JOGSC
Journal of Global Science
ISSN: 2453-756X (Online) Journal homepage: http://www.jogsc.com

Multidisciplinary level of observation of digital print from the point of view of informatics and criminology

Antonín Korauš *
Akadémia Policajného zboru v Bratislave
Sklabinská 1, 835 17 Bratislava, Slovakia
antonin.koraus@minv.sk

Jana Kuchtová *
Akadémia Policajného zboru v Bratislave
Sklabinská 1, 835 17 Bratislava, Slovakia
jana.kuchtova@minv.sk

Matej Barta *
Akadémia Policajného zboru v Bratislave
Sklabinská 1, 835 17 Bratislava, Slovakia
matej.barta@minv.sk

* corresponding author

Abstract: The aim of this post is to clarify the concept of digital print, pointing to the interdisciplinary nature of the issue, in particular by linking the two main areas of informatics and criminology. The solution of this issue is based on the partial outputs and conclusions of the research conducted between 2015 and 2018. The structure of the article has the character of the process from general to concrete, which means that in the first part of the article is defined digital print, its possible division from several points and their subsequent description. In the next part of the article there is clarified the criminalistic aspect of the search and the process of providing a digital track at the crime scene. The conclusion of the work provides an analysis of knowledge and proposals of recommendation character.

Keywords: Information security, informatics, criminology, trace, digital trace, ensuring traces, cyber security, security

JEL Classification: C22; C51; Q11; Q13

1. Introduction

Every individual during his existence leaves marks behind him - footprints, biological prints, memory marks. The technological development of the company and the innovations that have influenced the whole world has resulted in a new phenomenon - the creation of a digital print that every single person generates, regardless of technological knowledge. Digital shadows "or" digital footprints "relate to the traces of information we produce every day and the concern that arises on who can access and what can be done to this information.[1] There are some societal benefits arising from digital footprints. For example, we can use this information to study human behavior and social interactions.[2] A digital trace forms the basis for information science and is an integral part of every user ofinternet and digital device. Due to this, that digital trace affects to a high degree on every individual, it is necessary to focus on this evolving area, not only in terms of observing the changes that this area creates and provides through its constant development, but also, in particular, in terms of taking the single legislative position of the international level. To this issues is clearly included the issue of security and prevention against various forms of crime committed in the area.

[1] Golder, S. A.; Macy, M. W. 2014. Digital footprints: Opportunities and challenges for online social research
[2] Plachouras, V.; Leidner, J.L.; Garrow, A.G. 2016.Quantifying self-reported adverse drug events on Twitter: Signal and topic analysis.

© 2019 The Author(s). Published by Journal of Global Science.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The moral rights of the named author(s) have been asserted.

Nowadays, secure development has become a real and urgent matter in many countries around the world.[3] Due to this that this area is not well known to the public, an important factor is getting to know this issue, especially because parts of the digital print are very difficult to remove. As a result of ignorance and basically non-existent solutions to the removal of such unwanted data, it often results in loss of privacy, personal data, reputation and social degradation. The complete irremovability of the digital print is based on a criminalistic investigation, the success of which is in its permanent character, which enables it to be searched, secured and analyzed. However, the problem is the high degree of latency of such crime, as it is very difficult to detect, although generally well documented. Digital forensics investigations are an important task for collecting evidence based on the artefacts left in computer systems for computer related crimes. The requirements of such investigations are often a neglected aspect in most of the existing models of digital investigations. Therefore, a formal and systematic approach is needed to provide a framework for modeling and reasoning on the requirements of digital investigations. In addition, anti-forensic situations make the forensic investigation process challenging by contaminating any stage of the investigation process, its requirements, or by destroying the evidence. Therefore, successful forensic investigations require an understanding of the possible anti-forensic issues during the investigation.[4]

2. Classification of digital trace

The digital print is also considered to be user-generated when using the Internet and its services, technologies, and digital devices. For exmaple it is web site visits, social networks, apps, emails, ATM cards, and more. It is a unique set of digital activities, actions and communications that leave marks on the Internet or on a digital device to identify a particular user or device.[5] The term digital print in the larger sense can be defined as data left by users on digital services or devices.[6] In the narrower sense, it is also the consecuive analysis and utilization of collected and stored data.

