ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΕΙΔΙΚΑ ΘΕΜΑΤΑ ΔΙΚΑΙΟΥ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Ενότητα 4: FORENSICS

Λίλιαν Μήτρου, Αναπληρώτρια Καθηγήτρια

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Internet Forensics: Legal and Technical Issues

Maria Karyda and Lilian Mitrou
University of the Aegean, Department of Information and Communication Systems Engineering, Karlovassi, Samos,GR 83200, Greece
{mka, L.Mitrou}@aegean.gr

Abstract

This paper provides a combined approach on the major issues pertaining to the investigation of cyber crimes and the deployment of Internet forensics techniques. It discusses major issues from a technical and legal perspective and provides general directions on how these issues can be tackled. The paper also discusses the implications of data mining techniques and the issue of privacy protection with regard to the use of forensics methods.

1. Introduction

Within the last years, industry as well as governments uses Internet at an increasing pace in basic functions and core activities. Governments use Internet to provide citizens and businesses with public services. Electronic government services that are provided to citizens typically include paying income tax, demanding and issuing personal documentation such as birth and marriage certificates, issuing and renewing driving licenses, participating in election processes and so forth. Those addressed to businesses usually entail corporate tax and VAT paying, paying social contribution for employees, providing data for statistical purposes, and participating in public procurements. Businesses, on the other hand, become dependent on Internet not only to communicate and provide their product and services to customers but also to enact new business models which are entirely dependent on the use of the Internet, such as electronic marketplaces, online auctions, online bartering and information brokerage.

However, technological developments have also "a dark side": Since crime tends to follow opportunity and the Internet provides many new opportunities, new crimes as well as new ways to commit "traditional crimes" by means of new technologies emerge [1]. Due to the "anonymity" of the cyber-criminal activities and to the fact that these new (types of) crimes are not restricted by geographical boundaries, they have far-reaching consequences. In a networked world, where all points are equidistant from all others and are accessible from everywhere, the principles of the legal system cannot impose obligations on everyone to comply with all law [2].

As a result, governments and business become increasingly vulnerable to threats originating from the Internet. Currently, among the most common threats originating form the Internet, one has to face malicious programs that can expose confidential information (such as viruses, spyware, worms, Trojans), phishing attacks, identity theft, spam, key logging and denial of service attacks. The 2006 E-Crime Watch survey [3] reports that businesses cite a decline in security events, compared to previous years, yet an increase in the financial and operational losses caused by electronic crime incidents. 63% of respondents to the same survey reported that their businesses suffered operational losses as a result of e-crime, 40% reported financial losses and 23 % reported that their organization's reputation had been damaged by such incidents.

Due to the growth of cyber crime in recent years, digital forensics have become of paramount importance [4]. Investigating and gathering of appropriate evidence for prosecution often proves to be a difficult and complex task. “Communications laundering”, routing transmissions through a series of jurisdictions to frustrate attempts to trace the source, or the extensive use of cryptographic techniques to render data unintelligible are usual steps, taken by cyber-criminals, to hide or disguise their activities [5].

In this paper we use the term ‘Internet forensics’ (also referred to as Cyberforensics or Network forensics) as a sub-category of computer-forensics. Computer-forensics refers to the collection, preservation and analysis of computer-derived evidence to ensure its admissibility as evidence in a legal proceeding [6]. Internet forensics includes techniques and methodologies to collect, preserve and analyze digital data on the Internet for investigation and law enforcement purposes. It is a relatively recent field of research and practice that has evolved as a result of the increasing use of Internet and the move of criminal activity. It is also argued that Internet forensics evolved as a response to the hacker community [7].

