https://doi.org/10.25143/socr.24.2022.3.140-149

Digital Forensics and Criminal Policy: Latvian–Ukrainian perspective

Mg. iur. ***Aelita Zīle***
ORCID: 0000-0002-4378-738X
Rīga Stradiņš University, Latvia
Aelita.Zile@rsu.lv

Dr. iur. ***Andrejs Vilks***
ORCID: 0000-0002-5161-0760
Rīga Stradiņš University, Latvia
Andrejs.Vilks@rsu.lv

Ph. D. ***Anton Polianskyi***
ORCID: 0000-0003-3005-8206
National Scientific Centre "Hon. Prof. M. S. Bokarius, Forensic Science Institute", Kharkiv, Ukraine
anton_polianskyi@ukr.net

Abstract

Digital forensics and criminal policy are undergoing transformational processes related to technological development. In order to speed up the development of relevant knowledge and skills, a training process is intensively planned, which is characterised by a flexible approach to learning information. Learning digital forensics has certain challenges that both practising experts and future experts face. Therefore, in order to promote the development of this knowledge, it is important to offer international experience and knowledge transfer, including using open educational resources. The aforementioned would allow interested parties to gain in-depth knowledge in the field of digital forensics using the approach of different countries both in theory and in practice. The purpose of the article is to outline the role of digital forensics in modern life, as well as to emphasise its connection with the implementation of criminal policy. The article will examine the point of view of both Latvia and Ukraine on the development of digital forensics in interaction with the creation of forensics.

Keywords: digital forensic, open education, science.

Introduction

Scientific and technological progress in countering crime as well as the general digitalisation of all social spheres are closely linked to the development of a new field of forensic knowledge – digital forensics and the use of digital evidence in the process of obtaining proof. An important trend of criminology is the integration of knowledge, offering the latest, innovative developments of science aimed at solving the tasks of combatting crime (Shepitko, 2019).

Digital forensics and criminal policy is a component of science that has been widely used in the development of technological progress around the world. Both in theory and in practice, digital forensics and criminal policy are specific and the scope of their knowledge and skills depends on several factors (Margot, 2017).

Modern society is also called digital society. Essentially, it is a parallel and virtual world, creating new realities and precisely identifiable identities that are not always comprehensible. Digital technologies are gradually beginning to cover ever wider fields and areas of activity. As a result of the influence of objective and subjective factors, public life is moving towards the electronic environment, where our existential future is also possible. The legal field is not an exception either, in which digital legal proceedings and record keeping are successively included, also using electronic evidence. Digital forensics is interesting and promising, where innovative technologies are used to analyse the state of crime, predict its trends and develop proactive measures to prevent it.

Modern criminality increasingly uses modern technologies, including remote digital ones, which significantly expands the income of criminal organisations and makes it difficult to detect relevant crimes. In this context, the creation and improvement of new technological approaches in the detection of criminal offences is particularly effective.

Therefore, 21st century forensics must be methodologically and innovatively different from the crime detection processes of the last century, which are based on new technologies and innovative methodologies. The law enforcement system, following the process of transformation of criminal structures, creates and determines the development of *digital forensics*, which is a sub-branch of legal science regarding finding, taking and using possible evidence, in accordance with the provisions of the Criminal Procedure Law, as well as about the scientific research of objects of a criminal nature, using a new methodology. It can be recognised that the emerging digital forensics is a branch of forensic technique and methodology that deals with the acquisition of possible elements of a criminal nature on digital devices, their identification and the performance of investigative activities (expertise) in connection with cybercrimes. Originally, the term "digital forensics" was used as a synonym for computer forensics. By its very nature, digital forensics is the process of recording, identifying, preserving, analysing and documenting digital evidence, with the aim of adding relevant evidence to criminal cases, or using it in civil or administrative proceedings.

One of the known early cybercriminals is Kevin David Mitnick. In 1979, at the age of 16, K. Mitnick gained unauthorised access to a computer network for the first time. He broke into the DEC computer network and copied their software. DEC spent USD 160,000 on eliminating the consequences. Only in 1988 was he convicted of this crime. The conviction was based on digital evidence that proved K. Mitnick's unauthorised access to the DEC computer system. He was sentenced to 12 months in prison and three years of supervised probation. At the end of his probation, K. Mitnick still committed cybercrimes for which he was wanted. By the time of his arrest in 1995, he had become the most wanted computer criminal in the United States. It must be admitted that the cybercrimes committed by K. Mitnick and others contributed to the development of digital forensics.