The issue of the digital print is characterized by an interdisciplinary character, particularly in the fields of computer science, forensics and economics. From the informatics point of view, the very essence of the digital footprint, its storage, distribution and properties are examined. Criminology is concerned with the digital print of searching, securing and investigating digital prints in the process of investigating and illustrating illegal activities, criminal or other offenses. The economic point of view of the digital print is mainly in the statistical collection and analysis of the data needed for marketing purposes, allowing to businesses, companies and individuals to adjust their offer according to current market demand.

An active digital print is created by the user knowingly in order to create a certain content. The user publishes the information with the awareness of the availability of such content to other users. The most popular ways to create an active digital print include social networks, emails, blogs, and other electronic communication systems where there is voluntary web site information, phone calls, and interviews.

A passive digital print is created without the intention of the user to view and use Internet services. These are IP addresses, search terms on the Internet, cookies, connectivity providers, and localization. At the usual user level, it is not possible to prevent the passive digital print from being continually created during an Internet connection. Every device connected to the Internet has a unique internet protocol address that is static or changes at each login. Based on the device's IP address on the network, the web server can send the content of the page to the browser. The holder of personal information is the connection of the IP address with the personal data connection provider. A cookie is a saved text file that the web site saves on your device while browsing the Internet, with web pages storing information about the login name, password, language, and other settings.[7] Another use of cookies is to collect anonymous

[3] Korauš et al. 2017 The safety risks related to bank cards and cyber attacks.
[4] Beckett, P. 2018. Focus on protecting what's most important – the data, Computer Fraud and Security
[5] Digital footprint [online]. [cit. 18. 01. 2019]. Dostupné na internete: https://www.dictionary.com/browse/digital-footprint
[6] Arakerimath, 2015
[7] Európska komisia. Súbory cookie [online]. [cit. 19. 01. 2019]. Dostupné na internete: https://ec.europa.eu/info/cookies_sk

© 2019 The Author(s). Published by Journal of Global Science.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The moral rights of the named author(s) have been asserted.

statistics. The goal of cookies is to simplify web browsing - first page cookies on one side and, on the other hand, to help advertisers - a third-side cookie that can customize your personal preferences. In the case of third-side cookies, third sides may have uncontrollable third-side information.[8] Blocking these files increases user security.

In terms of identifiability, the ability to identify data and the source of information is an important factor. In the case of personally identifiable digital tracks, it is possible to track the real name of the source (IP address) of the published information and data. Anonymously generated information is sent under the pseudonym, or the user can use the technology to hide its IP address. One of the easiest ways to hide your own IP address is virtual private networks - VPN. In addition, VPNs encrypt data between the server and the user. Another extended option is a proxy server that provides different server addresses while browsing the site, but does not provide data encryption, which can lead to information gathering.[9] One of the most complex open-source resources available is The Onion Router - Tor, which protects user data. It works on the principle of identity protection by moving traffic across different servers and encrypting, resulting in random nodes on the Tor network, not on the user's computer.

A classic digital footprint consists of raw data / data, while a personal digital print, besides these raw materials, also contains data such as storage, analysis and value.[10]

3. Principles of searching and ensuring of digital traces

Digital trace as the object of investigation is ensured according to the same principles as the other subject, which serve as a source of important informations. The distinction of securing is based on the specifis properties of the carriers of these prints. Digital print can be found on every scene of crime and can be also included in all types of crime.[11] As an example, we can put regular desktop computer as one of the major carrier of print and divide it into the following categories:

1.) Crimes, where the computer is target – the computer as a digital print, stores data and informations and because of this is often the target of attacks by hackers (we recognize a hacker sucha s an individual, an organized group and in some countreys as state sponsored subject)

2.) Computer as the crime instrument – generally speaking, the tool refers to abuse of legally controlled item for simplification a crime, sucha s programming instructions for manipulation with computer analytical processes. For example, we may report abuse of bank accounts, credit cards, theft of identity and deceptions from transactions (sale of funds).

