NATIONAL UNIVERSITY OF PUBLIC SERVICES

ZSOLT ILLÉSI

Official and author's review of PhD thesis titled

Forensic investigation of attacks and criminal offenses in information technology environment

Scientific advisor:

Prof. Dr. LÁSZLÓ Kovács

Budapest
2012

The scientific problem

Sanctioning attacks and crimes offended in times of peace is the privilege of the state in modern countries which adhere to the rule of law. Penalisation rules are determined by the law. Imposing penalties is possible under conditions defined in law. The format and formalities to be followed also laid down in regulations. The court is to decide whether the conditions defined in the law are met. The court is to comply with the law and it is to enforce the compliance.

Thus it is not possible to take sanctions for one's own hand for those who become victims of any crime. They have to recourse to the court to vindicate their rights. With the proliferation of information technology the numbers of related cases are increasing simultaneously. Based on my experience the attacked (target, plaintiff) most of the time cannot enforce its rights efficiently, or the enforcement is partial. Inadequate approach may prevent the success of remedies, compensation, and as a result:

a) the quality and quantity of available evidence is not sufficient,
b) appropriate documentation of the forensic investigation is not available or not sufficient,
c) because of the inappropriate evidence handling the investigation is not repeatable,
d) analysis or interpretation may produce errors.

In the midpoint of my dissertation there is the IT forensic investigation. This is an **interdisciplinary domain**, where law supplies functional specification, the realisation framework comes from criminalistics, but all these shall be implemented in the field of information technology. My dissertation, in spite of its interdisciplinary nature, basically an information technology paper, which in the first line complies with the requirements of the PhD Institute in Military Technology of Military Engineering.

Traces extracted from the information technology, the trace acquisition method and toolkits, and the considerations of the related activities, however, are different of the physical trace concept built around current computer forensic science. Definitions used defines the methods of evidence acquisition, preservation and storage, determine the range of tests that can be performed, and provide a framework for the interpretation of the results. Residues and prints definitions serve well to describe the world constructed from physical entities. Here are all item has its unique feature, but data for example may available simultaneously in several places. The concept of physical trace determines which of the characteristics of the trace is in the centre of preserving, processing or interpreting during a criminal investigation or analysis. The methods and tools used will be appropriate for the selected features of the investigations. **In computer forensic investigations therefore**, in accordance with the specialty of data, **the definition of a digital trace concept is essential.Based on this digital trace concept the related evidence handling, processing and interpretation shall be developed.**

Forensic practice forced information technology experts to develop pragmatic techniques of taking evidence that will stand the test of courtrooms. **Applied techniques and methodologies these days are specific to related tools and technologies.** Windows, Linux, iOS, and other operating systems, different file systems, wired and wireless computer networks, cell phones, etc. have their individual investigation means. These available methods, techniques and tools do not establish a single scheme. There is no guidance that would be used to decide the overall relationship of these investigations, and there is no indication for the required professional competence.

As a result, the professional competence outlined in national law cannot or very difficult to interpret even for information technology experts.

In absence of appropriately identified computer forensic methods and techniques it is not possible to formulate correct and clear questions. As a result experts and the designating authorities often grind in two mills. Consequently, **a model is to developed that takes into account the characteristics of trace data, summarizes the activities undertaken in the course of IT expertise, their relationship, and providing a reference point for each professional competencies required to perform the activities**.

Besides the conceptual problems of the digital trace putting theory into practice also a key factor in the effective and efficient detection, trace preservation and acquisition in crime scenes involving information technology elements. Success of treating professionally the information technology based traces during investigations depends on the preparedness and IT knowledge of the members performing on-site investigations of the competent authority. However, this task is very important in terms of computer forensic investigations. As a tailor cannot create a superb suite without sufficient quality and quantity of materials, it is impossible for the best computer forensic expert to provide adequate evidence based on incomplete data, badly collected traces. **It is** therefore **necessary to develop a unified model that integrates the particular features of physical and information technology, including the main forensic procedures.** This model will establish the appropriate protocols and serve as a basis for the methodological manual of Hungarian computer forensic experts.

Aims of research

During my research the following sub-objectives were determined:

My aim is to **analyse in a forensic manner the attacks and crimes committed in the information technology environment**, i.e., to determine what kind evidence are available in information technology environment about people, technical components and what behaviours.During my research I want to study information technology systems as evidence source. I would like to decide if information technology has a set of special characteristics which are atypical in general forensic trace sources. Therefore **I would like to organize the layout of information technology, such as proof and evidence source characteristics, and I intend to outline digital evidence taxonomy**.

