SOME ASPECTS OF FORENSICS IN DIGITAL FUTURE

Snežana Stojičić[1]
Ministry of Interior of the Republic of Serbia

Nataša Petrović
Ministry of Interior of the Republic of Serbia

Radovan Radovanović, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Milesa Srećković
School of Electrical Engineering, University of Belgrade, Serbia

Zoran Milanović, MSc
University of Criminal Investigation and Police Studies, Belgrade, Serbia

INTRODUCTION

Forensic concepts related to growing digitalization process should continue to keep focus on providing support for legal proceedings, following defined and adopted guidelines. The application of technology has become dominant in many aspects of everyday life, having been enabled by the digitalization of processes and the application of information and communication technologies in all spheres of life.

In an era of digitization of processes all over the world and an evident increase in data and information available in digital form, law enforcement agencies around the world are facing significant challenges. Accordingly, it is necessary to build capacities to apply techniques and technologies in conducting investigations, and applying forensic methods. It is of utmost importance to adopt new approaches to address such challenges. This paper analyses the current stage of development

1 snezana.stojicic@mup.gov.rs

of the digitization processes from different points of view and the circumstances surrounding it in the area of forensics, contributing to this area by identifying and analysing challenges to be considered by law enforcement agencies. It also suggests future directions of research, which may contribute to the adoption of a new approach in addressing these challenges (Montasari, 2017; Montasari et al., 2020, Stojičić et al., 2022). According to the prosecutor for high-tech crime, 5,274 criminal acts were reported in 2021 only to the Special Prosecutor's Office, concerning something that could be deemed to constitute cybercrime. That is an increase of about 11 percent in relation to the number of crimes committed in 2020 (RTS, 2020).

The technological advancements include, but are not limited to: high volume of data, different digital devices, hardware and software technologies, anti-forensic techniques, video and media, encryption, communication infrastructures, wireless, virtualization, borderless services and dark web tools. Also, the lack of standardized tools and methods has been identified, as well as usability and visualization, raising interest of scientists to overcome these challenges. It is evident that technologies such as communication networks, mobile devices, Internet of Things (IoT) solutions, cloud-based services, cyber-physical systems bring many benefits but also challenges. At the same time, they bring new threats to cyber security, and it is an emerging issue.

The use of the Internet of Things (IoT) is growing exponentially, but the security aspects for IoT projects and their implementation are still not at a satisfactory level for many organizations. Device identification is more complex than simply using a certificate, especially considering that one of the basic components of IoT security is providing functionality so that devices and services have reliable identification methods so that they can achieve secure communication within their environments. However, there is a little information on how to build in forensic capabilities for it. The IoT forensic procedures might be related to data, service and/or architecture, all of which might be connected to the other external systems. This is an open area for research, innovative actions and work to make it easier, quicker and more reliable for the investigator.

Identification of persons was, is and will be a challenge as it involves efforts to provide adequate technological responses, especially based on the use of biometric data in electronic form and application of the principles and experiences of the best practices of electronic business in general. From the forensic aspect, as a response to potential violations and non-compliance with legal norms, this requires the development and application of new procedures and tools. Today, the need for constant monitoring of the development and application of new technological solutions and methods for the identification of persons, especially those that can be related to forensic aspects in the digital world, is evident (Stojičić et al., 2022).

Accurate and efficient identification has become crucial for forensic application as an answer to diversity of criminal activities. An advancement in biometric technology together with techniques of computational intelligence is replacing traditional identification processes in forensic science. The effectiveness of biometrics systems lies in different recognition processes, which include transferring data in digital form, extracting standardized characteristics and feature matching. The forensic biometrics covers a wide range of applications for physical and cybercrime detection. In a way, forensic biometrics also overcomes the loopholes of traditional identification system that were based on personal knowledge and competence (Saini & Kapoor, 2016).

DESIGN/METHODS/APPROACH

Achieving continuity in the development of forensic methods is an imperative in modern society. Monitoring the development and enabling the application of new technological solutions for dealing with evidence in digital form as well as in the field of determining the identity of a person, requires significant resources and adjustments while preserving the existing systems in accordance with the normative framework. Certain relevant references were reviewed and analysed in detail and a general assessment was made regarding the application of new technologies.

FINDINGS
CURRENT STATUS AND TRENDS

We have entrusted the backbone of civilization to machines and the Internet. Digital technologies, although they are an essential need of modern society, have always been a double-edged sword. Their application provides us with many benefits that we gain a lot in everyday work and life, but we also lose just as much.

Because of the IT development, almost all of data in the real-life is processed by electronic information. To this end, a tremendous amount of digital information is being made daily (Manyika et al., 2011). Nowadays, users tend to utilize multiple digital devices and access tenths of digital services per day (Purnaye & Kulkarni, 2021). The digital footprint of our everyday life has become enormous, and accordingly, the probability that illegal activities may leave digital evidence behind is very high.

