Digital forensics appliance in corporate ecosystem considering limitations in the EU legal framework

Vinko Rajič univ. bacc. ing. traff., Melita Milenković, LL. M. and Goran Vojković, Ph.D.
Faculty of Transport and Traffic Science, Department of Transport Planning, Chair of Transport Law and Economics
Zagreb, Croatia
gvojkovic@fpz.hr,
mmilenkovic@fpz.hr,
rajicvinko@gmail.com

***Abstract* - This paper presents appliance of digital forensics in a corporate ecosystem i.e. appliance of digital forensics investigation in a corporate or internal investigation as a result of an incident caused by internal or external threat while considering necessity of coexisting corporate policies and legal regulations. Conducting digital forensic investigation refers to the process of acquiring and processing data for the purpose of investigation which are commonly performed by the corporate investigation team, i.e. by the third-party investigators. Today's organizations need to be forensically ready to minimize a response time necessary for timely reaction, both in the cases of internal or external digital forensics incidents. The goal of this paper is to provide oversights of various companies as well as deficiencies of EU legal system.**

Key words* - *digital forensics, forensic investigation, data protection, data breaches, corporate ecosystem, GDPR

I. Introduction

Main goal of this paper is to allude on the insufficiency of EU legal framework when investigation is conducted in corporate ecosystem. After defining digital forensics and reviewing its existing impact on corporate ecosystem, recommendation for legal framework will be proposed. In the procedure of collecting, processing, interpreting and presenting digital evidence, and information about how the evidence was handled it is more important than the content of the evidence itself. This is due to a vaguely defined and/or non-transparent legal framework, in the context of the processing of an individual's data. This incompleteness of legal regulation limits the ability of forensic scientist to collect and process possible evidence, which can directly affect the outcome of the investigation.

Before laying the foundations of modern forensics, it was difficult to pinpoint the offender of any act. The reason for this was that the trials often relied on forced confessions and on the witnesses' testimony, and it wasn't uncommon that the actual offender was left unpunished. [1] For this reason, the need for examination of the very circumstances of a crime has occurred, instead of drawing conclusions based on incomplete statements of a witnesses. Forensic science has begun to be applied in order to enhance the validity of the conclusion reached on the basis of the investigation carried out by the competent authorities.

First instances of forensics development were seen on the local level when authorities could identify the prime suspect just on the M.O.[1] However, the first significant step in identification of an offender was introduction of fingerprinting method. Afterwards, forensics as a science has started to couple a variety of methods for identification of evidence at the scene of the crime such as hair, soil, stains, etc. [2]

Forensics science involves the application of scientific methods and processes, such as biology, chemistry, physics, computer science, etc.; in accordance with the law for the purpose of conducting a criminal investigation [3]. It is a set of carefully coordinated activities and processes by which evidence is acquired, analysed and interpreted. The moment when object started to be considered an evidence, it becomes a mute witness to the crime [4]. Forensics is a process of questioning a mute witness performed by the authorized personnel. Forensics science has had a crucial role in the legal framework by providing scientifically based information through analysis of physical evidence since the legal and professional aspect of forensics are interrelated, i.e. best evidence is useless if it is acquired illegally [5].

Forensic science has a various application on a vast field such as geology, accounting, botany, serology, etc. However, those fields started from the more common area of forensics: pathology, anthropology, odontology, entomology, behavioural forensic science and computer or digital forensics. [6] Main focus of this paper is on digital forensics which will be explained more in depth in the next chapter.

II. The Fields of Appliance of Digital Forensics

Although widespread use of computers began in the second half of the 20th century, digital forensics did not have any significant development until the end of the 20th century. The reason is that computers had been operating

[1] A modus operandi – someones habit of working in the context of criminal investigations. Term is used when addressing the methods applied by the criminals.

in the industrial production and were owned by corporations, institutes, government organizations, etc. Although computers had limited functionality at the time, they performed data processing that allowed organizations to perform their core business functions. In order to avoid data manipulation, information security and methods that could trace the perpetrator began to be considered [7]. While taking into consideration that digital forensics is relatively a new branch of forensics science, it can be said that the digital forensics went through three stages of development which can be seen on the Figure 1. Those are:

- The Ad Hoc Phase
- The Structured Phase
- The Enterprise Phase [8]; as seen on the Figure 1.

