Informatics Ethics and Law

Prof. Dr. Eşref ADALI

IT Law

13

IT Crimes-I

The European Economic Community divided IT crimes into 5 catagories:

1. Accessing, disrupting, erasing or destroying the data on the computer intentionally to ensure that it is illegally accessed to a resource or any value on the computer,
2. Intentionally entering, breaking, deleting, destroying computer data or programs to make a fraud,
3. Intentionally entering, breaking, deleting, destroying computer data or programs to prevent the operation of computer systems,
4. To harm the rights of the legal owner of a computer program in order to benefit commercially,
5. It is intentionally entering and intervening in the system by overcoming the security measures that have been put in place, without the permission of the computer system responsible.

IT Crimes-II

Crimes Committed with a Computer: Within the scope of crimes committed using a computer or an information system, robbery in Internet banking, attacks that render information systems inoperable, malicious software and actions to damage information systems can be considered. In the past, attacks on aviation systems, oil pipelines and traffic systems have been witnessed.

Crimes Committed on a Computer or an Information System: The process of stealing, changing or deleting the data in the database by intrusion the information system is the best example for this issue. Logical bomb placed in the information system and additions to existing software are other examples for this type.

Publications and Services in the Informatics Environment and Crimes Committed with the Services: Internet environment offers people broad and comfortable publication as much as possible. Using this free environment, useful publications can be made as well as very harmful works. Within the scope of such harmful studies:

- Publications contrary to general morality,
- Publications disrupting national security,
- Misleading news,
- Child pornography,
- Gambling

countable.

Laws Related to IT Crimes

New Turkish Turkish Criminal Code (TCK-5237):

- Article 243 - Crime of entering the Information System
- Article 244 - Blocking, Disrupting, Destroying or Preventing Data
- Article 245 - Abuse of Debit or Credit Cards
- Article 246 - Implementing a Security Measure on Legal Persons

New Criminal Procedure Law (CMK-5271):

- Article 134 - Search, Copy and Seizure of Computers, Computer Programs and Logs

Electronic Signature Law (5070):

- Article 15 - Inspection
- Article 16 - Unauthorized Use
- Article 15 - Fraud

Law on Regulating Broadcasts on the Internet and Combating Crimes Committed through These Broadcasts (5651)

Personal Data Protection Law (6698)

European IT Crimes Convention

- **Crimes against the confidentiality, integrity and use of computer data and systems**
  - Illegal access
  - Illegal intervention
  - Intervention in data
  - System intervention
  - Abuse of devices

- **Computer-related crimes**
  - Computer related fraud actions
  - Fraud actions associated with computers
  - Content-related crimes
  - Crimes related to child pornography
  - Crimes related to infringement of copyright and similar rights
  - Facilitating the protection of stored computer data
  - Facilitating and partially disclosing the protection of traffic information
  - Searching and confiscating stored computer data
  - Real-time collection of traffic information
  - Intervention in content related information

Investigation and Prosecution of IT Crimes

Since the quality of the crimes committed in the field of informatics is different from the known crimes, their investigations and prosecutions should be done accordingly. Some important points that make IT crimes different from other crimes:

The place where the crime was committed and the crime may not be in the same place: In known crime types, the crime offender usually happens where the crime is committed. In IT crimes, the criminal is almost never at the place where the crime was committed, or even near it. The culprit may be in another city or even in another country.

IT crimes can be of an international nature. Therefore, it requires international collaborations.

The investigation must be quick: Those who commit the crime of informatics do not always sit in the same place. They do not even connect to Internet from a fixed place. Thus, they try to ensure that their locations are not known. However, it is seen that they are connected from the same place for a certain period of time using the same IP address. Therefore, it is necessary to try to learn the location information as soon as the complaint is received in order to catch a criminal. At this stage, it would be appropriate to take advantage of information technologies.

It requires special knowledge to gather evidence: Evidence of IT crime can be found in the informatics environment, which we call digital evidence, documents, tables, sound recordings, photographs, films and data in different environments. If these data are not collected according to the rules, they lose their quality of evidence. Real criminals benefit most from such a mistake.

Only IT experts can evaluate the event: The form of IT crime, the traces and evidence left by it can only be evaluated by IT experts who are experts in this field.