Access to digital evidence has become a key element in police investigations, not only when it comes to prosecuting cybercrime, but also any other kind of crime. According to the European Commission, electronic evidence in any of its forms is relevant in about 85% of total criminal investigations and, in almost two thirds (65%) of these, the service providers to whom the requests are directed are located in a different jurisdiction. The combination of the two previous percentages results in fact that 55% of the total investigations include a request for cross-border access to electronic evidence (European Commission, 2018).

The diversity of digital devices is constantly increasing, data storage capacity is growing exponentially as well as the need to process ever-larger datasets with ubiquitous time imperatives (Yaacoub, 2021).

Nowadays, users tend to utilize multiple digital devices and access tenths of digital services per day (Purnaye et al., 2021). The digital footprint of our everyday life has become enormous, and accordingly, the probability that illegal activities may leave digital evidence behind is very high (Nance et al., 2010). One of the problems in obtaining and securing evidence in digital form is the nature of it as well as the use network environment, as it is the Internet itself. It poses serious challenges as jurisdiction is usually linked to the territory of the state, but the Internet has no borders. The intermediary that has the information may not necessarily be established in the same country where the criminal investigation is being carried out or, even if it is the case, the data may be on servers abroad. The characteristics of electronic evidence in itself add more problems, such as dynamic changes in cloud environment, since data are stored, duplicated or moved between servers somewhere in the cloud, in possibly multiple or unknown jurisdictions (Kleijssen & Perri, 2016).

CLOUD ENVIRONMENT CHALLENGES

Data collection techniques play a major role to identify the source of problems related to the attacks by acquiring evidence from various sources such as cloud storage, cloud log analysis, Web browsers, and last but not least, through physical evidence acquisition processes. Cloud computing enabling moves application software and databases to large data centres, where challenges arise such as the outsourcing of sensitive data and services that might not be trustworthy (Sree and Bhanu, 2020). It might be an entry point for various security threats and attacks in the cloud. As previously stated, Cloud forensics is a contemporary application of scientific principles, practices, and methods to reorganize the events through identification, collection, preservation, examination, and reporting of digital evidence (Zawoad and Hasan, 2013). From the forensic science perspective, the

need has been identified for developing a solution to preserve and acquire cloud data. It might be done by developing a library of forensic methodologies for the various cloud platforms (Montasari et al., 2017; Montasari et al. 2019, Yaacoub, 2021). The approach for this should be multidisciplinary effort and it should include legal and technical point of view in an exploratory manner. Developing new methodology should also include guidelines for cloud customers and incident handling in the cloud environment.

In order to identify the evidence, it has to be taken from trusted third parties, which in the case of cloud computing is a cloud service provider. In cloud forensics there are numerous techniques that arise on the basis of cloud service models and deployment models. In the Software as a Service (SaaS) and Platform as a Service (PaaS) models, as in these cases the users do not have any control of the hardware, have to depend on Cloud service provider (CSP) for collecting the evidence, whereas, in the case of Infrastructure as a Service (IaaS) model, users can acquire the virtual machine image and logs. The forensic examiner isolates the incidental system in the virtualized environment and analyses it based on the artifacts left by the perpetrator of the criminal offence (Dykstra and Sherman, 2012; Marty, 2011) in order to find information as to *where*, *why*, *when*, *by whom*, *what*, and *how* it has happened.

These indicate the need for both applied and theoretical published research consideration. It might help to get an early start in researching new techniques because of the increasingly stringent accrediting requirements for any new technique from the forensic perspective. The tools and procedures to ensure those data from a forensic point of view need to be identified and developed. There is certainly a need to develop tools which include both operational and infrastructural readiness and it can help with forensic investigations in the cloud. They may relate to the preservation of regular records of warehouse status, log authentication and access. Follow up log of user activities in a virtual environment requires specific knowledge, and it can be difficult especially if the structure of the virtual environment is disrupted.

IOT FROM THE FORENSIC POINT OF VIEW

The majority of IoT technologies have built-in flash memory to run a simple form of operating systems or real-time applications, therefore data from analysed devices need to be accessed and extracted using well-defined forensic methods. Moreover, to deal with the forensic methods related to IoT-connected devices, cloud cyber security will need to be reviewed as each IoT device produces data that is stored in the cloud (Montasari et al., 2020). Furthermore, investigations involving IoT

devices can be even more difficult than those in the cloud investigations due to the constant emergence of new and diverse devices with different operating systems, using different communication channels and protocols. As a consequence, more complex procedures are required for research on these devices. Therefore, IoT forensics must include the identification and extraction of evidentiary artifacts from smart devices and sensors, hardware and software that facilitate communication between smart devices and the outside world as well as hardware and software which are outside the network environment under investigation (Montasari et al., 2020).

Forensic investigation of IoT devices requires specialist knowledge related to the handling and knowledge of the detailed technical specifications of the device in order to obtain the necessary data. Also, forensic challenges, related to IoT devices, include issues such as availability, authenticity and non-repudiation which are essential for forensically sound use of data (Lillis et al., 2016). Persistency of data is also under question because of IoT devices' limited memory or no persistent data storage. Because of that, data stored for longer periods is likely to be stored in in-network hubs or to be transferred to the cloud for more persistent storage. Thus, we come to the problems associated with Cloud forensics.