Digital forensics is traditionally used in the activities of law enforcement agencies, recording possible criminal offences against users of digital technologies, unauthorised (illegal) intrusion into computer networks, illegal use of a wireless network, unauthorised access to restricted or private databases, development and use of malicious software, hacking of e-mails, theft of electronic identity data or its use, etc. It is traditionally associated with criminal proceedings where evidence is collected. Digital forensics is often part of a larger investigation that spans multiple disciplines. In some cases, the collected data is used as operational information for purposes other than legal proceedings (e.g., to detect, identify or stop other crimes).

Digital forensics in the current conditions, which is related to the socio-political order and the specific development trend of society, significantly overcomes the new boundaries. Forensic and security technologies are broader than the framework of forensic science.

Also worth noting are the main challenges facing digital investigation:

1) the sharp increase in the number of computers and other digital technologies, as well as the widespread and intensive use of internet access;
2) availability of simple hacking tools;
3) a specific process of taking and analysing digital material evidence, which often complicates criminal prosecution;
4) a large amount of disk space in terabytes, which makes this research work difficult;
5) any technological changes require updates or changes in solutions;
6) electronic records are extremely expensive to produce and store;
7) lawyers must have extensive and sufficient computer knowledge;
8) in the investigative process and in the courts, reliable and convincing evidence must be presented;
9) if the tool used for digital forensics does not meet the set standards, then the evidence in court can be rejected by the judge;
10) the lack of technical knowledge of the investigator may not have the desired result;

11) digital investigation has *new specific capabilities*;
12) new technologies provide additional opportunities to gather sensitive information when computer systems or networks are compromised;
13) cybercriminals can be effectively tracked from anywhere in the world;
14) help protect the material resources of digital technology users;
15) enable the obtaining, processing and interpreting of accurate digital evidence that proves the guilt of defendants in court.

1 Digital Forensics Is Used in the Learning Process

Digital forensics is also used in the process of learning forensics. In this process, there are opportunities to perform a virtual inspection of the scene, and the creation of a simulated scene. Modelling virtual situations and creating an appropriate training complex is useful for future investigators, operational officers, and law students.

The interactive training system allows one to simulate virtual forensic landfills, including accident sites, and to create training scene viewing scenarios. Situations can be used to practise qualitative investigative activities using specific forensic techniques (Kummer, Delémont, Voisard, & Weyermann, 2022).

Digital forensics can be used by comparing the nature of the criminal offence, and the means to be used, in order to record the coincidence of the specific crime with violations of an analogous nature in operational mode. Thus, the New York Police Department has developed artificial intelligence crime recognition computer software called *Patternizr*. The software, which is available in the unified intelligence database, allows each of the department's 77 police stations to compare robberies, thefts, murders or attempted murders with hundreds of thousands of crimes recorded in the New York Police Department's information system. So, for example, the software made it possible to detect two thefts, which were carried out in different regions, by identifying the suspect where a drill was used to break into the property. The person responsible was arrested and found guilty of theft as well as violent assault.

Currently, counterfeiting of Covid vaccine and testing certificates is increasing. There is an increase in the number of relevant service offers. So, in the UK, more than 1,200 fake sellers operating around the world have been caught offering fake documents with a negative Covid test result for £ 25. By March 2021, digital forensics researchers identified more than 1,200 respective service providers. Only certain software can be accessed on the respective internet network. Encrypted messages are available on the platforms WhatsApp, Telegram and Jabber.

2 European Union Criminal Law Policy in the Field of Digital Forensics

The European Union's security strategy aims to improve cross-border access to electronic evidence in criminal investigations. Electronic information and evidence is required in approximately 85% of serious crime investigations, while 65% of all requests are sent to service providers based in another jurisdiction. The EU can help law enforcement agencies develop the necessary capabilities to identify, secure and read data needed to investigate crimes and use that data as evidence in court. The Commission will explore measures to improve law enforcement's digital investigative capabilities, identifying how best to use research and the development of new technologies to create new tools for law enforcement, and how training can offer the right skill set for law enforcement and the judiciary.

Due to the intense development of cybercrime, the EC Council has created a certified forensic investigation programme (Council's Certified Hacking Forensic Investigator (CHFI)). EC Council Certified Hacker Forensic Investigator is the only comprehensive ANSI-accredited programme that provides organisation, vendor-neutral training in digital forensics. CHFI provides a rigorous understanding of digital forensics, introducing a detailed and methodological approach to digital forensics and evidence investigation based on the Dark Web, IoT and Cloud Forensics information analysis. The tools and techniques included in this programme focus on an innovative approach to digital investigations for trainees using revolutionary digital forensics technologies. The programme is designed for IT professionals involved in information systems security, computer forensics and incident response. Such a new approach will help strengthen the applied knowledge of digital researchers in digital forensics, cybercrime investigators, forensic analysts, incident responders, and security executives. But in this case there are also challenges related to data protection during the provision of the process (Verma & Ramanathan, 2022).

