NEW PERSPECTIVES ON COMPUTER FORENSICS*

Araş. Gör. Hasan SINAR**, ***

Introduction

In recent years,it is found out that there is a close relationship between the digitalisation process and criminal activities. This concept called "computer crime" or "computer-related crime", includes the use of computer technology to commit both traditional and new forms of crimes. However, contrary to this situation, computer technology can also assist in the fight against criminal activities from the forensic perspective. Meanwhile, the concept of "computer evidence" creates a new culture of forensic science in the digitalisation era.

This paper attemps to highlight some of the new forms of computer evidence and new techniques of evidence acquisition, preservation and analysis in digital environment.

But before evaluating these issues, it also examines the main trends which have importance in the growth of computer forensics. These

---

* This paper was presented at the 3rd European Academy of Forensic Sicence Triennial Meeting which was held in Istanbul in between September 22-27, 2003. I would like to thank Miss Funda Ünlü for her valuable support in the preparation of this paper.

** İstanbul Üniversitesi Hukuk Fakültesi Ceza Hukuku Anabilim Dalı.

*** Research Assistant, University of Istanbul Faculty of Law, Institute of Criminal Law and Criminology.

trends are[1]:

- the growth in the use of personal computers (PC),
- the new way of computer designing systems called as "distributed processing",
- the growth of computer networks, especially in the form of global internet.

It is easy to understand the effect of the first trend (the growth of the use of PC) on computer forensics. Because, unlike the early physically large computers, the progress in small, cheap and mobilized PCs allow people to use these machines in every part of their daily lives; thus, this enables us to store all kinds of (formal/informal) information in PCs[2].

The second trend called "distributed processing" has a little more complex effect on computer forensics. This new computer designing system constituted by a number of small computers which are linked together and that can feed one another with information and resources- like ATMs and bar code systems - . It is often used in big companies and other organisations as a primary way to see the performance of business. This system has some negative sides, like the opportunity of the misuse of data by the executives; but from the forensic perspective, it helps law enforcement officers to obtain information and evidence on criminal activities[3].

Third trend (networks and the internet) has a special importance in the growth of computer forensics. On the one hand, internet offers a new and powerful means by which a criminal can communicate, plan and commit a crime. But on the other hand, it offers means to law enforcement agencies to identify and detect criminal actitivites and also to reach and secure intelligence and evidence of these criminal activities in a powerful and effective way. Besides providing the possibility to obtain information, intelligence and evidence; internet is

---

1 SOMMER Peter, *"Digital Footprints: Assesing Computer Evidence"*. Criminal Law Review, Internet Special Edition 1998, 63.

2 SOMMER (dn. 1), 63.

3 SOMMER (dn. 1), 64.

a means of communication for law enforcement officers, whereby knowledge, information and practice can be easily and quickly exchanged[4].

These three trends have formed a new understanding of forensic science in the age of digitalisation. They have an impact not only on the progress in computer technology but also in computer forensics and in the types of evidence that can be found within computers.

Computer Evidence Processing

In General

The advancement of technology has created an entirely new source of evidence and also affected the practice of criminal law. According to the resources, today, 93% (percentage) of all business documents are created electronically. And also 70% of these documents stored just in computers and only 30% of them are printed out on paper[5]. So it's possible to say that, lawyers, experts and others, who are engaged in forensics business must be prepared to handle entirely new form of evidence which brings new and unique technical and legal aspects within it.

Before electronic evidence has become an integral part of investigation and procesecution process, the search and retrievel of these kind of evidence was an incredibly long and inaccurate process[6]. The documents obtained as electronic evidence could be opened only in their native format (i.e. accessed using the original software application in which they were created), printed out one by one, and scanned using old and slow methods (Optical Character Recognition - OCR-) and recreated electronically. This primitive process was not accurate enough and took unreasonable time. However, like other

---

4 SOMMER (dn. 1), 64-65

5 FELDMAN Joan E. - KOHN Roger I., *"Top Ten Things To Do When Collecting Electronic Evidence"*, http://www.forensics.com/pdf/Top_Ten.pdf.

6 LANGE Michele C. S. , *"E is for Evidence: Using An Online Repository to Review and Produce Electronic Data"*, http://www.krollontrack.com/LawLibrary/Publications/onlinerep.pdf.

information technology (IT) sectors, an increasingly improvement could be seen in the sector of "complex document research and recovery technology", especially by the effect of leaps and bounds. With the development of technology, electronic documents, spreadsheets and e-mails which are adressed; are created und functioned in multiple software applications and multiple operating systems (Windows, Unix, DOS and etc...). This enables to find evidence easily in that kind of typical storage areas. To convert the data to a read-only format such as pdf. or tiff. (tagged image file format) allows documents and e-mails, including all attachments, to be produced without the need to open the file in its original format. These improvements in computer technology provide us to save reasonable time, space and expense in the search and recovery of documents, e-mails and etc. and in the meantime to remain data in electronic form.

In the past, forensic expert testimony related to science and technology was accepted without question by criminal justice system (by the court, the judge, public prosecutor and by the attorneys). But today, because of the increased public awareness and possibility of the misuse of computer data; computer evidence processing is subject to challenge in criminal procedure[7]. Therefore, firstly, it is important to understand that computer evidence is very fragile and can easily and unintentionally be altered and destroyed. Secondly, because of its fragile nature, the processing of computer evidence must be done, by only properly trained computer forensic evidence experts who are specialised on the acquisition, preservation and analysis of such evidence[8], which are the main three elements of computer evidence processing. According to some writers, it is possible to say that, "the processing of such evidence for use in trial by an individual without proper triaining is like a first aid technician performing brain surgery with a pocket knife.[9]"

---

7 R. ANDERSON Michael, *"Computer Evidence Processing-Good Documentation Is Essential"*, http://www.forensics-intl.com/art10.html.