BIG DATA FORENSIC

The main challenges of big data are so-called the 3Vs: volume, variety, and velocity, in certain circumstances, it might not be satisfactory to alter the conventional principles and procedures, meaning that all data must be extracted as it is to be unamused according to forensic principles (Montasari et al., 2020, Manyika, 2011, Montasari, 2017, Soni, 2019). Therefore, techniques related to the main phases of standardized forensic processes, related to identification, acquisition, and analysis, have to be adapted to the context of a big data. In order to conduct forensic processes in a way as possible effective might approach with a proper prioritization or triage can be conducted is through visualization, both for low-level file system analysis and higher-level content analysis (Montasari et al., 2020).

EMERGED METHODS AND TECHNIQUES

From the judge's trail processes perspective, the standardization is an important tool to ensure that the evidence acquired during the investigative process are valid and acceptable. When comes to dealing with mobile devices, it is of special importance to be standardized and followed for the procedures from the forensic

point of view, due to very quick development of mobile devices and related technologies. Forensics of mobile devices, today, is an essential part of nearly every criminal investigation (Pawlaszczyk, 2022). Standardization should allow for quick adjustment of the necessary forensic procedures and in many cases saves the time needed to obtain evidence (FORMOBILE, 2022). Furthermore, keeping adherence to the standards during all steps of investigation is of critical importance for the evidences being regarded as reliable and accepted for the court, and development of standard is of utmost importance to secure the successful outcome of the investigation.

Through the FORMOBILE project was identified 61 standards, among them only 10 standards describe procedures in mobile forensics, and in addition, there was identified 18 non-formal standards (FORMOBILE, 2022).

BIOMETRIC DATA IN FORENSIC

Still, biometric data are increasingly used in a variety of contexts. According the assessment (Lunter, 2022) it is expected that between 2020 and 2025, the global biometric technology market will to grow at a compound annual growth rate of 10.5%. With respect of this the investment in research and development in this sector is also skyrocketing. Users like airports are ramping up their investments, the interest and tech partnerships are increasing too in area of the global biometrics ecosystem. It seems that in future this ecosystem will compound and correlate with all other technologies developing nowadays. However, with the expected increase in application, it is important to simultaneously implement activities to raise awareness about the challenges that biometric technologies bring, especially from the aspect of building trust in technological solutions (AEPD, 2020). Also, at EU level, processing of biometric data has been more and more used in the context of EU large-scale information systems. These systems more and more relay on biometric data, what might be seen through ongoing development of new systems and interoperability framework. The ongoing technological and societal developments, form the aspect of biometric systems should be able to provide the most accurate results in different circumstances and conditions. However, no less important aspect of the application of biometric systems is public acceptance.

Establishment of a systematic description of the concepts in the field of biometrics standardization (ISO) is all the time actual, although there is difference in solutions supporting work with biometric data pertaining to recognition of human beings.

Artificial intelligence (AI), shows that, although identification is main aim for biometrics, there is development aimed not primarily at identification, but at

the categorization of individuals. Directed to recognize individual according to different categories, it might be for instance on the basis of age or gender. It is however not always clear how the processing occurring for the purposes of categorization is linked to identification, or to what extent such practices can always be separated. Sometimes stay unclear, whether the data processed for categorization purposes concern an identified or identifiable person at all. Also sometimes is unclear whether the collected data (biometric or not) might be used for the identification of the individual, even if they are already processed for the purpose of categorization. Furthermore, sometimes the categorization of individuals, is in practice, a step taken towards identification.

Biometric technologies that enable artificial intelligence contribute to general safety and security, but also bring risks from the aspect of fundamental rights. The most talked about topic today is related to technologies that enable remote identification and tracking of individuals in public spaces, which can potentially negatively affect their rights to freedom of expression, freedom of assembly and association, changing the way individuals and groups can express themselves his social and political opinion (European Parliament, 2021). An example of this is the use of facial recognition technologies. Different uses of biometric technologies can have different specific types of impact. For the application of remote biometric identification in public spaces, solutions are sought, because it concerns the processing of a large amount of data about individuals without their consent, cooperation or knowledge.

Due to its critical role in cyber security, digital forensics has received significant attention from researchers and practitioners alike. The ever-increasing sophistication of modern cyber-attacks is directly related to the complexity of evidence acquisition, which often requires the use of several technologies.

THE CONCEPT OF DIGITAL FOOTPRINT

The concept of 'Digital footprint' including the meta data and content is linked with topics such as digital identity, privacy and trust, online safety, information management. As a picture says more than a thousand words, in picture 1, the current situation is shown, as one of the results of analyses, according to knowledge and analysed literature.

One of the most common Internet uses is communicating with others through social networking platform. This leads to an individual's Internet identity and creation of a person's digital footprint which is traceable data and information that a user generates when they go online (Thatcher, 2014).