Internet has become not only a crime scene, but also a breeding ground for primary and secondary sources of evidence. “Cyberspace has become the neighborhood wherein law enforcement officers must regularly interact with their constituency” [6]. A forensics investigation requires the use of disciplined investigative techniques to discover and analyze traces of evidence left behind after a committed crime [8]. In all contexts, Internet forensics involve the recognition, recovery and reconstruction of digital evidence and its management in a way that renders it admissible in prosecution and –more generally – in legal proceedings [4]. Like other forensic sciences, Internet forensics begin by collecting a large number of intensely diverse variables or attributes, and culminate in pattern matching among these variables in order to individualize evidence. Network forensics increasingly require and result in linking heterogeneous data sets pertaining to activities, oftentimes occurring across multiple social and business environment, and correlating digital traces contained within and among various data sources, such as Web pages, computer logs, Internet newsgroups, online chat rooms [6].

This paper provides a discussion of major issues affecting the deployment of Internet forensics methods, aiming to outline the field, to identify the major technical and legal challenges and provide suggestions for forensics practices that take into account the need to protect security as well as individual privacy. The paper is structured as follows. The next section discusses the concept of cyber crime and the sources of digital evidence. Section three identifies major technical challenges and obstacles, while section four discusses major legal aspects of Internet Forensics. Finally, the last section includes our overall conclusions and indications for further research.

2. Cyber crime

An electronic crime is defined as an illegal act that is carried out using a computer or electronic media. A cyber crime is an electronic crime that is carried out using the Internet, or a crime whose “crime scene” is the Internet. Cyber crimes are not necessarily new crimes; many cases involve rather classic types of crimes where criminals exploit computing power and accessibility to information. However, it seems that the anonymity provided through the Internet encourages crimes that involve the use of computer systems, since criminals believe that there is a small chance of being prosecuted, let alone being caught for their actions. Criminals are also increasingly taking advantage of hacker techniques and malicious code. Cyber crimes can be automated (such as spam, worms, Trojans, viruses, spyware) or specifically targeted such as theft of proprietary information or intellectual property, sabotage

etc. It is estimated that computer fraud is merely committed by relatively unsophisticated individuals [9], while Internet fraud, on the other hand, is believed to be the deed of highly sophisticated individuals [7].

2.1 Collecting digital evidence

With increased Internet use, considerable documentary evidence can be found with regard to any user. When investigating cyber crimes, evidence can be collected from multiple sources. Typically, ISPs maintain extensive logs with regard to user activity, indicating access points, IP addresses used, connection start and end time etc. These logs are usually kept for a few days; however lately the duration for which logs are maintained is prolonged to a week or even ten days, since the cost of storage media is declining. Most ISP's can also make router data available for the purposes of cyber crimes investigation. In the near future it is expected that ISPs will be asked by law enforcement to provide even more information with regard to Internet users. There already exist forensics schemes, which demand real time access to communication data and to tap specific sessions. Other sources of evidence include system logs (mailers, DHCP servers, firewalls), and even cash files.

It should be noted, however, that it is not only crime related evidence that can be retried by Internet forensics procedures. Information about a person's lifestyle, preferences, acquaintances and relations to other individuals can be collected, raising privacy implications concerns, which are further elaborated in the following of this paper.

3. Technical challenges for Internet Forensics

The increase in cyber crimes has resulted in an increasing need to develop Internet forensics techniques and tools to discover attacks. It has also been argued that Internet Forensics investigators should posses the same skill sets as their opponents, meaning hackers [7]. Besides the necessity for investigators to develop and apply suitable tools and procedures for performing digital investigations, there is also a wide range of issues that need to be tackled, which spans technical, social, procedural and legal aspects [10].

Procedural problems arise from the lack of standardization, as well as the lack of theoretical framework for the field of digital forensics. Using ad-hoc methods and tools for the elicitation of digital evidence can limit the reliability and credibility of the evidence, especially in a crime prosecution process where both the evidence and the processes used for collecting it can be disputed. To address this difficulty, practitioners' bodies and organizations have recently started the endeavor to develop suggestions to standardize forensics processes. For Internet forensics, however, standardization is even more difficult.

