OBTAINING DIGITAL EVIDENCE – LEGAL ISSUES

Objective

During this session, participants will examine legal framework and procedures for collection of digital evidence.

I. A FRAMEWORK FOR DIGITAL EVIDENCE

A. Law and digital evidence

1. Computers and the Internet have added significant new dimensions to criminal conduct, especially in the ability to store huge amounts of information, and the rapidly expanding communications network
2. This technological revolution presents challenges to law enforcement, including difficulties in identifying the perpetrator and extent of the crime, and the volatility of electronic data
3. Investigators and prosecutors must have laws and procedures to stay abreast of digital evidence issues

B. International standards

1. Cyber crime is a worldwide challenge that often leaves a trail of evidence across borders, but ***domestic*** laws establish lawful procedures for collecting digital evidence
2. The ***Convention on Cybercrime*** provides a framework for discussing procedures for investigating cyber crime, including:
    a. Crimes related to computers and the Internet
    b. Provisions for investigating cyber crime
    c. International legal cooperation
    d. Protection of human rights and liberties
4. This Council of Europe treaty entered into force in January 2004, and is open to all countries in the world; as of January 2008, 22 countries are parties, another 21 countries have signed but are not yet parties, and other countries are interested in joining; the convention and additional materials are at http://conventions.coe.int/

C. Types of information and privacy interests

1. Content data: The substance, purpose, or meaning of a communication or other data

2. Traffic data: Computer data relating to a communication by means of a computer system, generated by a computer system in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service (Convention, Article 1)

3. Subscriber information: Information, in computer data or another form, that is held by a service provider, relating to subscribers of its services other than traffic or content data (Convention, Article 18)

4. Collection by the government of non-public information requires an analysis of privacy interests; greater the privacy interest will result in more conditions and safeguards placed on collection of information (Convention, Article 15)

WHAT TYPE OF DATA?	Stored	Real-time Collection
Traffic Data	Privacy Interest	Privacy Interest
Content Data	Privacy Interest	PRIVACY INTEREST

II. PROCEDURES FOR OBTAINING DIGITAL EVIDENCE

A. General considerations

1. Every legal system has different procedures and limitations on obtaining evidence; your country may significantly restrict certain methods for obtaining digital evidence; for example, some countries do not permit real-time collection of data
2. Procedures generally include provisions to protect the confidentiality of an investigation

B. Preservation of data: Enables competent authorities to order the expeditious preservation of specified stored computer data; may include partial disclosure of traffic data; prevents loss or modification of data, such as intentional or accidental deletion or modification, or deletion in the normal course of business (Convention, Articles 16 and 17)

C. Production order: Enables competent authorities to order:

1. A person to submit specified stored computer data
2. A service provider to submit subscriber information (Convention, Article 18)

Different standards may apply to content data and traffic data

D. Search and seizure of stored computer data: Enables competent authorities to search and seize:

1. A computer system and its stored data
2. A data-storage medium (for example, drives, disks)

Law enforcement can also copy the data, remove offending data, and protect data (Convention, Article 19)

E. Real-time collection of traffic data: Enables competent authorities to:

1. Collect or record traffic data in real-time, by technical means

2. Compel a service provider to collect or record traffic data within its technical capability, or assist law enforcement (Convention, Article 20)

Requires significant conditions and safeguards

F. <u>Interception of content data</u>: Enables competent authorities to:

1. Collect or record content data in real-time, by technical means
2. Compel a service provider to collect or record content data within its technical capability, or assist law enforcement (Convention, Article 21)

Generally limited to investigations of serious offenses; this most intrusive form of evidence collection requires significant conditions and safeguards

---

This presentation was developed by the Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, www.cybercrime.gov.