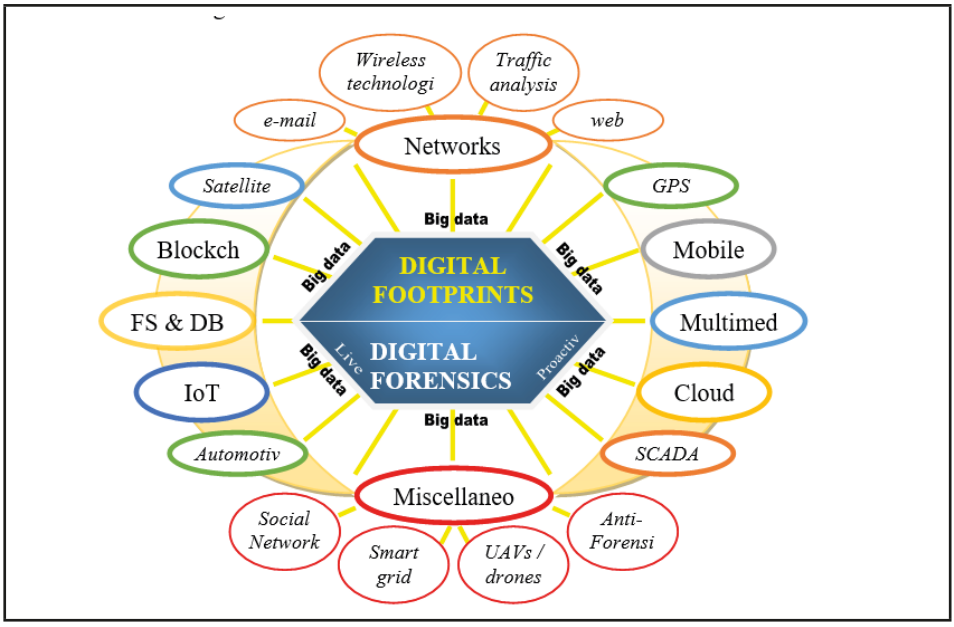

Figure 1: Everything digital leaves a footprint and to everything digital is applied forensics

THE SOCIAL NETWORK INVESTIGATION

Social network acts as a good platform as a matter of fact which afford many simple user actions, such as liking, favouriting, following, or commenting which are not necessarily considered active participation but nonetheless contribute to a digital footprint (Büchi, Lutz & Micheli, 2017). Although young individuals are often online, they do not consider deliberately how their Internet usage impacts their digital identity, instead, concentrating more on the short-term advantages of being able to network with friends (Oxley, 2010).

Mostly *netizens* use social networks as new media to document their lives effectively (Büchi, Lutz & Micheli, 2017). However, this may cause more harm rather than good. For example, cyber bullying. Englander et al. (2017) conclude cyber bullying as sending, posting or sharing negative, harmful, false or mean contents about someone else causing embarrassment or humiliation online. As to avoid that, it is important to educate people not only kids, but also includes all categories especially parents. This leads to awareness of digital citizenship to pay attention towards the improper behaviour that may lead to dangers of cyber bullying and other social-media events (Martin et al., 2018).

Digital footprints originate from active content creation, passive participation, and platform-generated data what we presented at Figure 2.

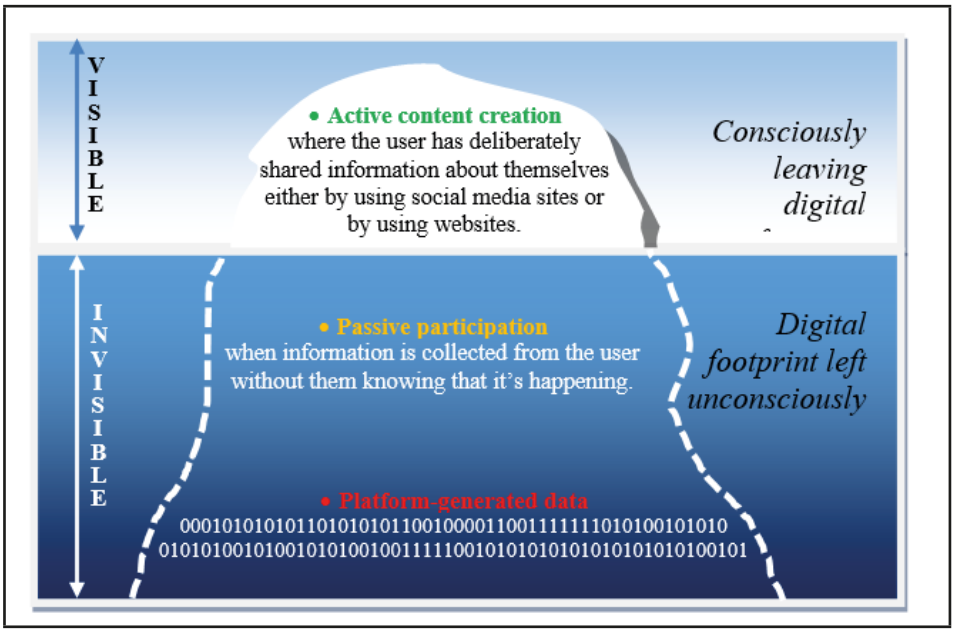

Figure 2: The iceberg, visible and invisible levels of digital footprints

The field of digital forensics still lacks formal process models that courts can employ to determine the reliability of the process followed in a digital investigation. The existing models have often been developed by digital forensic practitioners, based on experts' personal experience and on an ad-hoc basis, without paying attention to the elements relevant for establishment of standardization (Montasari et al., 2019).