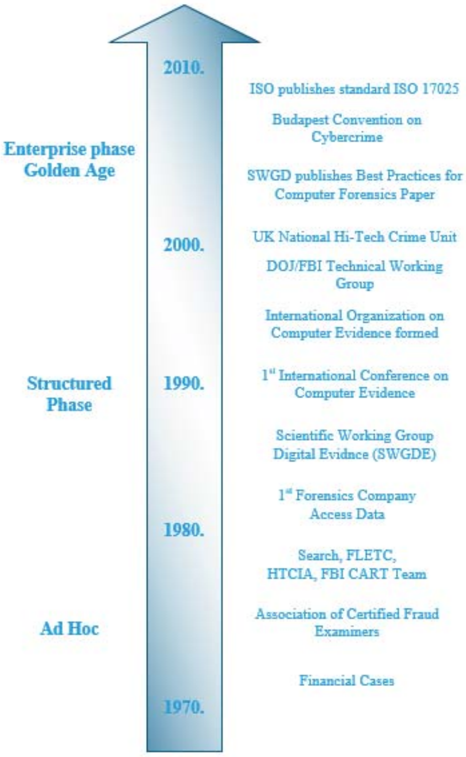
2010.
ISO publishes standard ISO 17025
Budapest Convention on Cybercrime
Enterprise phase Golden Age
SWGD publishes Best Practices for Computer Forensics Paper
2000.
UK National Hi-Tech Crime Unit
DOJ/FBI Technical Working Group
International Organization on Computer Evidence formed
Structured Phase
1990.
1st International Conference on Computer Evidence
Scientific Working Group Digital Evidnce (SWGDE)
1st Forensics Company Access Data
1980.
Search, FLETC, HTCIA, FBI CART Team
Ad Hoc
Association of Certified Fraud Examiners
Financial Cases
1970.

Figure 1 Digital Forensics Timeline [11]

Digital forensics, as a branch of forensics science involves identifying, acquiring, processing and interpretation of digital evidence that can be stored on various types of memories in different formats. Main purpose of digital forensics is extraction of data from device, its interpretation, and presenting the evidence to the authorized institutions in an intelligible form [9]. Digital forensics can be classified by different criteria, although the most common classification is by its usage on different aspects of information-communication technology:

- Computer forensics
- Network forensics
- Mobile device forensics
- Database forensics
- Other (cloud, e-mail, IoT forensics, etc.) [10]

Every mentioned sub-branch of forensics encounters the same challenges regarding the integrity of digital evidence. There are instances where data extraction cannot be done without alteration or contamination which renders evidence useless. All of the aforementioned points to standardization of methods and tools as mandatory in a manner acceptable by the law. Meaning that data is collected, handled, and stored using tools and methods that are verified to be in compliance with the law. This is also known as a Forensic Soundness [12]. From the moment when data begins to be considered as an evidence in forensic investigation, standardized measures should be considered.

Furthermore, careful handling regarding the evidence must be taken into account due to volatile nature of digital evidence. This means that the evidence must be documented from the moment when identified, acquired, processed, interpreted and presented in the court, i.e. Chain of custody[2]. Moreover, clear and structured process step-by-step can help investigator to determine if there was any unallowed action that can compromise the integrity of evidence. [13]

While digital forensics can have wide application regarding its variety of tools and methods, forensics should be performed using the forensic process shown on the Figure 2. It consists of four steps where each must handle the evidence without altering or contaminating them. These are: Collection, Examination, Analysis and Reporting, [14]. In order not to deviate from the procedures, there is a need to define the methodologies that can be followed when managing the evidence. Carefully considered and defined methodology can help with proper handling regarding the evidence.