My aim is also to **develop a computer forensic investigation model, which unifies the currently fragmented hardware and software technology based activities**. My aim is also to integrate the similar activities into classes, defining classification criteria of the functions, and determining the necessary professional competence of task execution.

Last but not least, I would like to **develop a high level model which homogeneously demonstrates key forensic activities including the actors with expert roles in criminal prosecutions, together with the general activities in combination with information technology system forensic investigation model**.This high level model shall serve as a basis for related professional protocols and the methodological manual of Hungarian computer forensic experts.

Applied research methods

My research based on my practical experience, and additionally I performed a wide range literature exploration, exploring both national and international literature. During my bibliography research I identified the most significant legal, general and forensic specific information technology factors from the standpoint of my dissertation. I continuously tested the acquired knowledge in my practice as a computer forensic expert in the course of criminal prosecutions and civil actions. Within the Chamber of Judicial Experts –based on my research– I have initiated the development of methodological manual of Hungarian computer forensic experts, and revived the regular professional conference for computer forensic professionals. I would like to organise this conference in the future, and to be a regular event in the future.

I attended regularly –as a member of the audience or a speaker– the related national and international scientific conferences and other proceedings. I presented the results of my research in a number of scientific conferences at home and abroad, both in Hungarian and in English. I published my findings not only in conferences but also in peer-reviewed journals.

Structure of the thesis

I split my thesis into three chapters:

Chapter 1: I reviewed the attacks and crimes which can be committed in information technology environment, the issues which substantiating the methods of proof, and the evidence requirements. In this chapter I define –in accordance with the concept of physical trace– the concept of digital trace, describing the characteristics of the legal classification. I also specify the forensic characteristic of the information technology environment.

Chapter 2: I propose some improvement and extension on Brian Carrier initial abstract layer model which. Thus, a complex taxonomy is available for computer forensic experts to put all existing information technology related investigation in order. This taxonomy also suitable to describe and determine all necessary professional skills.

Chapter 3: I analyze the professional issues of evidence acquisition, preservation and storage in the information technology environments. I prove that it is possible to model computer forensic functions, and based on this model it is possible to develop the methodological manual of Hungarian computer forensic experts. At the same time in this chapter I introduce the high level model for evidence acquisition, preservation and storage function.

Conclusions

Information and communication technology increasingly pervades our daily life, embedded in the socio-economic processes.The penetration of technology, however, has increased dependence of the individuals, organizations, states. Dependence also increased the vulnerability of all.A particular form of this vulnerability is a new type of conflict: the rising appearance of attacks and crimes committed in information technology environment.These conflicts, in time of peace, decided in the courts.Judicial law enforcement of court is grounded in law. However the effectiveness and efficiency of the law enforcement based on sufficient quality and quantity of evidence.As a new type of evidence source –based on a new type of technology– is the preventive subset of computer security. **In the focus of this new source there is the analysis of traces arouse from information systems.**This is an **interdisciplinary domain, in the intersection of law, criminalistics, and information technology: computer forensics**.

The current investigative activities, information related forensic methods, however, do not form a coherent system.The law controls in different ways and in different extent the professional competence level requirements of all persons who play expert role in criminal prosecutions.The current forensic investigations are operating system, file system, computer network, and cell phone specific at the moment. These investigative methods and techniques are individual and isolated. They each stand the test of the courtroom, but do not form a coherent professional methodology.

In my dissertation, **I reviewed** the organization of law and forensic traces, evidence and taking evidence, and **found that the trace concept serves as a base for the whole criminal investigation process**. The professional functions based on the applied trace concept during evidence acquisition, preservation and during all forensic activities.Comparing physical trace concept with the data-traces which come from information technology **I found that the trace concept based on residues and prints is not adequate. This physical concept does not reflect correctly the characteristics of digital trace initiator, trace carrier and the trace generation process**.Therefore, **I derived a new trace concept (digital trace), which is consistent with both criminalistic and trasology trace concepts**, and meet the characters of the information technology environment.Based on the clarification of the digital trace concept I **classified and organized the characteristics of digital traces based on their specific features**.