The international standard, Information technology - Security techniques - Incident investigation principles and processes (ISO/IEC 27043:2015, IDT), provides guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence. It includes processes from pre-incident preparation through investigation closure, as well as any general advice and caveats on such processes. The guidelines describe processes and principles applicable to various kinds of investigations, but not limited to, unauthorized access, data corruption, system crashes, or corporate breaches of information security, as well as any other digital investigation. In summary, this International Standard provides a general overview of all incident investigation principles and processes without prescribing particular details within each of the investigation principles and processes covered in this International Standard (ISO/IEC 27043:2015, IDT).

It should not be forgotten that the success of forensic science depends on human reasoning abilities. Although we should not forget that Human thinking has strengths and weaknesses. In this sense, the main challenge is to avoid biases arising from foreign knowledge or from the comparison method itself.

SOME SOLUTIONS FOR RESPONSE TO THE NEW CHALLENGES

In a case that crime occurs in cloud environment, it is very difficult to identify evidence. Moreover, the evidence collection plays a vital role to identify and access to data from various sources in the cloud environment for forensic investigation, as there no longer evidence stored in a single physical host, and data might be distributed and settled across different geographical locations.

Similarly, the evidence stored in Web browser cache at the root directory of a Web application might be used to identify the source of an incident. The reviews of collection process and recovery methods for various Web browsers can be found in literature (Sree and Bhanu, 2020).

As response for challenges in digitalization era, there are many tools developed and still developing to identify, collect, and analyse the forensic data for investigation. Juel and Kaliski developed the tool for the identification of online archives (Juels and Kaliski, 2007). Dykstra and Sherman proposed a forensic tool for acquiring the cloud-based data (Dykstra and Sherman, 2012). Moreover, Encase and Access data FTK toolkit might be used for the identification of trusted data to acquire the evidence. Similarly, tools such as evidence finder and F-response are used to find the evidence related to social networks. Dykstra and Sherman proposed an open-source OpenStack cloud tool for the identification of evidence from virtual disks, API logs, and firewall logs, etc. (Dykstra and Sherman, 2013). Some of the tools that might be taken in consideration regarding the forensic investigation are presented in Table 1 with reference links, according to the analysed sources of authors' choice. Bearing in mind the growing needs of the digital era, further investigation might be directed to analyse content based on some predefined criteria using tools that can be applied, and - wherever it might be possible - some practical testing.

Table 1 An overview tools (online services and software packages), solutions that might be used for forensic investigation

Tool	Purpose / link
Have I Been Pwned	Allows searching across multiple data breaches if a specific email address or phone number has been compromised. https://haveibeenpwned.com
IntelligenceX	An open-source Intelligence and forensics tools, many features and tools are available, including the 'email' tool that can help identify if leaked passwords and additional information is associated with a specific email. https://intelx.io/tools
Whois Lookup	A large database of whois information on DNS, domain names, name servers, IP addresses, registrar and owner data, and so on. https://whois.domaintools.com/
ViewDNS	A multi-tool on website can help to identify all the sites hosted on a given web server, including domain and IP, reverse whois lookup, finding domain names and their owners, and so on. https://viewdns.info
Sherlock	A tool that can find valid accounts on target websites given a specific username or email address. As its authors say, it can "hunt down social media accounts by username across social networks". https://github.com/sherlock-project/sherlock
Instant Username Search	A tool capable of checking more than 100 social media sites and verifying if a specific username is available. It can be very useful for obtaining additional details on the target usernames. https://instantusername.com/
Spiderfoot	An open-source intelligence (OSINT) automation tool. It integrates with just about every data source available and utilizes a range of methods for data analysis, making the data easy to navigate. https://github.com/smicallef/spiderfoot
Paraben Suite	Forensic platform with support for desktop forensics, Email forensics, Smartphone analysis, Cloud analysis, IoT forensics, from acquisition to analysis and result visualization. https://paraben.com/
DomainTools	Allowing to connect with nearly every active domain and IP address on the Internet. It is a proprietary threat intelligence and investigation platform that combines enterprise-grade domain and DNS-based intelligence with an intuitive web interface. https://www.domaintools.com/

