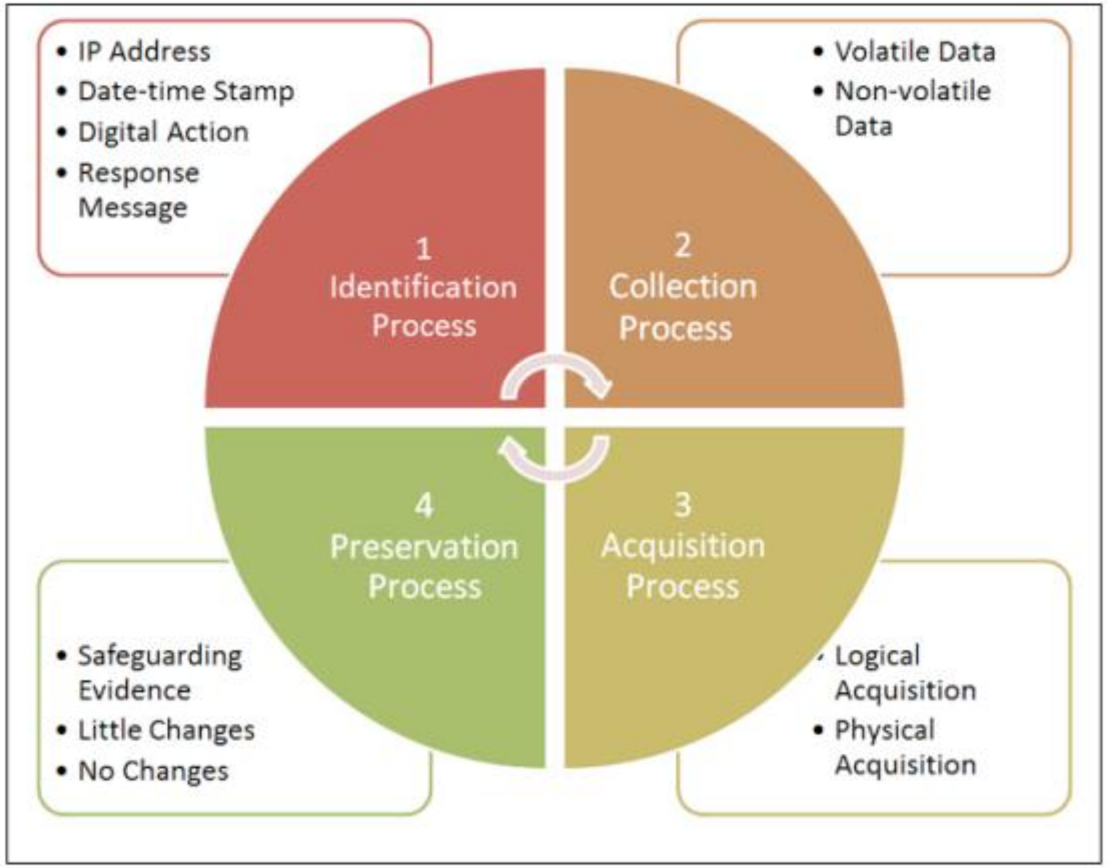
ISO 27037

Identification

Collection

Acquisition

Preservation



International Standards

NIST SP 800-86

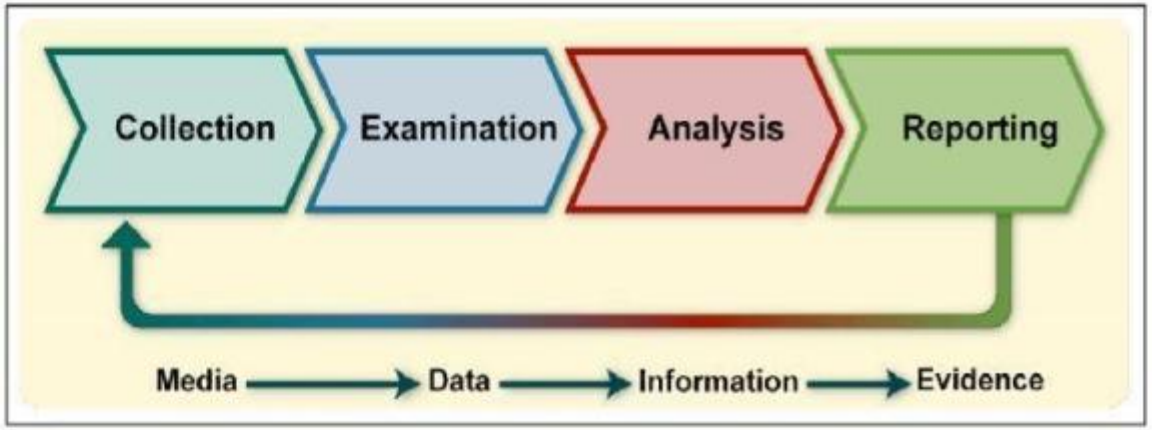


Table 1. Process Summarizes

No	Comparison	NIST SP 800-86	ISO 27037
1	Investigation	N/A	Available
2	Collection	Available	Available
3	Examination	Available	N/A
4	Analysis	Available	N/A
5	Acquisition	N/A	Available
6	Preservation	N/A	Available
7	Reporting	Available	N/A

OSCE
Organization for Security and Co-operation in Europe

International Standards

Digital Forensic Principles

ISO/IEC 27037:2012 Guidelines

1

Auditability

All processes and procedures applied to digital evidence must be fully documented and auditable. This ensures that actions taken can be independently reviewed and verified by others.

2

Repeatability

The same results should be obtained when the same processes are applied to digital evidence under the same conditions, demonstrating consistency in forensic methodology.

3

Reproducibility

Independent examiners should be able to obtain the same results using the same methods and tools, validating the reliability and integrity of the forensic process.

4

Justifiability

All actions and decisions taken during the forensic process must be justifiable and based on established methods, ensuring defensibility in legal and professional contexts.

OSCE
Organization for Security and Co-operation in Europe

International Standards

FIELD

Investigation:

- Plan the case, legal part included
- Identify E-Evidence
- Preserving, data must not altered

Collection:

- ON/OFF device, preserve business activity
- Document your actions, contradictory process
- Acquisition process, cloud information
- **Chain of custody, sealing, storage, traceability**

CONTRADICTORY

LAB

Examination:

- Forensically processing collected data
- Assessing and extracting data of particular interest,
- Preserving the integrity of the data.

Analysis:

- The results of the examination,
- Using legally justifiable methods and techniques,
- Useful information impetus

ALONE

TRIAL

Reporting:

- Describing the actions used,
- Explaining how tools and procedures were selected,
- Determining what other actions need to be performed

PUBLIC

Organization for Security and Co-operation in Europe

International Standards

digital evidence is governed by three fundamental principles:

- relevance
- reliability
- sufficiency

Handling process Sensitive :

- Identification
- Collection
- Acquisition
- Preservation

Key principles:

Human rights for fair E-Evidence

Chain of custody for strong E-Evidence

Court Reporting

Reporting:

- The process, from the beginning
- The legal framework
- The chain of custody
- The tools
- The collected data, and the evidence traceability
- The plausible explanations
- Audience consideration
- Actionable information

THANK YOU FOR YOUR ATTENTION

QUESTIONS