Information and Communication Systems e-Forensic Framework

Vladimir Remenar, Dragan Peraković, Goran Zovak
Faculty of Transport and Traffic Sciences
Vukelićeva 4, 10000 Zagreb, Croatia
{vladimir.remenar, dragan.perakovic, goran.zovak}@fpz.hr

ABSTRACT

Early identification, discovering and taking legal proceedings against the perpetrator of an electronic incident are necessary. It is necessary to investigate all electronic incidents adequately and promptly and adapt the legal framework and laws related to e-Forensics. e-Forensics is a relatively new discipline within which there is a low level of standardization and consistency. With the purpose of increasing the quality of performing e-Forensics and presenting the evidence in a possible judicial proceeding one has to define the legal framework of e-Forensics. e-Forensics procedures should be performed on every entity of information and communication system which include hardware, software, dataware, netware as well as lifeware and orgware. The analysis of current legal standards and methods used to perform e-Forensics is presented in the paper as well as the proposal of performing e-Forensics with defined procedures and methods with possible application on each and every entity in information and communication system.

KEYWORDS

forensics, e-Forensics, framework, information, communication, system

1 INTRODUCTION

In today’s world most of the information is created and saved on electronic media, mostly on hard drives. Computers are becoming extremely important in almost every investigation because of the increase in creating and storing information in digital form which is why e-Forensics represents the basis for discovering the evidence in the 21st century.

e-Forensics represents the combination of both technology and science which is trying to establish the way in which computer systems are involved in certain criminal activities. The science in e-Forensics includes knowing the methods and procedures which are used when collecting and analyzing the data i.e. possible evidence. On the other hand the technology represents different tools which enable the employment of e-Forensics methods and procedures. e-Forensics itself is a multidisciplinary skill in which a forensic must have a vast knowledge of network communication protocols, network communications and also about operating systems and file systems. e-Forensics is “who”, “what”, “when” and “how” on the electronic evidence. The aim of e-Forensics is to try to reconstruct the incidents in computer systems which have been performed by an individual or a group of people and present the gathered evidence in possible judicial proceedings (Wall & Paroff, 2004).

Although in most of the literature e-Forensics is called computer forensics, computer systems forensics or even digital investigation, those names do not show the real work area of e-Forensics. Computer forensics and Computer systems forensics terms are applied only while performing forensics of computers. And as such they should not be used while performing forensics on entire information and communications systems, its entities and data. Digital forensics term should only be applied while performing forensics on digital evidence because it does not include entities which participate in the process of creating, processing, storage and distribution of data. Due to aforementioned e-Forensics term should be used.

e-Forensics can be defined as a set of actions, procedures and methods in collecting and analyzing the data and entities in information communication system. As shown in Figure 1 information communication system includes all hardware, software, netware, dataware, lifeware and orgware resources as well as entities, products and services.

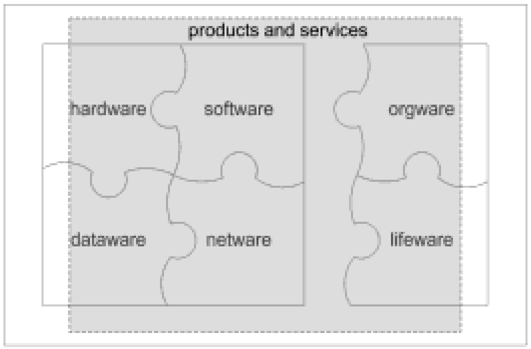

Fig. 1 – Information communication system

Since the legal framework is often nonexistent, insufficient or out of date the actions and procedures are left to individuals which lessens the possibility of accepting the gathered evidence in judicial proceedings. By defining the framework for carrying out e-Forensics and implementing it in regulations it is possible to achieve a significant progress in the quality of carrying out e-Forensics with the purpose of establishing the facts of a higher quality.