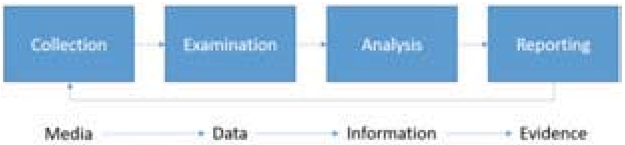

Figure 2 Forensic Process [14]

The data is transformed into information when analysis is being conducted and finally information becomes evidence when it is reported since a decision is made based on the evidence. [14]

III. Digital Forensics in Corporate Ecosystem

A. *Digital Forensics Process*

Purpose of forensic process is to acquire unbiased evidence of criminal activity and as such, it can give answers to the following:

[2] Chain of custody refers to as chain of possession of evidence from the moment the evidence is collected, examined, analyzed and reported.

- Association of criminal activities with the individual
- Assessing alibis and statements
- Determining intent
- Credibility of sources
- Document Authentication
- Data gathering and observation [12]

Digital forensics has a wide application in different areas of legal framework:

- Criminal investigation - Forensics methods and tools that are used in data extraction process depends on which type of device or media the data is being extracted from. Main purpose of digital evidence is to support or rebut a thesis or argument on which court decision is based on.
- Civil Litigation - In civil litigation, both parties have the right to review the evidence that will be used against them before the trial itself. The most common cases of civil litigation are divorce or child custody.
- Public sector security and operation - Security and public sector operations include stopping hacking attacks, investigating them, intelligence, and counterintelligence.
- Corporate investigation - violations can be committed in various ways, such as: disclosing sensitive information to competitors, intentional or unintentional sabotage, etc. In such cases, digital forensics is used to determine where the omission occurred., which may not necessarily be illegal, but if they contravene with the company policy, sanctions are imposed by the employer. [10]

When discussing digital forensics in a corporate ecosystem, two aspects are considered when it comes to a potential incident:

- Preventive measures as a mean of preventing an incident
- Corrective measures as a mean of repairing exploited weakness

B. Preventive measures as a mean of preventing an incident

Preventive measures are a set of measures and rules designed to protect and secure the information-communication system. This means defining and applying security policies and principles to prevent the intentional or unintentional damage to an organization's assets, financial power, or reputation. Information-communication systems are at risk of every-day exposure to threats which could easily compromise information on which organizations rely their core business function.

For this reason, three basic principles of information security have been defined: confidentiality, integrity, and accessibility [15]. Confidentiality ensures that classified information is available only to authorized personnel. Integrity implies that confidential information is protected against unauthorized changes. Availability ensures that the information is accessible to authorized users [16].

The stated principles of information security are implemented and enforced with security policy. Security policy is a set of rules of conduct when managing information-communication system and it applies to all employees of the organization. It defines acceptable and unacceptable behaviour as well as sanctions, i.e. consequences in case of non-compliance [17] Security policy is based on organizations requirements of the risk management as well as the balanced cost/benefit ratio which implies the question: Is it worthwhile to protect information that is not of great value to the organization? This means assessing whether it pays to invest in protecting information that has a little value to the organization [18].

Concerning organizational security in the EU companies it would be very hard to imagine such a system being operational without adhering to rules of a certain professional certification. Therefore, it has been noted that most appropriate system for standardization of information security practices would be ISO/IEC standard 27001, [19] although ENISA [20] currently works on forming of new cyber standards which will improve existing ISO/IEC 27001 standards. Standardization with detailed risk analysis has proven to be useful in cases of recovery from security incidents and it allows the organization to continue to operate undisturbedly.

Taking politics for granted is very often the reason why organizations find themselves in incident situations. Most common mistakes that are made are:

- Not having a policy
- Not updating the security policy
- Not tracking compliance with the security policy
- Having a “tech only“ policy
- Having a policy that is large and unwieldy [21]

Security policy is a process, not a one-time solution which results in corrective measures to be taken.

C. Corrective measures as a mean of "repairing" exploited weakness

Corrective measures are a set of activities undertaken after an incident has occurred. The purpose of remedial action is to eliminate the weakness that has been exploited in the system and to identify the perpetrator who has exploited the same weakness. The perpetrators may take the form of an external and internal threat. The most common use cases of digital forensics in a corporate ecosystem can be divided into:

- Intellectual property (IP) theft and Internal investigations
- Data recovery

- Damage control [22]