3 Digital Forensics Is Developing in Ukraine

Digital forensics is developing fairly rapidly in Ukraine. Its development is enhanced by new challenges caused by aggression from the Russian Federation and the need to develop new remote electronic tools for searching, collecting, recording and investigating traces of criminal offences (Kriminalistika ir teismo ekspertologija: mokslas, studijo, 2022).

The development of digital criminology takes place in three main directions:

1) the formation of a separate scientific field in criminology;
2) application of special knowledge when working with digital evidence;
3) conducting forensic examinations (in particular, computer and technical examination) (Shepitko, 2021).

Due to the accelerated forming of digital forensics, different definitions of it have been given by Ukrainian scientists. Mykhailo Dumchykov offers to define "digital forensics" as a new science dedicated to the issues of working with specific information traces, developing modern technologies to optimise the activity of the investigator, expanding the possibilities of interaction of various law enforcement agencies, expert institutions in the investigation of crimes (Dumcikov, 2020). Anna Kolodina and Tetyana Fedorova marked out "digital forensics" as an applied science of solving crimes related to computer information, researching digital evidence, methods of finding, obtaining and securing such evidence (Kolodina & Fedorova, 2022). There is also a more succinct definition of "digital forensics": applied science, the main purpose of which is the analysis and investigation of cybercrimes (Rudyy, Senyk, Rudyy, & Senyk, 2018).

In Ukraine, the understanding of Digital forensics is related to international definitions. Nevertheless, in practice these definitions are broader than the national understanding of digital forensics.

Definitions similar to these are offered by other researchers. Marie-Helen Maras in her book "Computer Forensic: Cybercriminals, Laws, and Evidence" says: "*Digital forensics is a branch of forensic science that focuses on criminal procedure law and evidence as applied to computers and related devices*" (Maras, 2014). According to Ademuyiwa Sanya-Isijola "digital forensics" is the collection, preservation, analysis and presentation of digital evidence extracted from any source of digital evidence that can be used to identify criminal activities or other activity that constitutes a violation" (Sanya-Isijola, 2009). Some scientists divide "computer forensics" from "digital forensics" like Talib M. Jawad Abbas did: "*Computer forensics focuses on extracting evidence from a particular platform (Computer), digital forensic covers extracting evidence from all forms of digital evidence*" (Jawad Abbas, 2013).

Common to all definitions is the application of the provisions of digital forensics in the investigation of offences committed in "cyberspace" and with the use of certain devices.

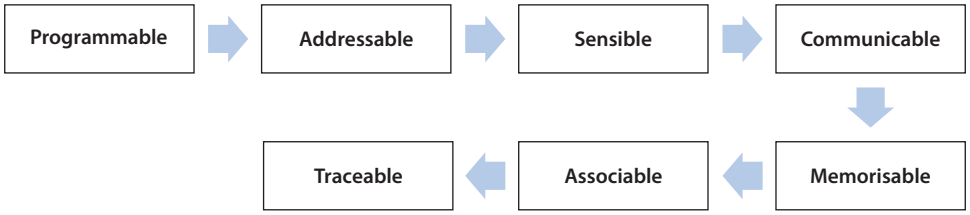
"Cyberspace" is defined in Ukrainian legislation by forensic scientists and lawyers, whose definitions are mainly common and similar in content.

According to the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine" (2017) cyberspace – an environment (virtual space) that provides opportunities for communication and/or the realisation of social relations, resulting from the operation of shared (interconnected) communication systems and the provision of electronic communications using the internet and/or other global data transmission networks. Dmytro Dubov interprets it as an environment created by an organised set of information processes on the basis of information, telecommunication and information-telecommunication systems united by general principles and rules, regardless of the form of ownership (Dubov, 2014).

Cyberspace is an environment, where digital traces of cybercrimes are left. Digital traces – technical devices or devices designed to receive and process information in digital

form using digital technologies (Avdejeva, 2018). As with other types of evidence, digital traces can be characterised by specific properties.

Specific properties of digital traces are as follows. There is another list of digital traces properties given by Jonas Hedman, Nikhil Srinivasan and Rikard Lindgren (Hedman, Srinivasan & Lindgren, 2013). They describe digital traces as:



Here we can see that both lists of marked out properties relate to digital traces as a result of the criminal's influence on digital information by accessing it, and constitute any changes related to the crime.