In my dissertation I have explored the general forensic features, the unique characteristics of information technology as well, and I presented these attributes to the consequences on computer forensic investigations.After completion of the digital trace taxonomy I systematized of related activities.The basic problem of the organization previously was that how the diverse computer forensic activities can be classified in a way that the resulting function groups form a closed logical unit, do not repeat the individual classes of functions, and to some extent define the tasks required to carry out professional competence.In the fulfilment of this task I **summoned the Brian Carrier's abstract layer model**.I **improved and extended** the original model, completed with the necessary elements, which have enabled it to have a complex manner suitable for forensic investigations of information technology environment that contain digital traces. In addition this enhanced model helps identifying the necessary professional competences.

Following the definition of digital traces I defined the taxonomy of traces. Then I organized the functions related to computer forensic and defined the legal requirements for methodological manual of Hungarian computer forensic experts. Consequently I developed a high-level model of forensic functions in criminal prosecutions.

After determining the activities of the players – with regards to the life cycle model of traces– I extended the traditional evidence search, preservation and analysis model to comply with all significant issues that arouse from the concept of digital traces of information technology environments.As a summary of these tasks I **developed a complex UML model that integrates the physical and information technology related characteristics of the forensic issues of the criminal prosecutions**.This complex model is not only supports forensic investigation, but in my opinion, also provides a basis for forensic protocols, as well as serves as a basis for methodological manual of Hungarian computer forensic experts.

In my opinion, my research was effective, I have been achieved the stated scientific objectives.I think, I can use profitably all the ideas from my dissertation in the future in my computer forensic activities.I believe that my achievements are useful not just for me or for a narrow circle of forensic experts, but also more widely. Therefore in defence and civil sectors may also profit from my research findings.

New scientific achievements of the thesis

1) I defined the digital trace in accordance with the trace definition of both criminalistic and trasology (residues and prints).
2) I classified and organised the digital traces by their individual characteristics.
3) Improving and extending Brian Carrier's original abstract layer approach of analysis, I recommend a complex taxonomy, which is suitable for organising, describing all information technology related forensic investigation, in addition the enhanced model helps identify the necessary professional competences.
4) I developed a high level UML model suite which integrates specific forensic features and questions of the physical and the information technology. My model-suite constitutes the relevant professional protocol set and the development of the methodological manual of Hungarian computer forensic experts

Practical usability of thesis

I propose to use my whole dissertation in higher education, in forensic and criminal science subjects. I also propose the use of my dissertation in computer forensic experts' periodic in-service training.

The layered model of computer forensic investigations –defined in my dissertation– is capable of classifying researches in the field of computer forensics. This high level model also capable of classifying the related methods and techniques, identifying and analysing their relationships.

The high level trace search, trace safeguarding, and trace preservation model I propose in my dissertation is applicable for defence services, especially their investigative branches.

My dissertation may constitute a basis for the methodological manual of Hungarian computer forensic experts.

Publications

Reviewed publications in Hungarian

1) László KOVÁCS, Zsolt ILLÉSI: Cyberhadviselés
in Hadtudomány Vol XXI. No. 1–2, pp. 29–41
ZMNE, Budapest, 05.2011.
ISSN 1215–4121

2) Zsolt ILLÉSI: Az igazságügyi szakértés modellezése
in Hadmérnök, Vol. V. No. 4, pp. 122–132
ZMNE, Budapest, 2010.
ISSN 1788–1919

3) Zsolt ILLÉSI: WiFi hálózatok igazságügyi szakértői elemzése:
WiFi hálózatok felderítése
in Hadmérnök Vol. IV. No. 3, pp. 285–302
ZMNE, Budapest,09. 2009.
ISSN 1788–1919

4) Zsolt ILLÉSI: Krimáltechnika szerepe az informatikai védelem területén
in Hadmérnök Vol. IV. No. 1, pp. 170–183
ZMNE, Budapest, 03.2009.
ISSN 1788–1919

5) Zsolt ILLÉSI: Számítógép-hálózatok krimináltechnikai vizsgálata
in Hadmérnök, Vol. IV. No. 4, pp. 163–175
ZMNE, Budapest, 12.2009.
ISSN 1788–1919

6) Zsolt ILLÉSI: Open source IT forensics – avagy nyílt forráskódú programok felhasz-nálása
az informatikai igazságügyi szakértésben
in Bolyai Szemle, Vol. XVII. No. 4, pp. 181–195
ZMNE, Budapest, 2008.
ISSN: 1416–1443

7) Zsolt ILLÉSI: Botnetek kialakulása, használatuk, trendjeik
in Hadmérnök. Vol. III. No. 2, pp. 129–137
ZMNE, Budapest, 2008. június
ISSN 1788–1919

8) Zsolt ILLÉSI: Számítógép-hálózat audit
Networkshop 2008. [Online]
Nemzeti Információs Infrastruktúra Fejlesztési Intézet, 04.2008.
http://nws.niif.hu/ncd2008/docs/phu/084.pdf
[last check: 30.09.2012.]