Internal investigations within the organization aim to identify the perpetrator who has violated the organization's policies. Violation of an organization's policy implies intentional or unintentional disregard for the interests of the employer or the employment contract. The most common case is a breach of the privacy statement. (proprietary files associated with a revenue model, customer/customer database or trade secret). Furthermore, digital forensics can also respond in cases of fraud, injury at work or sexual harassment. All digital media and devices used within the organization can be used as potential evidence. [23]

The most common cases of ‘’misconduct‘‘ in organizations are: accounting fraud, asset misappropriation, unauthorized use of organization assets, threats, sexual harassment and other forms of inappropriate behaviour and other violations of policies, misconduct or criminal activity [23]. For an internal investigation to be conducted, it is mandatory that the organization prepares in advance to conduct an effective investigation. To make the internal investigation more effective, it is necessary to: plan and organize, fast acting, thoroughness, honesty, accuracy and precision, confidentiality, and proper documentation. [23]

Data recovery is a process of recovering data from different types of memory that is damaged, inaccessible, lost or erased. The process itself often involves disassembling memory as well as repairing damaged parts. Data recovery does not fall directly under digital forensics but becomes part of it when recovery is done for the purpose of gathering evidence for criminal or internal investigations. This includes instances where there has been a violation of an organization's policy and the return of data is for the purpose of identifying the perpetrator and/or recovering sensitive data. In addition, the difference between a normal data recovery process (such as a memory failure) and data recovery due to an investigation is the documenting process. A recovery forensic scientist is required to follow a rigorous procedure, record, the extraction process and to submit a report. [24]

Damage control is a set of measures or activities undertaken after an incident has occurred. There is a possibility that sooner or later, every organization will be compromised by an internal or external threat. When this happens, organization must remain in "control" of the incident. When incident occurs, the organization must have in place procedures which should be prepared to apply. Damage control means controlling the loss of reputation, profits, and business partners. The methods of damage control depend on the current situation and there is no unique method of damage control. In order to minimize damage, the damage control team must find the right approach to gain "control" of the situation. Damage control is divided into three basic items:

- Communication
- Responsibility, and
- Solution [25]

For damage control to be successful, organization must be direct and up to date in dealing with the incident. This implies taking corrective action, accepting responsibility, and implementing the appropriate solution. When planning and anticipating potential threats, crisis management checklist should be made. The checklist should include: pre-incident planning, security measures, emergency contacts, establishment and implementation of a security policy and creation of a crisis management team. [24]

IV. Existing EU Legal Framework

A. Member States' insufficient regulation in the field of digital forensics

The conduct of digital forensics investigation resulting from the data breach in the company either by the internal or external perpetrator is not regulated by any particular EU Regulation or Directive. Rather, each company should have regulated its own Ordinance on data breach policy and have a dedicated department that handles such cases or it could outsource a company to investigate and resolve each case in the event of an attack. Each company independently decides how to conduct a digital forensics procedure in the event of an attack on the system, whether by internal factors or external ones. There is no legal binding act that fully defines data breaches and/or answers to question, such as: who can request data analysis when a security attack occurs and in which cases digital forensic data processing takes place. As seen in the Table 1, the following legal regulations regulate these issues, although only in the field of free movement of personal data and processing of personal data protection. It should be noted that the ePrivacy Regulation is intended to supplement and refine the GDPR, especially in the field of user metadata and cookie consent obligation, which is neither regulated by the GDPR or any other Regulation, so that the rules of the GDPR are always relevant and are an overall part of the legislative aspects of ePrivacy.

The EU's ePrivacy Regulation was proposed to extend the scope of the current ePrivacy Directive and to harmonize the various online privacy rules that exist in EU Member States.

Table 1 Overview of key regulations/directives and their implication

The EU legal framework	Implications
General Data Protection Regulation (EU) 2016/679	*Processing of personal data and ensuring the free movement of personal data*
ePrivacy Directive 2002/58/EC	
Directive 2000/31/EC	
Directive 98/34/EC	
Regulation 2018/1725	
Directive (EU) 2016/680	

B. Proposal for the new ePrivacy Regulation

On 10 January 2017, a proposal for a new ePrivacy Regulation (hereinafter: ePR) was adopted. The proposed ePR was intended to replace the existing ePrivacy Directive 2002/58 [26]. As well as updating the current ePrivacy framework in the EU. The Commission has qualified the proposal as a *lex specialis*[3] in regard to General Data Protection Regulation 2016/679 (hereinafter: GDPR), which is *lex generalis*[4]. The original aim has been for the proposed ePR to become enforceable on 25 May 2018 (at the same time as GDPR). [27]