3.) Computer as an accompanying phenomenon for other types of crime – a computer is not necessary for these crimes, but its use is related to a crime. These crimes can occur without the use of computer, but the computer allows the crime to become much more difficult to identify, monitoring and prosecuting (for example: money laundering, falsifying and child pornography).[12]

As it was mentioned, computer as an individual unit can be used immediately in variety of ways, so it is important to care and respect Fundamentals of inspection. In general, crime scene observation is defined as a „specific method of criminal investigation, that seacrhes for immediate observation, provides forensic prints, identifies, investigates, evaluets and documents the state of the material environment as well as other significant objects having

[8] Roos, D. How to surf the web anonymously [online]. [cit. 20. 01. 2019]. Dostupné na internete: https://electronics.howstuffworks.com/how-to-tech/how-to-surf-the-web-anonymously1.htm
[9] Casserly, M. How hide your IP adress [online]. [cit. 20. 01. 2019]. Dostupné na internete: https://www.techadvisor.co.uk/how-to/security/how-hide-your-ip-address-3674304/
[10] Fish, T. My digital footprint [online]. [cit. 20. 01. 2019]. Dostupné na internete: http://www.opengardensblog.futuretext.com/archives/2010/01/my_digital_foot_1.html
[11] Lerner, D. E. *Electronic crime scene investigation*, 2009
[12] Barbara, J. J. Digital forensic insider: Cybercrime in perspective, *In: Forensic magazine Vol. 14* [online] 11. 2. 2018. Dostupné na internete: http://www.forensicmag.com/

© 2019 The Author(s). Published by Journal of Global Science.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The moral rights of the named author(s) have been asserted.

a relation to a criminally relevant event, to find out total situation and informations servinf to understand the objective truth about a critically relevant event.“[13]

From this definition also follows the targets we want to achieve: to search and secure prints, to identify and clarify the mechanism of the prints, uncovering and securing other criminally significant events.[14]

The process of searching and tracing is governed by the different policies and result from the features of digital prints. A digital print is an indication of information that is transmitted on a carrier that indicates that it belongs to latent prints. Other important features include time sensitivity, changeability but can be easily damaged or destroyed. Nowadays, it is very important for IT managers to be able to effectively protect their assets against modern threats.[15] Instead of criminally relevant event, i tis necessary:

- to define and correctly identify, to search and to secure all digital prints
- to document the entire loacation and location of the evidence
- to collect and mark prints
- packaging and consecutive transport[16]

Under the conditions of Slovak republic, we are guided by the principles of crime´s scene observation, withing the digital trail and the procedure for securing the Directive for performance of expert and Professional activities in the Police Chambers. When the inspection starts, important is to focus first on computers but also on people working with them. To finish any activity of these people, including keyboard or mouse manipulation. These computer components may contain biological or dactyloscopis prints. If it is possible, these prints need to be ensured first. With the computers turned on, i tis very important to document photographed running programs or open files like the Word and so on. During the inspection is important to focus on searching for non-standard devices, such as various USB keys or for example mobile phones in wristwatches.

4. Techniques and tools for securing digital prints

Assurance of investigation objects at the place of criminally relevant event is done by forensic technician. Personal computers of all kinds are provided as complete asi t is possible, in case that some components of computer are missing, then, they are overlapped with the security tape. Paper tape is not recommended.

Computer is during the securing photographicaly documentated (photographic documentation of labels with type, model, and serial number is recommended). When we are securing computers, only the unit itself is provided. The accessories of the computer are not provided, except where these components need to be provided for other investigations, for example, fingerprints. Portable computers (notebooks) are provided with a power supply.

Mobile phones and mobile devices (tablets, GPS navigation, dictaphones, etc.) are similar to laptops with a power supply or a spare battery. Data storage devices, external drives, memory cards are mechanically poorly resilient and therefore must be taken care to avoid damage. If their original packages are available, these prints will be covered in them.