Technical challenges include the diversity and heterogeneity of the infrastructure (different platforms and different applications) and the physical barriers which prohibit investigators for accessing the sources of evidence, e.g. routing tables in routers. Tracking evidence through the Internet poses also difficulties in conducting date and timeline analyses on collected data. Furthermore, for most forensics models to be applied, it must be assumed that an attack has taken place so as to apply certain procedures in an attempt to discover and collect relevant traces. Thus, the type and characteristics of the attack have to be known and understood when the forensic investigation is launched. However, threats originating from the Internet grow exponentially; a McAfee report states that malicious threats included in their database have

doubled within less than two years. In year 2004, McAfee added 27,340 new threats to its database, but in 2005 that number more than doubled to 56,880 new threats [11].

Moreover, forensics procedures typically require that a vast amount of data is collected, stored and analyzed. This poses high requirements for the systems used, especially in the case of cyber crimes. Another challenge has to do with the fact that often investigators, presented with a great amount of data, find difficulties to choose the more significant or relevant pieces among them. To facilitate the analysis, data mining techniques are often employed. Also, when investigating cyber crimes, data need to be collected while computers, servers (e.g. routers, etc) are still running. In these cases, conducting a "live" discovery process entails even greater technical challenges.

Besides challenges which are inherent in the Internet Forensics process, cyber criminals often employ a wide range of techniques to thwart investigation and prosecution. These include actions to create hindrances to prevent an investigation, to eliminate or obfuscate evidence, or even to introduce doubt about the collected evidence in the prosecution process.

Traditional anti-forensic techniques include changing file extensions, using swap space, disk wiping software, physical destruction of media, anonymizing techniques, use of free anonymous internet access and free anonymous internet and email accounts, using other persons' access, cryptography and steganography. The use of encryption, especially, poses significant barriers to the forensics processes. Many countries pose restrictions to the use or export of strong cryptography; however, even weakened cryptography presents an obstacle to evidence retrieval. It should be noted, though, that use of encryption is at the same time identified as on of the most effective e-crime fighting technologies [3].

Anonymous online data storage is another obstacle for Internet forensics. Many online providers offer storage services, which can be exploited by criminals using stolen credit card data. Offenders also often chose to conduct criminal activities from countries where no computer crime or cyber crime laws apply. For instance, no legal action could be taken against the suspected author of the ILOVEYOU virus, whose rapid spread caused severe problems within the year 2000, as the suspect was located to reside in Philippines, which, at that time, had no legislation against computer crime.

Finally, individuals conducting offensive actions through the Internet often use compromised computers in different countries to thwart investigation, taking advantage of the different or conflicting legislation and legal codes and procedures. There are currently over 150 countries registered on the Internet; not all of them have jurisdiction with regard to hacking or cyber fraud.

4. Legal challenges for Internet forensics

Legal issues pertaining to investigating and prosecuting cyber crimes include differences in jurisdictions, handling of digital evidence, conditions that should apply for lawful investigations and the protection of individual privacy.

5.1 Digital data as evidence

Cyber crime and conventional crime differ significantly both in commission and in prosecution. It is especially difficult to track and investigate a cyber crime and prosecute the criminals within current legal systems, which have been tailored for the traditional types of crime. There are no fingerprints and/or not even any physical presence: cyber

crime does not require a physical presence from the perpetrator. Moreover, perpetrators can choose a – from legal perspective - “favourable”- place.[12].

The process of a digital forensic investigation is subject to considerable scrutiny of both the *integrity of the evidence*, meant as the “information by which facts tend to be proved [13], and *the integrity of the investigation process* [14].Electronic evidence is defined as “any information obtained from an electronic device or digital medium which serves to convince the truth of a deed” [15]. E-evidence is not intrinsically different from other types of evidence; rather the problems are raised from the fragility and the transience of many forms of computer evidence [16].

A fundamental question that needs to be considered, is whether and to what extent, digital traces and computer data can be treated as documentary evidence. Law enforcement is an information-intensive process, in which law enforcement agencies have to collect and to interpret large data sets. Digital forensic investigations are commonly used as a post-event response to a serious criminal incident. The effectiveness of the law enforcement and prosecution relies on the information gathered and reported. The evidences have to be considered and evaluated, but in most cyber crimes there is no physical evidence at place [12]. Data, which can eventually be classed as evidence, are volatile: they can be easily deleted or disappear [17]. Cyber evidence is undoubtly easier to destroy or to alter by the perpetrator without obvious traces [12, 13]. The digital evidence is fragile, as it can be also easily destroyed by inexperienced access and handling.