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) should particularize and complement GDPR regarding electronic communications data that qualify as personal data. This Regulation on the one hand does not apply to electronic communications services which are not publicly available; which on the other hand represents an issue for the companies in the real sector; the companies that don't have an obligation to the processing of electronic communications data in accordance with the Regulation. Such companies can only be guided by the GDPR and their internal rules of procedure, that is, national laws, assuming that they have been enacted, given that this area is fairly new and still deregulated.

Therefore, Member States should lay down in their national laws specific guidelines for dealing with attacks against electronic communications metadata, as such security attacks result in the loss of a significant amount of classified information. Real-sector companies whose electronic communications services are not publicly available are left to resolve such security attacks themselves without any legal guidance from the state.

Also, it is important to notice that Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereinafter: Directive on electronic commerce) is giving definition of information society, which, according to its recital 17, states: "The definition of information society services already exists in Community law in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services and in Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access; this definition covers any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service, except services in the indicative list in Annex V to Directive 98/34/EC which do not imply data processing and storage are not covered by this definition." The aim of this Directive is to create a legal framework to ensure the free movement of information society services between Member States, and not to harmonize criminal law as such.

C. Analysis of data protection according to the EU legal regulation

Moreover, all matters concerning the processing of personal data not specifically addressed by the proposal are covered by the GDPR. The alignment with the GDPR resulted in the repeal of some provisions, such as the security obligations of Article 4 of the ePrivacy Directive. Unfortunately, the proposal does not include any specific provisions in the field of data retention. It maintains the substance of Article 15 of the ePrivacy Directive and aligns it with specific wording of Article 23 of the GDPR, which provides grounds for Member States to restrict the scope of the rights and obligations in specific articles of the ePrivacy Directive. Therefore, Member States are free to keep or create national data retention frameworks that provide, *inter alia*[5], for targeted retention measures, in so far as such frameworks comply with Union law, taking into account the case-law of the Court of Justice on the interpretation of the ePrivacy Directive and the Charter of Fundamental Rights. [28]

According to the Regulation (EU) 2018/1725 [27] of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data in the preamble (1) states: ''The protection of natural persons in relation to the processing of personal data is a fundamental right.'' Article 8(1) of the Charter of Fundamental Rights of the European Union (the "Charter") and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provides that everyone has the right to the protection of personal data concerning him or her.

This right is also guaranteed under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. GDPR and Directive (EU) 2016/680 of the European Parliament and of the Council were adopted on 27 April 2016. While the Regulation lays down general rules to protect natural persons with regard to the processing of personal data and to ensure the free movement of personal data within the Union, the Directive lays down the specific rules to protect natural persons with regard to the processing of personal data and to ensure the free movement of personal data within the Union in the fields of judicial cooperation in criminal matters and police cooperation.

Also, there is OLAF [29], European anti-fraud office which has a legal basis for conducting a digital forensics operation in internal investigations under the Article 4(2)

[3] *Lex specialis* is a Latin phrase which means ''law governing a specific subject matter'', it comes from the legal maxim ''lex specialis derogat legi generali''. This doctrine relates to the interpretation of laws. It can apply in both domestic and international law contexts

[4] *Lex generalis* refers, literally means, to the ''general law''.

[5] Inter alia is a Latin phrase that means ''among other things''.

of Regulation (EC) 883/2013 empowering OLAF to take a copy of, and obtain extracts from any document or the contents of any data medium held by the institutions, bodies, offices and agencies, and if necessary, assume custody of such documents or data to ensure that there is no danger of their disappearance, [29] and with responsibility for conducting administrative fraud investigations. The Commission has given the Office full independence to exercise its investigative function. Under Decision 1999/352/EC, ECSC, Euratom provides that for the purposes of investigations the Office is to exercise the powers conferred by Union law. [29]