The subcommittee on standardisation in the field of information technology security of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC 1/SC 27 "IT Security techniques") of the Joint Technical Committee on Information Technology (ISO/IEC JTC 1 "Information technology") made the first attempt to regulate work with digital evidence by publishing the first international standard – ISO/IEC 27037:2012 "Information technology. Security techniques. Guidelines for the identification, collection, acquisition and preservation of digital evidence". Currently, this standard has been harmonised in Ukraine by being translated, and from 1 January 2019, it entered into force as the National Standard of DSTU ISO/IES 27037:2017 (ISO/IES 27037:2012, IDT) "Information technologies. Protection methods. Guidelines for the identification, collection, acquisition and preservation of digital evidence" (Nakaz Ukrainim, 2017; Nacionalnij Standart Ukraini, 2019).

3 Cases of Using Special Software in Ukraine

Computer systems in the field of forensic research include, for example, the "Rikoset" ballistic system. Foreign systems "Balex" used in the examination of firearms, "Kortyk" examination of cold weapons, "Avtoeks" investigation of vehicle collisions with pedestrians and many others (Ivanov, Ivanov, Karasjuk, 2010).

Also, among the programs for automating examinations, the following can be distinguished: "Pocerk", "Oldman", "Left", "AGE. SEX"; for portrait examination – "BARSPortret", "Portret-Poisk"; for examination of video and sound recordings – "PINGUIN – IP", "EXPAD", "Signal Viewer"; for the research of materials, substances and products – "Provoloka", "Spirt", "Farm", for explosion research – programme for

determining the power of an explosive charge "Руїна" (Hahanoskij, 2011). In Ukraine, statements and notifications about offences or events can be sent to the "102" unit using various types of communication, the integration of which with the "Information Portal of the National Police of Ukraine" system is allowed by the National Police of Ukraine, in particular: in the form of short text messages (SMS messages); by e-mail; from mobile applications; other specialised software and technical means (Rudyy, Senyk, 2018).

Conclusions

There is a growing interest in digital forensics, which is indicated both by the lack of experts at the national level, and also by the number of crimes based on offences committed in the digital environment, or offences that require digital skills for their detection. Accordingly, the demand for specialists is also increasing, but there are several obstacles to meeting the demand, related to both national-level policy planning and international regulation, which limit educational opportunities.

It is important to define the scope of digital forensics from a scientific perspective and study its impact on forensic science as a whole.

There is a clear lack of standardisation and structure in both existing educational programmes and those developing new digital forensics programmes. Proper exchange of information between educational and professional institutions, and an expanded educational base with cross-border practice is not established.

The field of digital forensics and its various sub-fields such as mobile devices, cloud, network and vehicle forensics have continuously attracted academic interest and attention.

Improving the quality of digital forensics can be achieved using open educational resources created based on requirements at the national level, but at the same time not limited to national expertise, but involving cross-border partners.

Acknowledgement

This research is funded by the Latvian-Ukrainian Joint Programme of Scientific and Technological Cooperation Project (2021) "Open Educational Resource: Forensic Science", Project No. LV-UA/2021/3

Bibliography

1. Ademuyiwa, S. (2009). Models of Digital Forensic Investigation. www.scribd.com
2. Avdyeyeva, H. K. (2018). Sutnist' cyfrovyx slidiv v kryminalistyci. *Aktual'ni pytannya sudovoyi ekspertyzy ta kryminalistyky: zb. materialiv mizhnar. nauk.-prakt. konfer., prysvyach. 95-richchyu stvorennya Xarkiv*. NDI sud. ekspertyz im. zasl. prof. M. S. Bokariusa. Xarkiv, 2018. S. 90–93. [in Ukrainian]
3. Danial, M., My-Nhi Tran C., & Young, P. (eds). (2013). Janus cyclic peptide–polymer nanotubes. *Nat Commun* 4, 2780. https://doi.org/10.1038/ncomms3780