In most cases, devices containing a digital track can be secured using standard tools and materials. However, it is important to ensure that digital devices are not collected, packaged or stored in order to avoid the changes, damaging or destroying the digital tracks. Do not use any tools or materials that could produce static electricity or magnetic fields, as they can damage or destroy the exploration object. In particular, it is recommended to use the following tools: camera or videocamera, gloves, cardboard boxes, security tapes, paper and plastic packaging, antistatic packaging, registration labels, etc.[17] If plastic pockets of the required sizes are available, computers and other devices are packed, but the principle is that only one print is wrapped in a single package. The security tape will

[13] Meteňko, J., Bačíková, I., Samek, M. *Kriminalistická taktika*, 2013. s. 134
[14] Porada, V. 2016. Kriminalistika
[15] Korauš, A.; Kelemen P .: 2018. Protection of persons and property in terms of cybersecurity
[16] Casey, E. Handbook of Digital Forensics and Investigation, 2010
[17] Lerner, D. E. *Electronic crime scene investigation*, 2009, s. 142

© 2019 The Author(s). Published by Journal of Global Science.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The moral rights of the named author(s) have been asserted.

overlay the drives where the data carrier can be located as well as the places for the power supply. When we are packaging the storage media, antistatic packaging is used. Every damage to the secured object needs to be documented thoroughly. Documentation of the crime scene is a matter of urgent action, so it is very important to accurately record the location of the crime-relevant event as well as the site itself. The photographic documentation, as well as topographic methods, are most frequently used in the conditions of the Slovak Republic. You need to document the status of computers and power, storage media, wireless networks, mobile phones, data storage devices, the Internet, and network access. Additional system and device documentation can be performed during the securing of prints. Ideally, the documentation should contain a detailed record using video, photos, and scene sketches.[18]

An example of where we would proceed as described above and where we could search for and secure a digital print can be referred to § 270 for counterfeiting, altering and unauthorized production of money and securities, or § 272 for the production and possession of counterfeit instruments.[19] Potential digital prints could in this case be:

- personal computers of all kinds,
- printers, copiers and scanners,
- mobile devices,
- information related to Internet activity,
- information about checks, currencies and money orders,
- removable media and external memory devices,
- photo editing software, graphics programs,
- false identification,
- information regarding financial records,
- email communication, etc.

From the example above, the print in the digital environment is on the rise and is growing with the progressive development of technology, demonstrating the need to focus on this issue as stated in the introduction to this paper. In similar cases where the digital print could be found in various offenses, there is a large amount. Of course, after the search and retrieval operations, there is a transport track for further investigation at the Institute of Criminology and Expertise.

5. Conclusions

The digital print can not be attributed to just one sector, since it is a multidisciplinary character of the solving problematics. In this post is points to the importance of the digital print in terms of informatics and criminology, while the study has demonstrated the close interconnection and inseparability of both sectors. If the principle of complexity is to be complied with, it is not possible to examine the digital print separately.The advancement of technological advances increases not only the digital print of the overall population but also the individual, resulting in an increased risk of loss of privacy, personal and other sensitive data, identity theft, illegal trade with illegally acquired data created by leaving a digital print, and others. It is essential for society to begin to perceive the issue of digital print abuse as it perceives document theft, money, good reputations, and other serious crimes, as the virtual environment has become a normal part of the life of the individual and society as such.In the long-term study of this issue, it has been found that the digital print leaves everyone regardless to his technological skill, and this print is virtually impossible to remove altogether. Therefore, it is necessary to link the digital print with criminology, in particular in terms of collecting statistics and prevention, which confirms the multidisciplinary nature of the digital print. Additionally, there is still a lack of sufficient legislation, resulting in the failure of competent authorities to deal with serious incidents, not only in the absence of qualified staffing in the police, but also in the courts' jurisdiction, and in the lack of specialized literature and incident handling practices related to the digital print.

References

[18] Lerner, D. E. *Electronic crime scene investigation*, 2009, s. 142
[19] Zákon č. 300/2005 Z. z. Trestný zákon

© 2019 The Author(s). Published by Journal of Global Science.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The moral rights of the named author(s) have been asserted.