2 INFORMATION AND COMMUNICATION SYSTEM

Information and communication system does not, for example, include only computer equipment. Information and communication system contains assets that can be defined as all and every element of information and communication system. Assets can be tangible (for example computers) and intangible (for example procedures that define how system works). According to aforementioned, e-Forensics procedures should be performed on all elements of information and communication system which can be categorized into: hardware, software, dataware, netware, lifeware and orgware as shown in figure 2. Products and services are the result of the work of information and communication system.

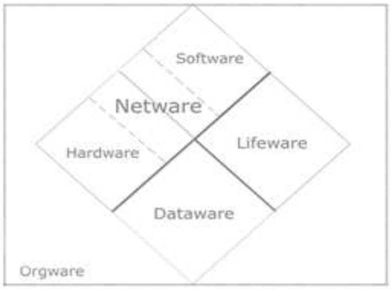

Fig. 2 - Elements of information and communication system

2.1 Hardware

All physical assets of information and communication system can be categorized as *hardware* entity of information and communication system. Hardware contains everything tangible like computers, rooms, room equipment, etc.

2.2. Software

Part of the nontangible assets of information and communication system, in which for example belongs operating system and applications, can be categorized as *software* entity. Any installed and running/non-running operating system and any application installed at any time in the timeline is software.

2.3. Dataware

Nontangible assets which is data and/or information of information and communication system can be categorized as *dataware* entity. Dataware entity holds all data and information as well as rules, standards and procedure for transferring and storing the aforementioned.

2.4. Netware

All communication entities of information and communication system can be classified as *netware* entity. Netware is every element of telecommunication and/or computer network used for collecting, transfer and distribution of data and information. The aforementioned includes communication media, routers, switches, etc.

2.5. Lifeware

All human factor which is somehow included in functioning of information and communication system can be categorized as *lifeware* entity. Lifeware can be any person which is using information and communication system, designers, operators, etc.

2.6. Orgware

Procedures, processes and similar which determine methods, procedures and principles of functioning of information and communication system can be classified as *orgware* entity.

3 REGULATIONS IN THE REPUBLIC OF CROATIA

The fundamental document in the Republic of Croatia relevant to the research of this field is Information Security Law in which the basic concepts of information security, measures and standards of information security and government bodies for information security such as ZSIS, UVNS and CARNet CERT are defined as well as their authorities and duties. The field of computer crime, i.e. cybercrime, is defined in the Decision on passing the law regarding Confirmation of Convention on Cybercrime. The Convention on Cybercrime represents a form of an international treaty which Croatia ratified in 2003. It was introduced by the European Council on 23rd November 2001 and it became effective on 1st July 2004. Extremely important documents related to the field of security are Regulations on Standards of Information System Security and Regulations on Coordination of Prevention and Response to Computer – security Incidents. The National CARNet CERT has published a vast number of documents, but the only document relevant to the subject of this paper is The Basics of Computer Forensic Analysis.

The procedures of performing e-Forensics are described only in CERT's document, the Basics of Computer Forensic Analysis, which, as the title itself suggests, covers only the basics. The document provides only a suggestion of performing e-Forensics and it has no legal grounds in judicial proceedings. As such it is a good basis for the development of a more detailed document which can serve as a guideline for performing e-Forensics.

The only document which defines performing of forensics is Regulations on Standards of Information System Security. Article 223 of the mentioned regulation provides that in case of computer security incident by a body or a corporation from article 2 (referring to article 1 subsection 2 of Information Security Law) one is obliged to act according to Regulations on Prevention and Response to Computer – security Incidents Coordination introduced by ZSIS in 2008. However, according to article 1, subsection 2 of Information Security Law, the mentioned regulations refer only to government bodies, local and regional government and corporations with public authority which use classified and non-classified data. According to afore mentioned, the Croatian laws do not state how private companies and corporations should deal with electronic incidents nor do they state how e-Forensics should be performed so that the evidence can be accepted in judicial proceedings.