Moreover, European Union Agency for cybersecurity (ENISA) has been working on making Europe cyber space secure. What ENISA advocates is development of the EU Cybersecurity Certification Framework which will make it easier for ICT manufacturers and developers to serve the EU market. A unified Cybersecurity Certification Framework across the EU will reduce the effects that a fragmented market has on the economy. To support the creation of certification schemes under this framework the role of standardisation bodies is key. [31]

V. Conclusion

As mentioned in the paper, the most typical case of corporate use of digital forensics is investigating internal policy violations such as intellectual property (IP) theft, e.g. if an employee leaves the organization and starts working for a competitor - and takes ownership files related to revenue model, customer databases or trade secrets. Digital forensics can also support cases against employees in cases of fraud, wrongful death or personal injury or even sexual harassment. Laptops, social networking applications and mobile phones can provide evidence in the form of conversation history as well as geolocation data. Emerging technologies will continue to shape digital forensics, and experts say it is crucial to keep up with the global trends in technology - such as newer and more secure mobile devices, Internet of Things (IoT) platforms and artificially intelligent systems.

Therefore, all of the mentioned Regulations and Directives make it easier to handle cyber-attack cases, however it can be deduced that none of the above legal acts clearly delineates how to proceed in the event of an attack and/after the attack has occurred, except for OLAF, which Commission has set up for this purpose.

It should also be noted that EU regulation is also desirable from the point of view of criminal prosecution, as cybercrime is mainly linked to more than one country, so that perpetrators are often prosecuted in a completely different environment from the place of the perpetration. Standardization is what makes it easier to prove the nature of the crime.

Therefore, in this paper we propose that services of the mentioned companies (real-sector companies engaged in virtual business and providing services online and for the ones who could easily become victims of cyber-attacks); would be appropriate to fall within the scope of the Directive on electronic commerce, due to the fact that all the services companies perform fall within the definition of the information society and fall within the activities of the information society, according to the Recital 17 of the Directive.

The next necessary step in regulating security risks is certainly adopting an ePrivacy Regulation which should be overregulated in relation to GDPR, and to harmonize standardization, which will regulate current deficiencies and legal omissions in the Member States' legal framework. It still remains unknown if the ePrivacy Regulation will be adopted and accepted, instead there is a possibility of amending ePrivacy Directive within the matters not specified with the scope of GDPR.

VI. References

[1] A. Embar-Seddon, A. D. Pass, "Forensic science", Salem press, 2008

[2] W. G. Eckert (edited), "Introduction to Forensic Sciences, Second edition", CRC Press, 1997

[3] National Institute od Justice, Forensic Sciences https://nij.ojp.gov/topics/forensics (Retrieved 1 of February 2020)

[4] J. E. Girard, Criminalistics: Forensics science, Crime, and Terrorism, 3rd Edition, American University, Department of Chemistry, Washington, DC,

[5] Z. Durdevic, "Admissibility of evidence, judicial review of the actions of the European Public Prosecutor's Office and the protection of fundamental rights", Head of the Department of Criminal Procedural Law, University of Zagreb, http://www.europeanrights.eu/olaf/pdf_eng/4-Admissibility%20of%20evidence-zd.pdf (Retrieved 1 of February 2020)

[6] K. Mirakovits, J. A. Siegel, Forensic science, the basics, Second edition, 2010, CRC Press

[7] M. Pollit, A History of Digital Forensics, 6th IFIP WG 11.9 International Conference on Digital Forensics (DF), Jan 2010, Hong Kong, China. pp.3-15

[8] I. Chartes, M. Smith, G. McKee, The Evolution of Digital Forensics: Civilizing the Cyber Frontier, 2009, http://www.guerilla-ciso.com/wp-content/uploads/2009/01/the-evolution-of-digital-forensics-ian-charters.pdf?fbclid=IwAR0v5iqcnlEhs9Y0UhgzZenhD5hcgpRHMuFt3-vxgh3UpdMVQUgwRsbl9Tk (Retrieved 11 of February 2020)

[9] Interpol, Global guidelines for digital forensics laboratories, 2019.