Barbara, J. J. 2017. Digital forensic insider: Cybercrime in perspective, In: Forensic magazine Vol. 14 [online] 11. 2. 2019. Dostupné na internete: http://www.forensicmag.com/

Beckett, P. 2018. Focus on protecting what's most important – the data, Computer Fraud and Security, Volume 2018, Issue 12, Pages 6-7, DOI: 10.1016/S1361-3723(18)30118-0

Casey, E. 2010. Handbook of Digital Forensics and Investigation. Published by Elsevier Inc., 567 s. ISBN 978-0-12-374267-4

Golder, S. A.; Macy, M. W. 2014. Digital footprints: Opportunities and challenges for online social research., Annual Review of Sociology, Vol. 40:129-152, https://doi.org/10.1146/annurev-soc-071913-043145

Korauš, A., Dobrovič, J., Rajnoha, R., Brezina, I. 2017. The safety risks related to bank cards and cyber attacks, Journal of Security and Sustainability Issues, 6(4): 563-574. http://doi.org/10.9770/jssi.2017.6.4(3)

Korauš, A.; Kelemen P . 2018. Protection of persons and property in terms of cybersecurity in Ekonomické, politické a právne otázky medzinárodných vzťahov 2018/Economic, Political and Legal Issues of International Relations 2018. Fakulta medzinárodných vzťahov Ekonomickej univerzity v Bratislave,1. - 2. júna 2018, Virt, Vydavateľstvo EKONÓM, 2018, ISBN 978-80-225-4506-8, ISSN 2585-9404

Korauš, A., Kelemen, P., Backa, S., Polák, J. 2019. The Challenge of Today's are Cyber Threats In International scientific conference Innovation and Entrepreneurship: Collection of scientific articles. - Ajax Publishing, Montreal, Canada, 25.01.2019. pp. 56 - 61. ISBN 978-1-926711-08-7

Korauš, A.; Dobrovič, J.; Polák, J.; Backa, S. 2019. Security aspects and protection of people in connection with the use of personal identification numbers, Journal of Security and Sustainability Issues, Issues 8(3): 322-335. http://doi.org/10.9770/jssi.2019.8.3(3)

Korauš, A.; Gombár, M.; Kelemen, P.; Backa, S. 2019. Using quantitative methods to identify security and unusual business operations, Entrepreneurship and Sustainability Issues 6(3): 1101-1012. . http://doi.org/10.9770/jesi.2019.6.3(3)

Korauš, A.; Dobrovič, J.; Polák, J.; Kelemen, P. 2019. Security position and detection of unusual business operations from science and research perspective, Entrepreneurship and Sustainability Issues 6(3):1070-1079. http://doi.org/10.9770/jesi.2019.6.3(15)

Lerner, D. E. 2009. Electronic crime scene investigation. Nova Science Publishers, Inc., 202 s. ISBN 978-1-60876-493-8

Meteňko, J., Bačíková, I., Samek, M. 2013. Kriminalistická taktika. Brno: Václav Klemm - Vydavatelství a nakladatelství, 307 s., ISBN 978-80-87713-08-2

Plachouras, V.; Leidner, J.L.; Garrow, A.G. 2016.Quantifying self-reported adverse drug events on Twitter: Signal and topic analysis. In SMSociety.ACM. DOI:10.1145/2930971.2930977

Porada, V. 2016. Kriminalistika, Aleš Čeněk, 1024 s. ISBN 978-80-73805-89-0

Porada V., Štraus, J. 2012. Kriminalistické stopy. Aleš Čeněk, 497 s. ISBN 978-80-73803-96-4

Veselovská, S.; Korauš, A.; Polák, J. 2018. Money Laundering and Legalization of Proceeds of Criminal Activity. In Second International Scientific Conference on Economics and Management - EMAN 2018 , March 22, Ljubljana, Slovenia, Printed by: All in One Print Center, Belgrade, 2018, ISBN 978-86-80194-11-0 https://doi.org/10.31410/EMAN.2018

Legislation

Zákon č. 300/2005 Z. z. Trestný zákon

Internet sources

http://www.opengardensblog.futuretext.com/archives/2010/01/my_digital_foot_1.html

https://ec.europa.eu/info/cookies_sk

https://electronics.howstuffworks.com/how-to-tech/how-to-surf-the-web-anonymously1.htm

https://www.dictionary.com/browse/digital-footprint

https://www.techadvisor.co.uk/how-to/security/how-hide-your-ip-address-3674304/

© 2019 The Author(s). Published by Journal of Global Science.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The moral rights of the named author(s) have been asserted.