4 e-FORENSIC PROCEDURES

e-Forensics used to be performed only on permanent data, i.e. the data stored on a certain kind of media even when there is no electrical power available to the media. With the increased usage of information communication systems the need to perform e- Forensics on volatile data, i.e. the data which is not permanently stored on some media but temporarily or in transmission through telecommunication or computer network and their entities, has emerged. The importance of performing e-Forensics on volatile data is constantly growing because of the aforementioned. Whether e- Forensics is being performed on permanent or volatile data the main aim is to identify, gather, store and analyze the data in a way which preserves the integrity of gathered evidence so that those could be used in possible judicial proceedings. At the same time it is necessary to determine how the data was created, modified and / or used and who performed the aforementioned in a time lapse on some information communication system element, as is shown in Figure 3.

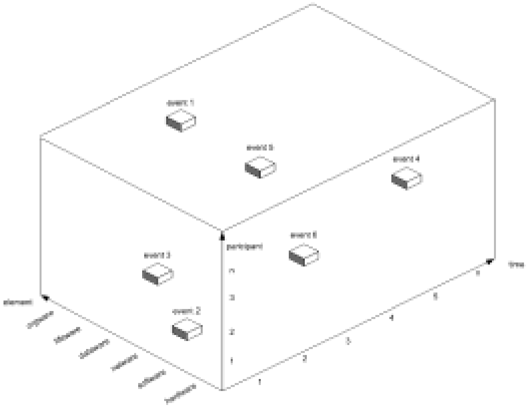

Fig. 3 – Determining the sequence of the events

During the mentioned steps it is necessary to make detailed records and in the end make a detailed report about what was found and about the performed procedures. In literature it is possible to find different definitions of the steps involved in the performing of e-Forensics. From three – step generalized models which include preservation, searching and reconstruction (Carrier, 2005) or preservation, authentication and analysis (Bidgoli, 2006) to five – step models which include consultations with the client, preservation, gathering, discovering, analyzing and testifying (Wall & Paroff, 2004) and even nine – step models which include identification, preparation, approach strategy, preservation, gathering, testing, analyzing, presenting and returning to the owner (Reith et al., 2002). The mentioned models have advantages but there are also some disadvantages like insufficiently defined procedures or the presence of unnecessary procedures with the absence of particularly necessary ones.

5 FRAMEWORK FOR PERFORMING e-FORENSICS

Based on the conducted research described in chapters 2 and 3, an optimal model for performing e-Forensics in 6 steps, whether on permanent or volatile data, has been designed. The suggested model can be used for performing the procedures of e-Forensics on information communication system as a whole or on its entities. It can be used on computers, computer systems (hardware, software) or telecommunication network and its entities. The suggested model consists of six steps: identification, gathering, preserving, analyzing, documenting and reporting. The sequence of events can be seen in Figure 4.

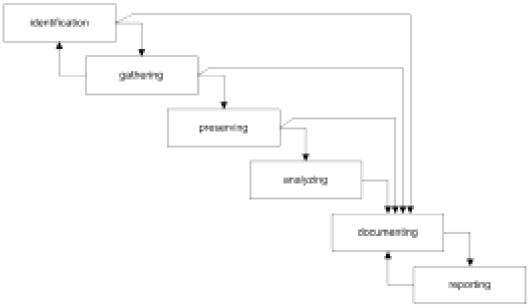

Fig. 4 - 6 steps of performing e-Forensics

Suggested model is a framework for performing forensics analysis on any entity of information and communication system. As such these steps can be implemented in legislation as steps for performing e-Forensics. Depending on analysed entity of information and communication system (hardware, software, dataware, netware and so on) it is necessary to use specialized tools and procedures necessary for that entity.