If the data in the informatics environment are not collected according to the rules, they lose their quality of evidence. Real criminals benefit most from such a mistake.

International Conventions-I

Turkey is a party Article 19 of the European Convention on Cybercrime is on the search for data and confiscating in the IT environment. The format approved by the Turkish Grand National Assembly is given below.

Article 19 - Searching and confiscating stored computer data

1. Each of the parties shall be responsible for the competent authorities in its country,
    a. All or part of a computer system and stored computer data in it; and
    b. A computer data storage device where computer data may be stored it will adopt legislative and other measures that may be necessary for them to have the authority to seek and access them.
2. Each party has the grounds to believe that, in accordance with paragraph 1.a, their authorities search for all or part of a particular computer system or access it in a similar manner and believe that the data sought is stored in all or part of another computer system in their country; and will adopt legislative measures and other measures that may be required to enable authorities to quickly extend their search or similar access to the other system when such data are lawfully accessible or available for the first system.

International Conventions-II

3. Each Party shall adopt legislative or other measures that may be necessary to authorize its competent authorities to seize or similarly secure the computer data accessed in accordance with paragraph 1 or 2. These measures are:

a. seizing or similarly securing an entire or part of a computer system or computer data storage device;

b. creating and maintaining a copy of said computer data;

c. to protect the integrity of the relevant stored data;

d. to render and remove computer data on the accessed computer system

will include powers to.

4. Each party is authorized to provide its competent authorities with the reason to provide reasonably necessary information to any competent person who has knowledge of the operation of the computer system or measures to protect the computer data in order to allow the measures specified in paragraphs 1 and 2 to be applied. It will adopt legislative and other measures that may be necessary.

IT Forensic

Evidence collection requires special knowledge in computer, information system and information environment related cases. Also, there is a need for environments where these examinations can be made. For this reason, countries have started to form the institutions we call Informatics Forensic. Forensic information is defined as follows:

- It is the process of converting the findings obtained from the informatics environments into legal evidence by using various technical hardware and software.

- From this aspect, it can be said that forensic informatics is more of a technical issue rather than law. Because the process of transforming the findings in information systems into legal evidence by separating them from each other is a very intense, highly technical and demanding job.

- Disc examination,
- Examination on memory,
- Those related to the computer network,
- Examination on mobile systems,

Regardless of the field of study, the work of forensic information is carried out in three stages:

1. Obtaining evidence and keeping it,
2. Review and analysis
3. Reporting and presenting to court

If the data in the informatics environment are not collected according to the rules, they lose their quality of evidence. Real criminals benefit most from such a mistake.

Judicial Evidence

In all cases that are the subject of the case, we encounter numerical evidence and ask the following questions:

- Can the information stored in the computer's memory be considered forensic evidence?
- Can the information stored in the computer's disc be considered forensic evidence?
- Can the information on the CD or DVD be considered forensic evidence?
- Can the information on the removable disk and memory stick be considered forensic evidence?
- Can the information stored in the cloud be considered evidence?
- Can e-mails be considered forensic evidence?

It is useful to identify forensic evidence before giving detailed answers to these questions and is defined as follows:

Objects that can prove an incident are called evidence, and the evidence must be material, lawful, and reasonable.

Collecting evidence in cases involving a computer is very different from collecting evidence from a murder incident. By seeing this difference, laws should be prepared and methods should be produced.

Information in Computer's Memory

- Information in the computer's memory may be evidence. However, the computer must be operational during the evidence collection phase. In addition, the program associated with the crime must be running. When the computer is turned off, the information in its memory disappears. In addition, information about a program is loaded into memory while this program is running.

- It is not always possible to access information in the computer's memory. In addition, data is usually kept in documents, charts or databases. These are programs that take up space in memory.