[10] D. Peraković, Authorized course lectures: Forensic analysis of information and communication system, University of Zagreb, Faculty of Transport and Traffic Sciences, Department of Information and Communitcation Traffic, "Basic of digital evidence" (in Croatian), 2019

[11] Overview of Digital forensics, Cybersecurity Nexus, ISACA, 2015

[12] E. Casey (edited), Handbook of digital forensics and investigation, Published by Elsevier Inc., 2010

[13] D. Peraković, Authorized course lectures: Forensic analysis of information and communication system, University of Zagreb, Faculty of Transport and Traffic Sciences, Department of Information and Communitcation Traffic, "Forensic analysis methodologies for information communitaction system" (in Croatian), 2019

[14] K. Kent, S. Chevalier, T. Grance, H. Dang, Guide to Integrating Forensic Techniques into Incident Response, Recommendations of the National Institute of Standards and Technology, Special Publication 800-86, Gaithersburg, National Institute of Standards and Technology, 2006, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (Retrieved 11 of February 2020)

[15] D. Peraković, Authorized course lectures: Security and protection of the information and communication system, University of Zagreb, Faculty of Transport and Traffic Sciences, Department of Information and Communitcation Traffic, "Information security terminology" (in Croatian), 2017

[16] I. Kokot, "Criminal-law Protection of Computer Systems, Programs and Data" (in Croatian), Zagreb Law Review, e-Journal of Postgraduate Studies of Faculy of Law, University of Zagreb, Faculty of Law of the University in Zagreb, vol. 3, p.p. 301-327, 2014.

[17] Croatian academic and research network, Security policy (in Croatian), CCERT-PUBDOC-2009-05-265 https://www.cert.hr/wp-content/uploads/2009/05/CCERT-PUBDOC-2009-05-265.pdf (Retrieved 1 of February 2020)

[18] M. S. Corpuz, The Enterprise Information Security Policy as a Strategic Business Policy within the Corporate Strategic Plan, Information Security Institute, Queensland University of Technology, Brisbane, Queensland/4000, Australia, 2011. Available: SemanticScholar, https://eprints.qut.edu.au/51493/1/RA717ZB.pdf (Retrieved 1 of February 2020)

[19] S. Aksantijević, E. Tijan, B. Hlača, "Importance of organizational information security in port community systems", MIPRO 2009, 32nd International Convention on information and communication tecnology, electronic and microelectronics, Proceeding, Opatija, pp. 105-110

[20] European Union Agency For Cybersecurity, https://www.enisa.europa.eu/news/enisa-news/standardisation-and-the-eu-cybersecurity-act-1, (Retrieved 7 of July 2020)

[21] A. Chuvakin,Five basic mistakes of security policy, https://www.computerworld.com/article/2537565/five-basic-mistakes-of-security-policy.html, (Retrieved 5 of February 2020)

[22] S. Walden, Three Business Use Cases for Digital Forensic, https://www.delltechnologies.com/en-us/perspectives/three-business-use-cases-for-digital-forensics/, (Retrieved 5 of February 2020)

[23] D. Adu, A. Oyeola, Nigeria: Conducting Internal Investigations In Organisation, http://www.mondaq.com/Nigeria/x/860156/Health+Safety/Conducting+Internal+Investigations+In+Organisation, (Retrieved 7 of February 2020)

[24] P. Lohberg, The Data Recovery Expert Vs The Computer Forensics Specialist, https://www.ontrack.com/uk/blog/pieces-of-interest/what-sets-the-data-recovery-expert-apart-from-the-computer-forensics-expert/, (Retrieved 8 of February 2020)

[25] Damage Control in Crisis Management, https://www.universalclass.com/articles/business/crisis-management/damage-control-in-crisis-management.htm, (Retrieved 9 of February 2020)

[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 , 31/07/2002

[27] Study of proposal for an ePrivacy Regulation, https://www.digitaleurope.org/resources/study-of-proposal-for-an-eprivacy-regulation/, (Retrieved 11 of February 2020)

[28] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10.1.2017 COM(2017) 10 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN, (Retrieved 11 of February 2020)

[29] OLAF – European Anti-fraud Office Digital Forensics Operation Leaflet https://ec.europa.eu/anti-fraud/sites/antifraud/files/digital_forensic_leaflet_en.pdf, (Retrieved 7 of July 2020)

[30] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), Official Journal of the European Union L 295/39

[31] Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), Official Journal L 136 , 31/05/1999