Network derived evidence must have all the attributes of conventional evidence. Primarily it has to be *admissible*, i.e. to comply with the legal principles and requirements in the judicial criminal procedure. E-evidence must be “irrefutable authentic”, i.e. it must be possible to positively tie evidentiary material to the incident [1] and collected in accordance with formal requirements to establish its reliability [13, 17]. Information security practices can be used to safeguard the quality and reliability of collected information [4].

Establishing the integrity and authenticity of material in court, requires standard techniques and methods for the collection, preservation and presentation of stored material. As the use and handling of data and information collected by detection tools are closely related to standardization, the European Commission emphasizes the need to create technical standards to ensure that the data collected complies with the requirements of law for the use of such data in court proceedings [18]. It has also been proposed that “the technical means and methods should be subjected to independent testing and certification” [17].

Specific rules of criminal procedure address law enforcement access to sources of evidence. The respective law regulates the means by which facts may be proved in courts. However cyberspace raises a range of issues in relation to the applicability of these rules. The admissibility of evidence from computer records in courts depends to a great extent on the underlying fundamental principles of evidence in the respective country. The admissibility of digital evidence is essential since in most countries coercive powers are only applicable to material that would be admissible in evidence at a trial [19]. There is a legal debate regarding the acceptance of digital evidence as documentary evidence. Council of Europe’s Recommendation No R(95) 13 concerning problems of criminal procedural law connected with information technology was one of the first efforts at

making a direct attempt to establish equality for digital evidence with other forms of documentary evidence.

In Europe, continental legal systems operate according to the principle of free introduction and free evaluation of evidence and provide that all means of evidence, irrespectively of the form they assume, can be admitted in legal proceedings. Legal systems based on these principles in general do not hesitate to introduce computer records as evidence [13, 15, 19]. In the past, the use of computer-generated evidence in court has posed legal difficulties only in common law countries, and especially in Australia, Canada, the United Kingdom and the United States of America: these countries are, to a greater extent, characterized by an oral and adversarial procedure. Knowledge from secondary sources, such as other persons, books, or records, is regarded as “hearsay evidence”, and is, in principle, inadmissible but there are several exceptions to the hearsay evidence rule. However, digital evidence seems to become widely admissible now. Furthermore, parties to the Convention on Cybercrime should make it explicit in their own laws that information contained in digital or electronic form can be used as evidence before a court, regardless of the nature of the criminal offence [17].

5.2. Search for evidence and jurisdiction

In a traditional environment, a search involves gathering evidence that has been recorded or registered in the past in tangible form. In the off-line search the precondition for obtaining legal authority to undertake a search is the existence of grounds to believe that such data exists in a particular location and will afford evidence of a specific criminal offence [4]. One aspect of the use of search and seizure warrants in a cyberspace environment concerns the geographical scope of the warrant issued by a judge or a court authorizing access to digital data [5]. Digital forensic autopsies are no longer performed on single machines with small data storage capacities. Rather, the scope for potential evidence has expanded to networks of interconnected computers [20].

The Cybercrime Convention has taken into account the cases, that a lawfully authorized search in a single site should potentially be extended to interconnected systems located anywhere within the jurisdiction of the investigation authority. The Convention requires (Art. 19 § 2) the signatories states to adopt legislative and other measures as may be necessary to ensure that where its investigating authorities search (or similarly access) a specific computer system or part of it and have grounds to believe that the data sought is stored in another computer system and such data is lawfully accessible from or available to the initial system, they shall be able to expeditiously extend the search or similar accessing to the other system [1].

