AL-FARABI KAZAKH NATIONAL UNIVERSITY

FACULTY OF INFORMATION TECHNOLOGY AND ARTIFICIAL INTELLIGENCE
DEPARTMENT OF CYBERSECURITY AND CRYPTOLOGY

LEGAL REGULATION OF INFORMATION SECURITY

Lecturer: PhD, Acting Associate Professor Assem Turarbek

MODULE 4

INCIDENT RESPONSE AND INVESTIGATION

LECTURE 15

LAW ENFORCEMENT INVESTIGATION OF INFORMATION SECURITY CRIMES

LECTURE OBJECTIVE

Explain how investigators collect and assess digital evidence and distinguish the roles of investigators, specialists and experts.

LECTURE PLAN

1. Criminal procedure and digital evidence
2. Evidence collection and assessment
3. Investigative roles and attribution

INCIDENT AND CRIMINAL INVESTIGATION

Concept or participant	Meaning, duties and application
Incident assessment	Establish what happened and what systems, services or records were affected.
Criminal investigation	Establish facts relevant to a suspected offence through authorized procedural actions.
Stages	The lecture distinguishes pre-trial investigation from judicial proceedings.

A criminal investigation uses authorized procedures to establish facts relevant to a suspected offence. Incident response supplies technical information and restores service, while the criminal process determines the legal use of evidence. Early cooperation helps preserve traces that could otherwise disappear during repair, routine retention or continued system operation.

SOURCES OF DIGITAL EVIDENCE

Concept or participant	Meaning, duties and application
System records	Logs, audit trails and access records can document actions, accounts and times.
Electronic documents	Messages, transaction records and files can provide evidence of communication or conduct.
Physical media	Devices and storage media may contain relevant data.
Testimony and expert findings	Witness statements and specialist or expert materials can help interpret technical records.

Different evidence sources answer different questions. Logs can show an account action, documents can show its content, devices can retain traces and witnesses can explain circumstances. A complete assessment compares these sources. Missing records and inconsistent times are examined rather than treated as confirmation of one version of events.

DISCOVERY, RECORDING AND PRESERVATION

Concept or participant	Meaning, duties and application
Discovery	Identify potential traces and record where they were found.
Recording	Document the source, time, method and circumstances of collection in the appropriate record.
Preservation	Protect originals and use verified copies for analysis when appropriate.
Handling history	Record transfers and access so reviewers can trace how the evidence was handled.

Collection records the location, method and circumstances of obtaining material. Preservation protects originals and documents access or transfer. Verified copies allow analysis while retaining a reference to what was collected. The handling history supports later review of whether the material remained consistent and whether the procedure followed applicable requirements.

ASSESSMENT OF EVIDENCE

Relevance

Determine whether the material helps establish a fact at issue.

Admissibility

Assess whether the material was obtained and recorded in accordance with applicable procedural rules.

Reliability

Check the source, integrity and consistency of the material.

Sufficiency

Consider whether the evidence as a whole supports the conclusion.

Relevance concerns the relationship to a fact at issue. Admissibility concerns the procedure for obtaining and recording material. Reliability concerns confidence in the source and content. Sufficiency concerns the evidence as a whole. A technically detailed record can still leave an essential question unanswered.

INVESTIGATORS, SPECIALISTS AND EXPERTS

Investigator

Directs authorized actions and documents their purpose and results.

Specialist

Provides technical assistance during procedural actions and helps interpret or document technical findings.

Expert

Performs an assigned examination and issues a written opinion.

The investigator organizes procedural actions and records their results. A specialist assists with technical work during those actions. An expert performs an assigned examination and gives a written opinion. The task and authority of each participant determine how the work is performed and how its results enter the proceedings.

ATTRIBUTION AND CORROBORATION

Account activity

A log can identify an account and time. Further evidence may be needed to establish who performed the action.

Corroboration

Compare independent records, relevant documents and witness accounts.

Impact

Document the effects on data or services and how the affected organization assessed any damage.

Attribution requires more than finding an account name or network address. Shared credentials, compromised devices and automated actions can complicate the link to a person. Independent records and testimony can clarify that link. The analysis also considers authorization, the method of interference and the effects on the resource.

CASE DISCUSSION

A registry records an unauthorized change under an employee’s account. The employee denies making the change.

What sources would help determine who acted, and how would investigators preserve their evidentiary value?

Analysis

Compare application logs with authentication records, endpoint activity, change approvals and testimony. Record provenance and handling and preserve originals. Attribution requires evidence linking activity to a person as well as to an account.

METHODS OF RECORDING DIGITAL EVIDENCE

The lecture distinguishes verbal, graphic, physical and visual forms of recording. Examples include protocols, audio recordings, plans, photographs, video and preserved copies.

Several methods can be combined. Their evidentiary value depends on lawful collection and a record that explains the source, method and circumstances of the action.

A device may be seized for later examination when the procedure permits it. Some systems are too large or operationally important to remove without serious disruption.

The source describes detailed recording and specialist examination at the location. Copying relevant information can preserve its evidentiary properties while allowing the original infrastructure to continue operating under the applicable arrangements.

SCIENTIFIC AND TECHNICAL MEANS

Technical methods help discover, record and examine traces. Their use must support accuracy and preservation of the material. The investigator documents the equipment and procedure used.

A verified copy supports repeatable analysis. Integrity checks and handling records help show whether the analysed material remained consistent with what was originally collected.

The investigation establishes the affected resource, the relevant access conditions, the method of interference and the consequences. It identifies potential witnesses and the location of relevant records.

Further actions compare logs, messages, devices and expert findings. An account identifier, network address or device association contributes evidence, while attribution requires assessment of the complete record.

CONCLUSION

1. Investigators obtain and record digital evidence through authorized procedures.

2. The evidence must be assessed for relevance, admissibility, reliability and overall sufficiency.

3. Attribution requires evidence linking activity to a person as well as to an account.

SELF-ASSESSMENT QUESTIONS

1. What sources can provide digital evidence in a cybercrime investigation?
2. Why must evidence collection and handling be documented?
3. How do the roles of investigators, specialists and experts differ?
4. What factors determine the relevance, admissibility and reliability of digital evidence?
5. Why is identifying an account or device insufficient to establish who committed an offence?

REFERENCES

1. Lecture 15. Law Enforcement Investigation of Information Security Crimes. Course materials.

2. Republic of Kazakhstan. Criminal Procedure Code.

3. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response.