Tool	Purpose / link
CloudNine Discovery	A cloud-based eDiscovery automation platform that streamlines the litigation discovery, audits, and investigations by allowing users to review, upload, and create documents in a central location, include discovery consulting, computer forensics, managed review, online hosting, information, governance, litigation support, and project management. https://cloudnine.com/
PassMark Software	Extract forensic data as it is passwords, decrypt files and recover deleted files quickly and automatically from Windows, Mac and Linux file systems, identify evidence and suspicious activity through hash matching and drive signature analysis features. https://www.passmark.com/
MailArchiva	MailArchiva is a professional enterprise grade email archiving, e-discovery, forensics and compliance solution. https://www.mailarchiva.com/
Cyber-Triage	Forensics software for incident response, automated incident response software for fast, comprehensive, and easy intrusion investigations (malware, ransomware, account takeover). https://www.cybertriage.com/
Quest	Dedicated to collecting and reviewing from a variety of sources, both on premises and in the cloud, makes it easier than ever to reduce the complexity of searching, analysing and maintaining critical IT data scattered across information silos. https://www.quest.com/
Truxton	Solution, easy-to-use, with analyst-driven interface allowing to get up to speed quickly, without mastering specialized code or techniques, has open architecture that allows to take data into other tools for verification and reporting. https://truxtonforensics.com/
SandBlast	SandBlast Network and Harmony Endpoint utilize Threat Extraction technology to eliminate threats and deliver safe, clean content. Allowing to remove exploitable content, reconstruct files to eliminate potential threats, and deliver sanitized content to users in a short time to maintain business flow, with threat extraction supports of the most common document types used today. https://sc1.checkpoint.com/documents/R80.40/SmartEndpoint_OLH/EN/Topics-EPSG/Forensics.html
X-Ways	An advanced work environment for computer forensic based on the WinHex hex and disk editor and an efficient workflow model. https://www.x-ways.net/

Tool	Purpose / link
Cellebrite	Allowing to conduct in-depth analysis and generate custom reports, with advanced searching with filtering capabilities, and built-in AI media categorization, supporting investigators to find Internet History, Downloads, Locations, Recent searches, and so on. https://cellebrite.com/en/home/
Barracuda	A powerful delivered-email search and rapid deletion from all inboxes, identify anomalies that may indicate threats, based on insights gathered from analysis of previously delivered email by using intelligence gathered from previous threat responses to block future emails from malicious actors, and to identify your most vulnerable users. https://www.barracuda.com/
CrowdStrike	It is a comprehensive data collection while performing triage analysis during an investigation. Allowing faster response to investigations, conduct compromise assessments along with threat hunting and monitoring. Represent a single solution to analyse large quantities of data both historically and in real-time to uncover vital information to triage an incident. https://www.crowdstrike.com/
CyFIR	A digital security and forensic analysis solutions provide unparalleled endpoint visibility, scalability, and speed to resolution. Allowing cyber risk solutions to identify, analyse, and resolve active or potential threats. https://sourceforge.net/software/product/CyFIR-Investigator/
TIBCO	It provides the industry's first enterprise class, end-to-end log management solution, providing possibility to find and act on critical information hidden inside volumes of machine and log data. https://www.tibco.com/
Imperva Analytics	It provides automatic detection of non-compliant, risky, or malicious data access behaviour across all of organisation databases, enterprise-wide, automatically uncovers data access behaviour whether accidental, poor practice or deliberately malicious. It enables visibility into a broad range of risks from accidental exposures to persistent attacks by an evasive exploit. https://www.imperva.com/products/attack-analytics/
Omnis Cyber Investigator	It is an enterprise-wide network threat and risk investigation platform that helps to detect, validate, investigate and respond to threats. Reduce the impact of cyber threats with an analytics system that also integrates with popular Security Information and Event Management platforms. This cloud-first approach helps to manage threats across complex digital infrastructures and to deal with cyber threat security with visibility across physical and hybrid-cloud infrastructure. https://www.netscout.com/product/cyber-intelligence

Tool	Purpose / link
Qintel CrossLink	Search results from six synergistic verticals of network and actor-centric data and provide key information that can be assembled and shared. Data verticals include an unparalleled range of actor profiles, communications, historical Internet registration records, IP reputation, digital currency records, and passive DNS telemetry that jump-start investigations into actors and incidents. https://www.qintel.com/products/crosslink/
Xplico	It is installed in the major distributions of digital forensics and penetration testing: Kali Linix, BackTrack, DEFT, Security Onion, Matriux, BackBox, CERT Forensics Tools, Pentoo and CERT-Toolkit. Xplico allows concurrent access by multiple users. It can be used as a Cloud Network Forensic Analysis Tool by provision of extract from an internet traffic capture the applications data contained. https://www.xplico.org/
Parrot-OS	It includes a full portable laboratory for all kinds of cyber security operations, from pentesting to digital forensics and reverse engineering, but it also includes base to develop own software or keep data secure. https://www.parrotsec.org/
EnCase-Forensic	The Gold Standard in Forensic Investigations – including Mobile Acquisition. Improve investigation efficiency with the release of optical character recognition support that seamlessly extracts embedded text from scanned images, documents and PDFs as part of the evidence collection workflow. Also expands social media artifact support and includes an enhanced workflow. https://security.opentext.com/encase-endpoint-security
ProDiscover	It addresses a wide range of cybercrime scenarios encountered by law enforcement and corporate internal security investigators. It is also support for diagnostic and evidence-collection tools for corporate policy compliance investigations and electronic detection. Contains a wide range of tools to explore the evidence disks and extract artifacts relevant to the investigation. It was one of the first products to support remote forensic capabilities. https://prodiscover.com/
AD-Enterprise	Provides support to respond quickly, remotely and covertly while maintaining chain of custody, and facilitates focused forensic investigations and post-breach analysis, without interruption to business operations. Allowing to perform collections from endpoints in multiple locations. https://accessdata.com/knowledge-library/product/ad_enterprise
Quin-C	Quin-C, works seamlessly with the AccessData solutions, already know and trust, and provide maximum control over the way to collect, process, review, analyse and report on key pieces of data. https://www.quincforensics.com/