Information on the Computer Disk

- The disk of the computer may contain the operating system, programs for various purposes, documents, data, sound recordings, photos and movies. Other than the operating system, the owner of the computer or someone else may have produced it.
- If the application programs are licensed and the manufacturer is known, there is no problem in terms of evidence. If the producer of the program is not certain, the proof feature is not certain. In particular, programs for offensive and robbery may have these qualities.
- The most important issue in the cases is the documents on the computer. As it is known, there are different Word processing programs used to prepare documents. In most of these programs, information such as the name of the author of the document, the date of writing, if their additions were made by others, and the date of modification, and the date of publication are added to the document as header information. In cases, this header information is required to be used as evidence. The information in question is information that can be changed at any time. All information about the past recorded by the program can be changed later. Therefore, they do not have value as a forensic evidence.
- Spreadsheet programs also hold information about those who prepared and changed the Spreadsheet, similar to the Word processing programs. Since this information is information that can be changed later, it cannot be forensic evidence.
- Similarly, in the attachment of photographs and films, the camera used, technical information, time information and the name of the photographer or film are written. Since this information is also interchangeable, they cannot be counted as forensic evidence.
- Information such as the producer name, modifier name, production or shooting date on a document, spreadsheet, photo or a movie indicates that this object is not enough proof, and that there is no evidence. The same is true for photos and movies

Information on CD / DVD

1. By looking at the date when a CD or DVD was written, it cannot be said that it was written on the date written on that CD or DVD. The writing time information displayed on the CD or DVD is the time information of the computer. Since a computer's time setting can be changed at any time, therefore time information on a CD or DVD cannot be forensic evidence.
    - The production date of the program used to write information to a CD or DVD cannot be definitive evidence. If the program used to write information on CD or DVD is in use before the date of review, there can be no forensic evidence. More precisely, it cannot be concluded that this information was prepared in that range, as the writing times of the documents on CD or DVD are compatible with the time interval of writing program.
    - More specifically, if the writing times of the documents on the CD or DVD show before the release of the writing program, it is clear that the CD or DVD in question was prepared for the purpose of misleading.

2. Documentation, tables, photographs and movies on a CD or DVD are the name of the producer, date of manufacture, date of modification, and so on. Therefore, forensic evidence cannot be counted.

Information on External Disk and Memory Stick

- Nowadays, external disk and memory stick are widely used. The programs, documents, photographs and movies stored in such information storage devices are information downloaded from the computer.
- They can be read and uploaded to the computer as they are installed. All information that prepares and modifies after it is transferred to the computer can be changed. When these changes are made, when they are loaded into removable disk and stick memory again, the information about the producer and modifiers is changed.
- Consequently, documents such as documents, table, photographs and movies in portable disk and memory stick, the production time, producer name, the name and time of the modifier cannot be considered as forensic evidence.

Information in Remote Environment and Cloud

- Today, it is possible to store documents, spreadsheets, sound recordings and video recordings outside the computer. While free disk space can be provided in the cloud, large disk requirements can be provided for a fee. Cloud computing adds program usage service to this feature. So today, a person can do all their work in the cloud and keep their data in the cloud without leaving any traces on their computer.

- In order to evaluate the data stored in the remote environment and in the cloud as forensic evidence, it is necessary to trust the organization that provides this environment first.

E-mails

- In some cases, e-mails are provided as evidence. The person sending the e-mails can keep their identity and address and send them with a fake ID. Therefore, it is difficult to count e-mails as forensic evidence.
- In addition, the content of the e-mail and the imprint information of the e-mail can be edited later.
- However, action reports and traffic information from e-mail service providers can be used as evidence. How to collect the numerical data that can be considered as forensic evidence will be explained in the next section.

Forensic Evidence Collection-I

All kinds of information in the information system must be collected according to certain rules in order to be considered as forensic evidence. The prosecutor, law enforcement officers and forensic IT specialists, if any, should be present during the process that should be done at the scene. If information systems are running, they must be stopped. Evidence is then collected by the following methods. Matters that constitute a legal basis for the issue are included in the Criminal Procedure Law (5271) Art.134:

- Image copies of the memory or disks of computers in the environment must be taken under the supervision of the interested parties. To eliminate the possibility of replacing the received copy later, it should be summarized using the Hash algorithm. Copies and hash must be given to the defendant.
- If there is a external disk, memory stick and CD / DVD in the media, image copies of them should be made and summary of each copy should be made. One copy from each copy and hash should be given to the defendant.
- There are devices manufactured to make a image copy of those registered in an information storage unit. These devices consist of hardware and software running on it. Most of the products on the market are capable of making an true copy of the memory of individual computers. There are closed and open source ones for the programs running in these products.