8 For an extensive review of this issue from practical aspect see DAVIS David J., *"Criminal Law and the Internet: The Investigator's Perspective"*, Criminal Law Review Internet Special Edition 19998, p. 48-59, especially 54.

9 R. ANDERSON Michael, *"Electronic Fingerprints-Computer Evidence Comes of Age"*, http://www.forensics-intl.com/art2.html.

Below I am going to attempt to examine the three main elements of compuer evidence processing, which are;

- acquisition
- preservation and
- analysis of computer evidence.

The Acquisition of Computer Evidence

In forensic computer investigations, the identification of relevant data is important but once the location of relevant data is identified, it must be retrieved. Computer forensic experts can retrieve data from virtually all stogare and operating systems, including many antiquated systems. By using proper tools, the acquisition of wide range data can include the rules in below[10]:

- Retrieval of data from seemingly inaccesible media
- Accessing active data on media
- Recovering deleted data and deleted e-mail
- Accessing inactive and unused data storage areas of various computer media and retrieving potentially important text.
- Accessing password protected and encyrpted files.
- Gathering information from databases, contact manages, electronic calenders and other proprietary software.

At this point there is a huge gap between individual Pcs and larger cooperate systems from the aspect of evidence acquisition from a computer as a computer forensic technique[11]. Therefore if an individual PC is handled in a proper and legal way and if it was within the control of a suspect, a great deal of important evidence about the suspect's activities is potentially available. But if it is a larger

---

10 NIMSGER Kristin M. - LANGE Michele C. S., *"Examining the Data- A beginners guide to computer-based evidence"*, http://www.krollontrack.co.uk/LawLibrary/US_articles/securityproducts.pdf.

11 SOMMER (dn. 1), 69.

cooperate system which consists of a number of computers and linked together by networks, things will change. Because, that sort of a large computer system has a greater potential that its seizure will cause damage to innocent people including employees, customers and creditors. And also if the computer system belongs to an international company there may be different components in different juristictions and time zone. So it is vital that only computer forensic experts who took enough computer forensic trainee courses and are specialised on larger corporate systems deal with such cases.

Here, once more, it is necessary to outline the importance of acquisition of computer evidence. Because once, raw evidence is required and the acquisition is complete; then the computer forensic analysis begins. And when you fail to obtain reliable evidence, this will prevent you to reach proper analysis result.

Another element of computer evidence processing is, the preservation of evidence.

The Preservation of Evidence

One area of the law that remains uniform despite technological advancement is evidence preservation. Electronic evidence, just like the other types of evidence is, fragile; even more fragile. When computers are involved, the duty to preserve the evidence is more significiant. Entering data, loading software, performing routine system maintenance or simply booting a computer can possibly destroy valuable files or metadata (data about the data) that is stored on the hard drive and that could be relevant in a lawsuit[12]. So it's vital for a forensic expert to check out[13],

- No possible evidence is damaged
- No possible computer viruses are introduced
- Extracted data is protected from mechanical or electromagnetic damage; and

---

12 SCHULTZ David H., *"Beyond Fingerprints- Recovery of Electronic Evidence"*, http://www.krollontrack.com/LawLibrary/Articles/beyondfingerprints.pdf.

13 NIMSGER Kristin M. - LANGE Michele C. S., (dn. 10).

- A proper chain of custody is maintained.

It is also important to mention that preservation of evidence is the primary element of all criminal investigations and computer evidence is certainly no exception. These basic rules of evidence never change. So, the original evidence should be properly preserved at all costs.

The Analysis of Computer Evidence

It's impossible to reach reliable results in a computer forensic analysis without taking into consideration the data recovery process. Data recovery enables us to access not only to active data, which can originally accessible from the hard drive but also, the deleted or unused files and directories in a computer system. In other words, this process reveals the mass of evidence which can then be mined for documents and data relevant to the criminal investigation.

Beyond data recovery process, in many cases, computer forensic experts face the problem of the alteration, damage or removal of computer evidence. In such cases, sometimes it is possible to recover the files completely and easily, but sometimes it requires long and tiring expert analysis process to put the puzzle back together. Therefore, it is necessary to remind that computer forensic experts must be well-traineed for such spesific situations and also they must never violate the basic rules and standarts of computer evidence processing.

After the acquisition of the computer evidence, the forensic analysis of preserved evidence must include the rules which are illustrated in below[14]:

- Recreating a spesific chain of events or user activity, including Internet activity and e-mail communication.
- Searching for key words and key dates
- Searching for copies of previous document drafts
- Searching for privileged information

---

14 NIMSGER Kristin M. - LANGE Michele C. S., (dn. 10).

- Authenticating data files and the date and time stamps of those files
- Comparing and contrasting computer code to determine whether a particular program is original or copied from a similar program; and
- Advising on what evidence is likely to be found on the computer media and identifying the most effective set of data to search.

Conclusion

Computer evidence is not basicly different from other types of evidence produced in criminal proceedings. The problems, in the evaluating process of computer evidence, arise especially from the fragility and transient nature of this new source of evidence. Therefore, in assembling the computer forensic puzzle pieces, it is necessary that the forensic experts identify a strategy for the investigation, ensure data acquisition, data preservation and generate the forensic analysis. By following the rules of these main elements of computer evidence processing, no electronic pieces of the evidence puzzle are left out and a successful investigation process can complete. But I must stress that since 1992 Amendments in Turkish Criminal Procedure Code, all evidences must be obtained legally. So must the computer evidence. As to the need to special legal provisions, it has to be discussed in future.