Tool	Purpose / link
SmartEvent	This event management provides full threat visibility with a single view into security risks. Take control and command the security event through real-time forensic and event investigation, compliance, and reporting. Respond to security incidents immediately and gain network true insights. https://www.checkpoint.com/quantum/event-management/
Cado Security	Represents a response platform, takes the complexity out of cloud and helps to focus on what's most important. It provides detailed detection for malicious files, suspicious events, and financial information. Cloud systems disappear quickly, and automated data collection allows to secure incident data safely before it is gone. https://www.cadosecurity.com/
Change Auditor	Change reporting and access logging for Active Directory and enterprise applications is cumbersome, time-consuming and, in some cases, impossible using native IT auditing tools; it helps to get complete, real-time IT auditing, in-depth forensics and security threat monitoring on all key configuration, it also tracks detailed user activity for logons, authentications and other key services across enterprises to enhance threat detection and security monitoring. https://www.quest.com/change-auditor/
FireEye	Combines heuristics, code analysis, statistical analysis, emulation, and machine learning in one solution. Enhances detection efficacy with frontline intelligence derived on the frontlines of the world's biggest breaches. Provides possibility to choose from a complete set of deployment scenarios, including in-line and out of band, on-premise, hybrid, public and private cloud, and virtual offerings. Consolidate network security technology stack with a built-in Intrusion Prevention System and Dynamic Threat Intelligence. https://www.fireeye.com/
Agari	Use unique AI with machine learning model updates method. Global intelligence powered by trillions of global email messages provide deep insights into behaviours and relationships. https://www.agari.com/
IBM-Security-QRadar	Intelligent security analytics for insight into the most critical threats. Provide a comprehensive insight to quickly detect, investigate and respond to potential threats, a comprehensive visibility into enterprise data across on-premises and cloud-based environments. Detect known and unknown threats, go beyond individual alerts to identify and prioritize potential incidents, and apply AI to accelerate investigation processes. https://www.ibm.com/qradar

Tool	Purpose / link
BloxOne-Threat-Defense	It operates at the DNS level to see threats that other solutions do not and stops attacks earlier in the threat lifecycle, protect network and automatically extend security to digital environment, including SD-WAN, IoT and the cloud. It powers security orchestration, automation and response solutions, slashes the time to investigate and remediate cyber threats, optimizes the performance of the entire security ecosystem and reduces the total cost of enterprise threat defence. https://www.infoblox.com/products/bloxone-threat-defense/
FORST	Open stack cloud computing platform to acquire Api's logs, Virtual disk and guest firewall logs. FROST is the first forensics tool built into IaaS model. https://www.openstack.org/

However, good forensic analysis often requires forensic scientists to look at and evaluate some evidence independently of everything else known about the case. It is certainly necessary for individuals and laboratories to make continuous efforts to improve their capacities, find ways in which they can develop procedures to facilitate analysis, constantly follow the development of technologies and new solutions in order to avoid the limitations that they bring and find a way to keep up with the challenges that it brings (Spellman, Eldridge & Bieber, 2022).

ORIGINALITY/VALUE

Presented paper gives an overview and analyses, from the authors' perspective, current challenges that forensic science is faced with. In respect of general trends in digitalization processes in all spheres of life, an attempt has been made to identify the effects that these have on forensic methodologies that might be used for person identification. Given the fact that urgent needs for identification have been recognized, new technologies and measures have to be taken into consideration in order to be able to properly respond from the forensic point of view. The surveys carried out to date have identified various areas within the field identification where it would be valuable to direct further efforts and to engage in research. Due to its critical role in cyber security, forensics dealing with evidence in electronic form represents a challenge for both researchers and practitioners.

Given the ever-increasing prevalence of modern technology, there is a corresponding increase in the likelihood of digital devices being pertinent to a criminal investigation or civil litigation. It can be anticipated that the number of cases dealing with evidence in the digital form or converted into digital form that need to be analysed will significantly increase in the future.

Identified and presented topics are relevant and in line with both the researchers' point of view and their professional experience, including different fields of expertise and confirmed multidisciplinary nature of forensic science.

Therefore, in order to keep pace with the new challenges, what is required is a multi-faceted approach in which evidence can be collected and analysed from a variety of sources.