Often, the data under search are stored in equipment located in other state/jurisdictions. In 2000, the FBI accessed computers in Russia via the Internet, using surreptitiously obtained passwords to download data from computers operated by the accused hackers Vasiliy Gorschkov and Alexey Ivanov, already under arrest in the US [5]. This case illustrates the important issues of sovereignty and territoriality that may occur, as activities like the access to data stored in another jurisdiction or transnational “police patrols” on the Internet [19] infringe the sovereignty right of the involved states. Jurisdictional issues present some of the greatest challenges to combating cyber crime.

Network boundaries intersect and transcend national borders [21] However, while Internet is borderless the investigation and prosecution of electronic crime is strictly

related to territorial sovereignty and territorially defined jurisdiction. Jurisdiction over activities on the Internet has become “one of the main battlegrounds for the struggle to establish the rule of law in the Information Society” [22].

The international community has developed longstanding methods for obtaining and providing legal assistance. These processes, however, are time consuming and often contain limitations as to what type of assistance can be obtained. The issue of when an investigative authority is permitted to unilaterally access data stored in another state, without seeking mutual assistance, was a question that the drafters of the Convention on Cybercrime discussed at length [1]. Member States under the Cybercrime Convention accepted the trans-border access to stored computer data in two situations: a) where the data being accessed is publicly available, and b) where the investigative authority has accessed or received data located outside of its territory through a computer system in its jurisdiction, and it has obtained the lawful and voluntary consent of the person, who has lawful authority to disclose the data to the investigation au through that system (Art. 32).

Who is a “person” that is “lawfully authorized” to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned [1]. It has been argued that the extraterritorial extension of criminal procedure jurisdiction may strengthen sovereignty in a transnational cyberspace environment [5]. However, it is undeniable that this provision represents a compromise solution, which, while eroding the traditionally perceived sovereign rights of a state, tries to face the threat of cyber crime.

5.3 Data mining as forensics tool

Investigating authorities are confronted with the need to extract relevant information from huge numbers of documents. Modern software tools for data and text mining can face the challenge of the constant increase in the volume of documentation and information the authorities have to process [18]. Data mining technology includes massive data collection, data warehouses, statistical analysis and deductive learning techniques and uses vast amounts of data to extract information from data, to generate hypotheses and discover general patterns [23]. Data mining agents use information technology to find trends and patterns in a heap of information that originates from several sources [4].

The computerization of data and the possibility of carrying out full-text searches create an unlimited number of ways of querying and sorting information. Through computerization and data mining it is much easier to search data, initially not related to each other, to combine them and to bring about new information [24]. Through combination of publicly available data from different sources a profile of the situation or behaviour of individuals can be obtained. In forensics, user agents can be exploited to reveal patterns of behaviour in investigating criminal acts [4, 25]. Like the first account of profiling, the Malleus Maleficarum (1400s), which came to serve as an outline for recognizing witches, our day’s profiling is “overly inclusive and may lead to suspicions against innocent people”[12].

Data and text mining tools increase the risk of collection of data for secondary and often improper purposes [24, 26]. It is noteworthy that data mining techniques are fuelled by the increasing public availability of data and the growing integration of public, Internet-based data with existing private data sets. Programs like the “Total Information Awareness” (TIA) in the US, which sought to use data mining to identify terrorists, are

premised on a tightly interlinked relationship between government and private-sector databases, including, according to the TIA Website, “financial, medical, travel, transportation, housing and communication” [27] .

In this context, data mining may result in mass aggregation of information not only for perpetrators but also for an indefinitely large number of individuals. Data mining activities require, according to data protection commissioners, extra safeguards for the use of these data and the monitoring of the use of these operations. The use of data and text mining tools should be grounded on a specific and appropriate legal basis [25, 26].

5.4. Forensics and their impact in privacy

The use of forensics methods may itself constitute an intrusion of citizen’s fundamental right to privacy [18]. Therefore, the lawfulness and, consequently, the admissibility of electronic evidence in court depend upon the respect of legal constraints and guarantees, laid down in legislation pertaining to informational and communicational privacy. Material and procedural rules have to ensure that collection and further processing of electronic evidence complies with the provisions guaranteeing data protection and communication secrecy [15]. Article 8 of the European Convention and Article 7 of the Charter of Fundamental Rights in the European Union govern the protection of individual privacy at the EU level. In parallel, data protection in the EU is governed by Directive 95/46/EC, by Directive 2002/58 and by Article 8 of the Charter of Fundamental Rights in the European Union. The legislators have to specify the procedures to be procedures to be followed and the conditions to be fulfilled in order to investigate a cyber crime incident in accordance with necessity and proportionality requirements. Proportionality, which is a key principle in European law, requires further an assessment of the necessity of the measure and its suitability to achieve its aims. The objective pursued must be balanced against the seriousness if the interference, which is to be judged taking into account inter alia the number and nature of persons affected and the intensiveness of the negative effects.

Most European countries regulate the legality of investigating activities in general or sectoral data protection laws. However, the relevant legal framework varies considerably, especially in comparison to the common law countries: the differences concern not only the substantive law requirements but also the constitutional background, the legal context as well as the legislative technique of the relevant provisions [19]. In US the critical constitutional framework for informational and communicational privacy consists of the Fourth Amendment and its interpretation by the courts, mainly the U.S. Supreme Court. The Fourth Amendment affirms the right of the people to be secure in their persons, homes, papers and effects, against unreasonable searches and seizure [28, 29]. In general, the use of forensics methods in the course of a criminal investigation is usually subject to relatively strict procedural controls and guarantees, such as judicial warrant. [5, 30].

6. Conclusions

This paper elaborates on the technical and legal aspects of Internet forensics, sketching the agenda for future research. It identifies and elaborates on the technical and legal critical issues that need to be addressed. Cyber crime presents two main challenges: a) technical challenges, caused by the rapid changes in technology and the technical shortcomings that impair finding and prosecuting cybercriminals, and b) legal challenges caused by the difficulty (if not

inability) of legal frameworks around the globe to keep pace with the changing technological environment. Digital forensics, if compliant with the fundamental rights, can serve to bridge this gap.

This paper argues that the starting point should be that the rule of law and constitutional values must drive technical capabilities [22]. The General Assembly of the UN in its Resolution "Combating the criminal misuse of information technologies" notes that the "fight against the criminal misuse of information technologies requires the development of solutions taking into account the protection of individual freedoms and privacy" [31]. Being more specific, the European Commission stresses that the "design, manufacture and use of detection technologies and associated technologies, must fully comply with Fundamental Rights as provided for in the EU Charter of Fundamental Rights and the European Convention on Human Rights" [18].

7. References

[1] Council of Europe (CoE), "Explanatory Report to the Convention on Cybercrime" (ETS 185), 2001. Available at: http://www.coe.int

[2] Post, D., Text presented at the Symposium "The Internet and the Law: a Global Conversation", Ottawa 1-2 October 2004. Available at http://web5.uottawa.ca/techlaw/

[3]E-crime Watch Survey, CSO magazine, U.S. Secret Service, CERT Coordination Center, Microsoft Corp, 2006. Available at www.cert.org/archive/pdf/ecrimesurvey06.pdf

[4] Mitrakas, A., Zaitch, D., "Law, Cybercrime and digital forensics: Trailing Digital Suspects", in Kanelis P., Kiountouzis, E., Kolokotronis, N., Drakoulis, M.(Eds), Digital Crime and Forensic Science in Cyberspace, London 2006, pp. 267-290.

[5] Walden, I., "Crime and Security in Cyberspace", Cambridge Review of International Affairs, Vol. 18, Number 1 2005, pp. 51-68.

[6] Kenneally, E.K., "The Internet is the Computer: the role of forensics in bridging the digital and physical divide", Digital Investigation, Vol. 2, Issue 1, 2005, pp. 41-44.

[7] Berghel H., "The Discipline of Internet Forensics", Digital Village, Communications of the ACM, August 2003/Vol. 46, No. 8, pp. 15-20.

[8] U.S. Department of Justice (DOJ), "Electronic Crime Scene Investigation: A Guide for first responders", United States Department of Justice, Washington DC, 2001.

[9] Disley V.N., "Nailing the Intruder", SANS Institute, 2001. Available at http://www.sans.org

[10] Digital Forensic Research Workshop, A Road Map for Digital Forensics Research 2001, Digital Forensics Research Workshop, 6 November 2001. Available at http://www.dfrws.org/dfrws-rm-final.pdf

[11] "Internet threats double in two years" Available at http://www.computing.co.uk

[12] Nykodym, N., Taylor, R., Vilela, J., "Criminal Profiling and Insider cyber crime", Digital Investigation, Vol. 2 Issue 4, 2005, pp. 261-267.

[13] Leroux, O., "Legal Admissibility of Electronic Evidence", International Review of Law Computers and Technology, Vol. 18, No 2, 2004, pp. 193-220.

[14] Rowlingson, R., "A ten Step Process for Forensic Readiness", International Journal of Digital Evidence, Winter 2004, Volume 2, Issue 3. Available at: http://www.utica.edu/academic/institutes/ecii/ijde/

[15] CYBEX, "The admissibility of electronic evidence in court – Fighting against high-tech crime – Study", 2006, available at : www.cybex.es

[16] Sommer, P., "Digital Footprints: Assessing Computer Evidence", Criminal Law Review - Special Edition 1998, pp. 61-78.

[17] RAND Europe, "Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries – Study for the European Commission", Directorate-General Information Society, 2002

[18] Commission of the European Communities, "Green Paper on detection technologies in the work of Law Enforcement", Customs and other Security Authorities - COM, 2006, 474 (final).

[19] Sieber, U., "Legal Aspects of Computer-Related Crime in the Information Society", COMPRIME Study, 1998.

[20] Kenneally, E.K., Brown, C.L.T., “Risk sensitive digital evidence collection”, Digital Investigation, Vol. 2, Issue 2, 2005, pp. 101-119.

[21] Johnson, D.R., Post, D., “Law and Borders – The Rise of Law in Cyberspace”, 48 Stanford Law Review 1367 1996, available at: http://www.temple.edu/lawschool/dpost/writings.html

[22] Reidenberg, J.R., “Technology and Internet Jurisdiction”, 153 University of Pennsylvania Law Review, 2005, pp. 1951- 1974.

[23] Sumathi, S., Sivanandam, S.N., “Major and Privacy Issues in Data Mining and Knowledge Discovery”, Studies of Computational Intelligence 29, 2006, pp. 271-291.

[24] Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung – Data Warehouse, Data Mining und Datenschutz, 59. Konferenz (Hannover, 14-15/03/2000), available at: http://www.bfdi.bund.de/

[25] Data Protection Working Party (DPWP), Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities (WP 129), available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

[26] Conference of the European Data Protection Authorities , Common Position of the European Data Protection Authorities on the use of the concept of availability in law enforcement, Spring Conference, Cyprus, 11.05.2007. Available at: http://www.bfdi.bund.de/

[27] Steinhardt, B., “The Surveillance-Industrial Complex: How the American Government is Conscripting Businesses and Individuals in the Construction of a Surveillance Society”, 27 International Conference on Privacy and Personal Data Protection, September 2005.

[28] Kerr, O.S., “Searches and Seizures in a Digital World”, 119 Harvard Law Review, 2005, pp. 531- 586.

[29] Salgado, R.P., “Fourth Amendment and the Power of the Hash”, 119 Harvard Law Review, 2005, available at: http://www.harvardlawreview.org/forum/issues/119/dec05/salgado.pdf

[30] Jekot, W., “Computer Forensics: Search Strategies and the Particularity Requirement” 12 University of Pittsburgh Journal of Technology Law and Policy, Spring 2007, available at: http://tlp.law.pitt.edu/articles/Vol_12_Jekot.pdf

[31] UN Resolution, “Combating the criminal misuse of information technologies” 2000.