5.1. Identification

In order to gather relevant and high – quality data it is necessary to identify which data and resources during e-Forensics are needed. By identifying the type of the data (classified and non classified) or resources and possible format of data or resources it is possible to assess the feasibility of e-Forensics, if necessary get all the permits and forms needed and hold consultations with lawyers, owners of the resources and other stakeholders on whose resources e-Forensics is going to be performed. By identifying the data that a person wants to gather and analyze the possibility of making a mistake or destroying the data lessens while the possibility of breaching certain legal regulations during the performing of e-Forensics lessens or even completely disappears by identifying the type of the data. By examining the feasibility one is trying to assess the possibility of gathering and analyzing required data without changing or destroying it and determining whether it is possible to perform e-Forensics on the system which is working or whether it needs to be turned off. Consultations with lawyers are necessary when it is not possible to determine whether or not some constitutional or legal act will be breached during e-Forensics. Consultations with the owners of the resources and other stakeholders are necessary when changing the state of the system, for example if it is of the utmost importance that the system is working and it is not possible to turn it off.

5.2. Gathering

After identifying the data which need to be analyzed they have to be gathered in their original state, preserving the authenticity. During the gathering of the data it is possible that some new relevant data is found and so one has to go through the step of identifying the new data and then continue with the gathering. During the gathering of the data it is necessary to preserve the data in its original state and mark it unambiguously for later identification with the purpose of proving its authenticity. For that purpose it is possible to use MD5 hash algorithm for calculating a hash value of an evidence file. Gathering itself does not necessarily signify gathering only electronic data but also physical resources like CDs and DVDs, different paper notes etc. Such resources also need to be unambiguously marked, their position must be photographed and other possible physical parameters should be determined.

5.3. Preserving

Gathered data or resources must be preserved in their original state before analyzing. In the case of physical resources preserving the resources might mean that the computer has to be transported into a safe laboratory and if not necessary not turned on or connected to the network. If for example dealing with a hard drive or a CD one has to make its identical bit-by-bit copy on which analysis will be performed and the original disc needs to be deposited in a safe place. In the case of electronic evidence one has to provide their copy and the stability of volatile data gathered from telecommunication network or RAM. Before storing the gathered electronic data on a media, the media needs to be disinfected in order to avoid the reappearance of some previously stored data during the analysis. For preserving the authenticity of the original data one has to use various hardware and software solutions which make writing on the media, on which the data is stored, impossible.

5.4. Analysis

The analysis of the gathered materials should be performed in a controlled environment and on the previously made copies in order to avoid or at least lessen the possibility of destroying or changing the original data i.e. resources. During the analysis one has to establish the timeline of the events and entities which were involved in the creating, changing or accessing the resource which is being analyzed. For example if the communication in the communication network is being analyzed it is necessary to establish the source, the destination, the entities involved in the communication network and the human factor that initialized or in some way influenced the communication process in a certain time frame. In case an analysis of a computer or a mobile terminal equipment is being performed, the dates of creation, modification and accesses have to be determined for each record individually. Also, possible hidden data of the application and the timeline of the interaction between an individual and the user equipment have to be analyzed. Each analyzed data or resource has to be unambiguously marked, identified and compared with the original using for example MD5 checksum algorithm in order to prove that the data or the resource has not undergone any changes during the analysis.

5.5. Documenting

During each of the previous steps one has to make detailed notes and documentation about the undertaken activities. The notes and documentation have to be complete, accurate, comprehensive and without any mistakes or corrections. The notes and documentation should at least contain:

- a warrant for starting the procedures of e-Forensics,
- the documentation about authorisations and responsibilities of the participants in e-Forensics process,
- the exact procedures performed in each of the steps which enable the correct repetition of the undertaken steps,
- for each procedure one has to record the description and the results of that procedure,
- all the unusual occurrences which appeared while e-Forensics was performed,
- all the relevant data about the users of the system on which e-Forensics was performed,
- all the changes which happened while e-Forensics was performed,
- time and date have to be specified for each note.

Notes and documentation have to be stored in a safe place. It is also advisable not to delete the notes but rather mark the incorrect note and write the new correct one.