Forensic Evidence Collection-II

- The system that makes an image copy must be reliable. First of all, it should be ensured that it will not add to the storage it will copy. Therefore, it is very important that both the copy system and its user are impartial and reliable. It is correct to use hardware and software with reliability certificate in making copies.
- Some of these systems can also bring deleted data to some extent.

- The equipment does not need to be taken away after the work at the scene is completed. Thus, a wrong application is terminated. However, computers and peripherals obtained in case of a conflict can be taken away for forensic information examination, provided that necessary precautions are taken.

- In addition to those described above, it is useful to make the following reminder. When uncertain disc, CD / DVD or memory stick from where and how they are obtained are presented to the court as evidence, it is first necessary to thoroughly investigate who, how, where and when they were obtained. The information in these environments may be accurate or fraudulent information prepared to mislead the court. After this preliminary evaluation, it would be more accurate to make a technical evaluation.

- Today, documents, data, sound and images can also be stored in the cloud. Whether an information system uses the cloud environment can be learned as a result of computer research. Image copies of the records kept in the cloud should be made.

Examining and Evaluation

- Evidence collected at the scene needs to be examined and evaluated in a laboratory setting. If we make an analogy, forensic medicine does technical studies on examining and evaluating a murder. Those working in the forensic medicine institution are specialists. Therefore, it is expected that the people who will examine, analyze and evaluate the numerical data in the forensic IT institution will also be expert IT experts.

- It is clear that special hardware and software will be needed during the examination of digital data. Such hardware and software can be obtained from the market ready. Therefore, they are experts who can use them. Experts should be people who know how to find what they are looking for in the existing records.

- The collected numerical data may be encrypted. In this case, firstly, it is aimed to learn the decipher password from the defendants. In cases where the password cannot be learned, it is resolved.

Reporting

After examining and evaluation, a report is prepared based on the language and evidence that the judge will understand. In this report:

- The subject should be introduced together with its stages,
- Findings should be supported by technical information,
- The result should be explained precisely.

Forensic IT Studies-I

Disk Examination

- The following situations are encountered during the review of records on the disk:
- Examining documents, sound recordings, photographs and films related to the case,
- Opening encrypted records,
- Recovering deleted records
- It is known that there will be different kinds of records on the disc. In these records, those related to the case should be removed. The subject of the case is usually the files created by the owner of the computer. The operating system on the computer and the application software of which the manufacturer is known should be kept separate. The contents of the files thought to be related to the case should be examined one by one. Since the files can be very large in size, the scans in them can be word-based.
- Keys of encrypted files can be requested from the owner. In cases where it cannot be obtained, password resolution can be made.
- Fetching deleted records is not possible in all cases. It is possible that files that have been deleted but have not been overwritten are returned. However, it is not possible to return files that are overwritten or specifically scraped to prevent them from being returned.
- What is described for the disc of the computer also applies to removable disks and stick memories.

Forensic IT Studies-II

Memory Examination

Memory examination is a study that can be done while the computer is running. The information in the action report can only be accessed after the computer is turned off.

Computer Network Examination

Traffic information on computer networks can be obtained from organizations with leak detection systems and Internet service providers. From this information, who can communicate with whom, when, what kind of communication and how long the communication lasts can be obtained.

Mobile Systems Examination

Especially the widespread use of smart phones has led the forensic informatics to work on this issue. It is necessary to work on the SIM cards and memory of the phones. These studies provide information about the person's speech records, message records and the information they convey.

With the information to be obtained from the mobile phone operator, the current location of the owner of the phone and the places he traveled in the past can be learned together with the time information. In order to obtain this information, special permission must be obtained from the court.

The Importance of IT Forensic

- Forensic information provides technical evaluation of the findings in the informatics environment and presentation to the cases as valid evidence. Such a service is important not only to reveal the criminals but also to identify the innocent. For this reason, today it is at least as necessary as a forensic medicine institution.

- In order for the forensic information institution to be established and live, centers that have the necessary hardware and software should be established and specialists who can use them should be trained.