Publication in English

1) Zsolt ILLÉSI: NEEDLE IN A HAYSTACK – A Quest to Identify, Classify, and Reduce
Data to Find Adequate Digital Evidence
in VIII Konferencija Naukova Studentóv 8th Students konference, pp. 275–281
Oficína Wydawnicza Politechniki Wroclawskiej, Wroclaw, Poland, 2010.
ISSN 1732–0240

Publication in Conference Proceedings

1) Zsolt ILLÉSI: Information violation (?) and computer forensics
Óbudai Egyetem, Budapest: 19.11.2011.
ISBN 978–615–5018–20–6

2) Zsolt ILLÉSI: Bizonyítás a kibertérben
Hacktivity 2011. [Online]
https://hacktivity.com/hu/archivum/videostream/139/hu/
[last check: 30.09.2012.]

3) Zsolt ILLÉSI: Tűt a szénakazalban
Hacktivity, [Online], 2010.
https://hacktivity.com/hu/letoltesek/archivum/47/
[last check: 30.09.2012.]

4) Zsolt ILLÉSI: Computer forensics need for a domestic and/or EU 'hash factory'
in XX VI. Nemzetközi Kandó Konferencia kiadványa
Óbudai Egyetem, Budapest, 04.11.2010.
ISBN 978–963–7158–04–9

5) Zsolt ILLÉSI: Hackers beware! – Digitális nyomok az informatikai rendszerekben
Hacktivity 2009, [Online], 2009.
https://hacktivity.com/hu/letoltesek/archivum/105/
[last check: 30.09.2012.]

6) Zsolt ILLÉSI: Rádiós hálózatok krimináltechnikai vizsgálata
in 2009. XXV. Nemzetközi Kandó Konferencia kiadványa
Óbudai Egyetem, Budapest, 2009.
ISBN 978–963–7158–04–9

Curriculum Vitae

First name:	Zsolt
Last name:	ILLÉSI
Date of Birth:	11.02.1967.
Education:	PhD Institute in Military Technology of National University OF Public Services (prior: Miklós Zrínyi National Defense University): PhD studies (2007 -) Kodolányi János University of Applied Sciences: BA faculty of social science and economic translator (English), Budapest, Hungary (2007) University of Veszprém: MSc in teaching informatics, Veszprém, Hungary (2005) University of Pécs: BL faculty of state and legal sciences, Pécs, Hungary (2002) College of Dunaújváros: BSc in computer science, BT in Teaching Technical Sciences, Dunaújváros, Hungary (1997)

College of Dunaújváros: BE in technical instruction, specialization on Mechanic, Dunaújváros, Hungary (1993)

Work experience:

assistant professor (adjunktus), College of Dunaújváros (Dunaújváros, Hungary) (02.2011. -)

partner, senior consultant, Proteus Consulting Kft. (Budapest, Hungary) (2001. május –)

IT audit and compliance manager, Mazars (Írország, Dublin) (05.2005. – 06.2006.)

individual entrepreneur (Dunaújváros, Hungary) (01.1999. –)

IT expert, Insurance Technology Kft. (Budapest) (06.1998. – 12.1998.)

senior IT supervisor – hot rolling mill, Dunaferr Acélművek Kft. (Dunaújváros, Hungary) (06.1993.– 05.1998.)

Language skills:

English C1 complex

German B1 complex

Professional activities: **Teaching:**

- Intelligent systems
- Quality assurance and audit of Information Systems
- Database Management

Research and development, consulting:

IT forensics

IT risk management and audit

main international references:

- Allied Irish Bank (AIB), Ireland
- BUPA Ireland, Ireland
- Courts Services, Ireland
- Department of Agriculture, Ireland
- Health Service Executive, Ireland
- Saudi Arabian Monetary Agency, Saudi Arabian Stock Exchange (TADAWUL), Saudi Arabia
- Saudi Arabian Telecommunication Company (STC), Saudi Arabia

main national references:

- BNP Paribas Bank Hungary
- ERSTE Bank Hungary
- FHB
- KBC GSH (prior: K&H Bank Hungary NyRt.)
- MATÁV
- OMKMK
- Paksi Atomerőmű Rt.

Specialities: forensic investigation of IT systems

criminal informatics

IT risk management

IT audit