4. Dubov, D. V. (2014). *Kiberprostir yak novyj vymir heopolitychnoho supernyctva: monohrafiya* / D.V. Dubov. K: NISD, 2014. p. 328. [in Ukrainian]
5. Dumchikov, M. (2020). Didzhytalizaciyi i kryminalistyka: rektrospektyvnyj analiz. *Kryminalistyka i sudova ekspertyza*. Vyp 65, p.100–108. [in Ukrainian]
6. Hahanovskyj, V. G., (2011). Teoriya i praktyka kryminalistychnoyi informatyky: avtoref. dys. K, 28. [in Ukrainian]
7. Hedman, J., Srinivasan, N., & Lindgren, R. (eds). (2013). Digital Traces of Information Systems: Sociomateriality Made Researchable. Proceedings of the 34th International Conference on Information Systems. https://www.researchgate.net/publication/257313647_Digital_traces_of_information_systems_Sociomateriality_made_researchable
8. Informacijni texnolohiyi. Metody zaxystu. (2019). Nastanovy dlya identyfikaciyi, zbyrannya, zdobuttya ta zberezhennya cyfrovyx dokaziv. Na zaminu DSTU ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT); Chynnyj vid. Kyyiv. Nacional'nyj standart Ukrayini. [in Ukrainian]
9. Instrukciya z orhanizaciyi reahuvannya na zayavy ta povidomlennya pro kryminal'ni, administratyvni pravoporushennya abo podiyi ta operatyvnoho informuvannya v orhanax (pidrozdilax) Nacional'noyi policiyi Ukrayiny. 16.02.2018 No. 111. Verxovna Rada Ukrayiny. [in Ukrainian] https://zakon.rada.gov.ua/laws/show/z0371–18
10. Ivanov, V. H., Ivanov, S. M., & Karasyuk, V. V. (eds). (2010). Pravova informaciya ta komp'yuterni texnolohiyi v yurydychnij diyal'nosti: navch. posib. X.: Pravo, 240. [in Ukrainian]
11. Kolodina, A., & Fedorova, T. (eds). (2022). Cyfrova Kryminalistyka: Problemy Teoriyi i Praktyky. *Kyyivs'kyj Chasopys Prava*, (1), 176–180. [in Ukrainian]. https://doi.org/10.32782/klj/2022.1.27
12. Kummer, N., Delémont, O., Voisard, R., & Weyermann, C. (eds). (2022). The potential of digital technologies in problem-based forensic learning activities. *Science and Justice, 62*(6), 740–748. https://doi.org/10.1016/j.scijus.2022.04.005
13. Latysh, K. (2022). Digital Forensics During the War in Ukraine: Possibilities of Using Special Knowledge in the Field of Information Technologies. ISSN 2783–7068, 2022, T. 18. [in Ukrainian] https://repository.mruni.eu/handle/007/18524
14. Maras, M.-H. (2014). Computer Forensic: Cybercriminals, Laws, and Evidence (2-ed, Jones & Bartlet Learning), p. 29.
15. Margot, P. (2017). Traceology, the bedrock of forensic science and its associated semantics. *The Routledge International Handbook of Forensic Intelligence and Criminology* (pp. 30–39). https://doi.org/10.4324/9781315541945. Available: www.scopus.com
16. Nakaz vid 06.12.2017 No. 400 "Pro pryjnyattya nacional'nyx normatyvnyx dokumentiv, harmonizovanyx z yevropejs'kymy ta mizhnarodnymy normatyvnymy dokumentamy, skasuvannya nacional'nyx normatyvnyx dokumentiv, zmin do nacional'nyx normatyvnyx dokumentiv". Verxovna Rada Ukrayiny. [in Ukrainian]. https://zakon.rada.gov.ua/rada/show/v0400774–17
17. Omelian, O. (2020). "Concept and signs of digital traces that form during cybercrimes". https://doi.org/10.33994/kndise.2020.65.45
18. On Basic Principles of Cybersecurity in Ukraine. (2017). *Vidomosti Verxovnoyi Rady* (*VVR*), 2017, 45, 403) [in Ukrainian]. https://zakon.rada.gov.ua/laws/show/2163-19
19. Rudyy, A. T., & Senyk, S. V. (eds). (2018). Organizational and legal, criminalistic and technical aspects of opposition of cybercrime in Ukraine. http://dspace.lvduvs.edu.ua/bitstream/1234567890/1225/1/35.pdf

20. Shepitko, V. (2019). Innovacii v kryminalistyci yak viddzerkalennya rozvytku nauky. In *Innovacijni metody ta cyfrovi texnolohiyi v kryminalistyci, sudovij ekspertyzi ta yurydychnij praktyci: mater. mizhnar. kruhloho stolu*, 147. [in Ukrainian]
21. Shepitko, V., & Shepitko, M. (eds). (2021). Doktryna kryminalistyky ta sudovoyi ekspertyzy: formuvannya, suchasnyj stan i rozvytok v Ukrayini. *Pravo Ukrashy*. 8, 21. [in Ukrainian]
22. Verma, A. K., & Ramanathan, K. (eds). (2022). Data privacy preservation in digital forensics investigation. Paper presented at the *AIP Conference Proceedings, 2519* doi:10.1063/5.0109813. www.scopus.com