REFERENCES

Agencia Española de Protección de Datos (AEPD), and the European Data Protection Supervisor (EDPS). (2020). 14 misunderstandings with regard to biometric identification and authentication | European Data Protection Supervisor (europa.eu)

Alabdulsalam, S., Schaefer, K., Kechadi, T., Le-Khac, NA. (2018). Internet of Things Forensics – Challenges and a Case Study. In: Peterson, G., Shenoi, S. (eds), Advances in Digital Forensics XIV. DigitalForensics 2018. IFIP Advances in Information and Communication Technology, 532. Springer, Cham. https://doi.org/10.1007/978-3-319-99277-8_3

Alghamdi, I. M. (2021). Digital Forensics in Cyber Security—Recent Trends, Threats, and Opportunities. In (Ed.), Cybersecurity Threats with New Perspectives. IntechOpen. https://doi.org/10.5772/intechopen.94452

Aminnezhad, A., Dehghantanha, A., Abdullah, M. T., & Damshenas, M. (2013). Cloud forensics issues and opportunities. International Journal of Information Processing and Management, 4(4), 76.

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. *IEEE Security and Privacy Magazine*, 15. DOI: 10.1109/MSP.2017.4251117.

Dykstra, J. & Sherman, A.T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, 9, S90-S98. DOI: 10.1016/j.diin.2012.05.001

Dykstra, J., & Sherman, A. T. (2013). Design and Implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. *Digital Investigation*, 10, S87-S95.

European Commission (2018). Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal rep-

resentatives for the purpose of gathering evidence in criminal proceedings, SWD/2018/118 final – 2018/0108 (COD), 17 April 2018, p. 14.

European parliament (2021). Person identification, human rights and ethical principles, Rethinking biometrics in the era of artificial intelligence, Study, EPRS_STU(2021)697191_EN.pdf (europa.eu)

Fahdi, M. Al., Clarke, N.L., & Furnell, S.M. (2013). Challenges to Digital Forensics: A Survey of Researchers & Practitioners Attitudes and Opinions, https://digifors.cs.up.ac.za/issa/2013/Proceedings/Full/64/64_Paper.pdf

FORMOBILE (2022). From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices, H2020, ID: 832800, DOI: 10.3030/832800, https://cordis.europa.eu/project/id/832800

Glinski, M. (2022). Validate your Digital Footprint, Security Scorecard, Available at https://support.securityscorecard.com/hc/en-us/articles/4402645460763

Horan, C., & Saiedian, H. (2021). Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. Journal of Cybersecurity and Privacy. 1. 580-596. DOI: 10.3390/jcp1040029.

ISO, STANDARDS BYISO/IEC JTC 1/SC 37 Biometricsh. https://www.iso.org/committee/313770/x/catalogue/

ISO/IEC 27043:2015, Information Technology - Security Techniques - Incident investigation principles and processes (ISO/IEC 27043:2015, IDT)

Janarthanan, T., Bagheri, M., & Zargari, S. (2021). IoT Forensics: An Overview of the Current Issues and Challenges. DOI: 10.1007/978-3-030-60425-7_10.

Juels, A., & Kaliski B. (2007). Proofs of retrievability for large files. In: Proceedings of the 14th ACM conference on Computer and Communications Security; ACM. 2007. pp. 584-597. DOI: 10.1145/1315245.1315317

Kleijssen, J. & Perri, P. (2017). Cybercrime, Evidence and Territoriality: Issues and Options, Netherlands yearbook of International Law, 147-173. Available at: https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-op-tions/168077fa98

Lillis, D., Becker, B. A., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. Proceedings of the 11th Annual ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Daytona Beach, FL. Academic Press. https://commons.erau.edu/adfsl/2016/tuesday/6

Lim, N. (2020). Cloud Forensics and the Digital Crime Scene, Available at https://www.appdirect.com/blog/cloud-forensics-and-the-digital-crime-scene

Lunter, J. (2022). Top 8 Advancements in Biometrics That Will Mark 2022, Biometrics Technology Industry, https://doi.org/10.1287/LYTX.2022.02.15

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. et al. (2011). Big Data: The Next Frontier for Innovation, Competition, and Productivity, McKinsey Global Institute, pp. 1-137.

Marty. R. (2011). Cloud application logging for forensics. In: Proceedings of the 2011 ACM Symposium on Applied Computing; 2011 Mar 21; ACM. 2011. pp. 178-184. DOI: 10.1145/1982185.1982226

Mitchell, F. (2014). The use of Artificial Intelligence in digital forensics: An introduction. Digital Evidence and Electronic Signature Law Review. 7. DOI: 10.14296/deeslr.v7i0.1922.

Montasari, R. (2017). A standardised data acquisition process model for digital forensic investigations, Int. J. Information and Computer Security, 9(3), 229-249, DOI: 10.1504/IJICS.2017.10005908

Montasari, R. (2017). An Overview of Cloud Forensics Strategy: Capabilities, Challenges, and Opportunities. In: Hosseinian-Far, A., Ramachandran, M., Sarwar, D. (eds) Strategic Engineering for Cloud Computing and Big Data Analytics. Springer, Cham. https://doi.org/10.1007/978-3-319-52491-7_11

Montasari, R., Hill, R., Carpenter, V., & