Доцент д-р Олга Кошевалиска
olga.gurkova@ugd.edu.mk
Универзитет „Гоце Делчев“ Штип, Правен Факултет

Насловен вонреден професор д-р Лазар Нанев
lazar.nanev@ugd.edu.mk
Универзитет „Гоце Делчев“ Штип, Правен Факултет

Дигиталната форензика и дигиталните докази во кривична постапка

АПСТРАКТ

Сведоци сме дека Интернетот даде нова географска димензија на криминалот, „бришејќи“ ги националните граници на државите. Од овие причини, утврдувањето на местото на извршување на кривичното дело и идентификувањето на сторителите на кривични дела од областа на компјутерскиот криминал е вистински предизвик. Целта на овој труд е да дадеме еден краток преглед на дигиталната форензика со цел правилно да ги дефинираме дигиталните докази, понатаму да ги елаборираме основните принципи кои што се однесуваат на евалуацијата и аквизицијата на овие докази, да ги дефинираме можните извори на дигитални докази и конечно да го илустрираме третманот на овие докази во македонското кривично законодавство за да можеме да дадеме препораки за истото. Конечно, целта на овој труд е да укаже на неопходноста од адекватно и прецизно „осовременување“ на законските одредби на материјалното и процесното кривично законодавство и тоа не е само заради прецизна инкриминација или навремено и полесно откривање на сторителите на кривични дела од областа на компјутерскиот криминал, туку и заради искористување на предностите кои ги дава употребата на компјутерите и на доказите кои што можат да се обезбедат во дигитална форма.

Клучни зборови: дигитални докази, дигитална форензика, дигитална истрага, кривична постапка, компјутерски криминал, Македонско законодавство.

Digital forensics and digital evidence in criminal procedure

ABSTRACT

Internet has given a new geographic dimension of crime by “removing’’ national borders of states. Therefore, the location of the crime scene and the identification of perpetrators or executors of cybercrime became a real challenge. The purpose of this paper is to give a brief overview of digital forensics in order to define digital evidence, to define the possible sources of digital evidence, to elaborate the basic principles relating to the evaluation and acquisition of these evidence so we can finally illustrate the handling of these evidence in the Macedonian

criminal legislation in order to give recommendations for the same. Finally, the purpose of this paper is to point out the necessity of adequate and accurate "modernization" of the statutory provisions of our substantive and procedural criminal law. This isn't only because of the need of precise and accurate incriminations or for timely and easier detection of perpetrators of cybercrimes, it's also for using the advantages provided by the use of computers and the evidence that can be provided in digital form.

Key words: digital evidence, digital forensics, digital investigation, criminal procedure, cybercrime, Macedonian legislative.

Заклучок

Целта на овој труд е преку прикажување на генералните дефиниции за дигиталната форензика и дигиталните докази од компаративните законодавства, идентификување на можните извори на дигитални докази и конечно елаборирање на основните принципи кои што се однесуваат на евалуацијата и аквизицијата на овие докази да го прикажеме третманот на овие докази во македонското кривично законодавство. Согледувајќи ги сите слабости на нашето казнено процесно законодавство кога станува збор за дигиталните докази, на мислење сме дека во Законот за кривична постапка на РМ мора јасно да биде дадена дефиницијата за тоа што преставува дигиталниот доказ како и постапката на собирање, ракување и чување на овие докази и постапката на форензичка аквизиција и анализа која подразбира откривање, обезбедување и изведување на дигиталните докази во доказната постапка. Исто така сметаме дека е неопходно постоењето на конкретни принципи врз основа на кои ќе се врши евалуацијата на дигиталните докази во судската постапка. Конечно, сметаме дека е неминовно да бидат предвидени IOCE стандардите со цел да се осигури можноста за презентирање на дигиталните докази, обезбедени во Македонија, пред суд во странска држава.

Conclusion

The purpose of this paper was to give a brief overview of the general definitions on digital forensics in order to define digital evidence in the comparative jurisdictions, to identify the possible sources of digital evidence and to elaborate the basic principles relating the acquisition and evaluation of these evidence in order to show their treatment in the Macedonian criminal legislation. Because of all the flaws in our criminal procedure law when it comes to digital evidence, we are of the opinion that our Criminal procedure Law must be amendment with definition on what is digital evidence and to give a precise procedure for the collection, handling, storage and presenting these evidences on the evidentiary hearing before court. We

also believe that it is necessary to implement the specific principles that address the evaluation of digital evidence in judicial proceedings. Finally, we believe that it is of a great importance the implementation of the IOCE standards in our criminal procedure law in order to ensure that the digital evidence that had been seized in our country to be admissible before a court in a foreign country.

Користена литература:

A Road Map for Digital Forensic Research, Report from the First Digital Forensic Research Workshop (DFRWS), August 7-8, 2001, Utica, New York;

Ali Obaid Sultan Alkaabi (2010): Combating Computer Crime: an international prespective, Doctoral Thesis on Information Security Institute, Faculty of Science and Technology, Queensland University of Technology;

Angus M. Marshall (2008): Digital Forensics Digital Evidence in Criminal Investigation, A John Wiley & Sons, стр.1;

Bradley Schatz (2007): Digital Evidence: Representation & assurance, Information Security Institute, faculty of Information Technologies, Queensland University of Technologies, Austria, стр.3;

Chang-Tsun Li (ed.) (2013): Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security, Idea Group Inc (IGI), стр.240;

Colin Evans, Criminal justice: Evidence, 2010 by Infobase Publishing, New York, стр. 17 -28;

Commonwealth Secretariat (2001): Law in Cyber Space, Commonwealth Secretariat, стр.1;

DasunWeerasinghe (ed) (2009): Information Security and Digital Forensics, First International Conference, ISDF 2009 London, United Kingdom, September 7-9, 2009, Revised Selected Papers, School of Engineering and Mathematical Sciences Northampton Square, London, Springer, стр.1;

David Watson, Andrew Jones (2013): Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements, Newnes;

Eoghan Casey (2011): Digital evidence and computer crime: forensic science, computers and the internet, Published by Elsevier, стр.103-136;

ForensicScience.org,, official expert Anthony Falsetti, http://www.forensicscience.org/resources/digital-evidence/ last access 18.09.2013

Gordana Buzarovska Lazetik, Olga Koshevaliska: Digital evidence in Criminal procedures, A comparative approach, Balkan Social Science Review (BSSR), Faculty of Law, UGD, official web site http://js.ugd.edu.mk/index.php/BSSR/index последен пристап 15.12.2013;

Ibrahim Baggili (Ed.) (2010): Digital Forensics and Cyber Crime, Second International ICST Conference ICDF2C 2010 Abu Dhabi, United Arab Emirates, October 4-6, 2010, Revised Selected Papers, Sprnger, p. 1- 3 ;

IOCE Princips & Definitions, IOCE 2. Conference, Marriott Hotel, London;

ISO/IEC 27037 prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques, Reference number ISO/IEC 27037:2012(E);

John J. Barbara (ed.) (2008): Handbook of Digital and Multimedia Forensic Evidence, Humana Press Inc, New Jersey, стр.65;

John Jackson, Máximo Langer, Peter Tillers (ed.) (2008): Crime, Procedure and Evidence in a Comparative and International Context - Essays in Honour of Professor Mirjan Damaška, Hart Publishing, Oxford and Portland Oregon;

John R. Vacca (2005): Computer Forensics: Computer Crime Scene Investigation, Volume 1, Cengage Learning, стр.7;

Josiah Dykstra, Damien Riehl (2013): Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing, Richmond Journal of Law & Technology, Volume XIX, Issue 1 стр.6;

Larry E. Daniel, Lars E. Daniel (2012): Digital Forensics for Legal Professionals Understanding Digital Evidence from the Warrant to the Courtroom, Elsevier, London, стр.13;

Leah Voigt Romano (2005): VI. Electronic Evidence and the Federal Rules, 38 Loy. L.A. L. Rev. 1745, Loyola Marymount University and Loyola Law School Digital Commons at Loyola Marymount University and Loyola Law School;

Mark L. Krotoski (2011): Effectively Using Electronic Evidence Before and at Trial, Obtaining and Admitting Electronic Evidence, United States Department of Justice Executive Office for United States Attorneys Washington, DC 20530, Volume 59, Number 6, p.52;

Mark Pollitt, Sujeet Shenoi (ed.) (2005): Advances in digital forensics, IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13-16,

Michelle Potter (ed.) (2006): Digital crime and forensic science in cyberspace, Published in the United States of America by Idea Group Publishing;

Official web site: http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html last acces 17.11.2013;

Peter Mell & Tim Grance, The NIST Definition of Cloud Computing, NAT'L INST. OF STANDARDS & TECH., 2 (Sept. 2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf last access 18.10.2013;

Peter Sommer , (2012): Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers, The Information Assurance Advisory Council (IAAC), Third Edition, стр. 25-27;

Računalna forenzika NCERT-PUBDOC-2010-05-301, Nacionalno središte za sigurnost računalnih mreža i sustava, Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Risto Hristov, Atanas Kozarev (2011): Digital evidence - Annual Review, Year II, No. 3, European University, Republic of Macedonia, Skopje, p.873 – 891;

Stoilkovski, Marjan and Kaevik, Zorica and Gelev, Sasо (2012) *Корпорациска истрага на компјутерски криминален инцидент.* In: Четврта конференција за информатички технологии за млади истражувачи;

Terrence F. Kiely (2001): Forensic evidence: science and the criminal law, CRC Press LLC, New York, стр.140;

U.S. Department of Justice Office of Justice Programs: (2001) Electronic Crime Scene Investigation: A Guide for First Responders, written and Approved by the Technical Working Group for Electronic Crime Scene Investigation, Washington, USA;

Xuejia Lai, Dawu Gu, Bo Jin, Yongquan Wang, Hui Li (2010): Forensics in Telecommunications, Information and Multimedia: Third International ICST Conference, E-Forensics 2010, Shanghai, China, Revised Selected Papers, Springer, стр.227;

Zakona o kaznenom postupku Hrvatska, »Narodne novine« br. 121/11, precisteni tekst;

Законот за Финаниска Полиција на Република Македонија (Сл.Весник 55/2007);

ЗКП на Р.Македонија (Сл.Весник 150/2010 година);

Никола Матовски, Гордана Бужаровска – Лажетиќ, Гордан Калајџиев: Казнено процесно право, второ и дополнето издание, Академик, 2012 година стр.205-249;

Николоска, С.: Методика на истражување на компјутерскиот криминал, http://www.fb.uklo.edu.mk/aktivnosti.Nikoloska.aspx последен пристап 0.03.2013 година;

Поп – Јорданова, Софија (2013): Дигитална Форензика – современи сознанија, Трета меѓународна научна конференција, Промените во глобалното општество, ЕУРМ, стр.98;

Сашо Гелев, Марјан Стоилковски, Зорица Каевиќ (2012) *Корпорациска истрага на компјутерски криминален инцидент.* Во: Четврта конференција за информатички технологии за млади истражувачи;