5.6. Reporting

The making of the final report depends on the demands of the organization or bodies for which it is being made. It should at least consist of:

- the data about the organization or individual that asked for e-Forensics,
- the data about the organization or individual that performed e-Forensics,
- an identification mark of the procedure of e-Forensics ,
- the data about the participants involved when e-Forensics was performed,
- the date of starting and finishing all the steps performed in e-Forensics,
- the list and the pictures of all the gathered and analyzed resources as well as their identification marks such as the unique identification mark and possible serial or identification numbers (such as mobile phone IMEI number or SIM card IMSI number),
- the list of all gathered electronic data and their unique identification marks and relevant characteristics (for example time and date of sending and receiving an SMS, time and date and identification mark of the user who accessed a certain file, log, etc),
- the description, time and date of the undertaken steps while e-Forensics was performed,

- the results of e-Forensics,
- the opinion and the conclusion.

6. CONCLUSION

Based on the conducted research numerous inadequacies of a former way of performing forensic procedures in the field of information communication traffic and applying it within Croatian laws have been noticed. An optimal model of performing e-Forensics in 6 steps is presented in the paper. The application of the suggested model with some corrections in Croatian regulations will increase the quality of procedures performed in e-Forensics and the quality of results of a forensic procedure, i.e. unique, unquestionable establishment of facts. In addition, the data about all involved entities will be preserved if applying the suggested model.

Based on the suggested model it is possible to define specific rulebooks and guidelines for performing e-Forensics on the each and every entity of information and communication system.

7 REFERENCES

1. Bidgoli, H. Handbook of Information Security. Wiley. 2006.
2. Brenner, S. W. U.S. Cybercrime Law: Defining Offenses. Information System Frontiers. 2004;6(2):115-132.
3. Carrier, B. File System Forensic Analysis Addison-Wesley Professional. 2005.
4. Computer Forensics. US-CERT. 2008.
5. Giordano, S. M. Electronic Evidence and the Law. Information System Frontiers. 2004;6(2):161-174.
6. Legiland, R., & Krings, A. W. A Formalization of Digital Forensics. International Journal of Digital Evidence. 2004; 3(2):1-31.
7. Meyers, M., & Rogers, M. Computer Forensics: The Need for Standardization and Certification. International Journal of Digital Evidence. 2004;3(2):1-11.
8. Decree for Proclamation of Information Security Law (In Croatian: Odluka o proglašenju Zakona o infroamcijskoj sigurnosti). Hrvatski Sabor. 2007.
9. Decree for Proclamation of Law for Affirmation of Convention on Cybercrime (In Croatian: Odluka o proglašenju Zakona o potvrđivanju Konvencije o kibernetičkom kriminalu). Hrvatski Sabor. 2002.
10. Basics of Computer Forensics Analysis (In Croatian: Osnove računalne forenzičke analize). CARNet CERT. 2006.
11. Rulebook for Coordination of Prevention and Response on Computer Security Incidents (In Croatian: Pravilnik o koordinaciji prevencije i odgovora na računalno-sigurnosne incidente). Zavod za sigurnost informacijskih sustava. 2008.
12. Rulebook of Information Systems Security (In Croatian: Pravilnik o standardima sigurnosti informacijskih sustava). Zavod za informacijsku sigurnost. 2008.
13. Reith, M., Carr, C., & Gunsch, G. An Examination of Digital Forensic Models. International Journal of Digital Evidence. 2002;1(3):1-12.
14. Schwerha, J. J. Cybercrime: Legal Standards Governing the Collection of Digitl Evidence. Information Systems Frontiers. 2004;6(2):133-151.
15. Taylor, M., Haggerty, J., & Gresty, D. The Legal Aspects of Corporate Computer Forensic Investigations. Computer Law & Security Report. 2007;23:562-566.
16. Volonino, L. Electronic Evidence and Coputer Forensics. Communications of AIS. 2003;12:1-23.
17. Wall, C., & Paroff, J. Cracking the Computer Forensics Mystery. Utah Bar Journal. 2004;17(4):10-14.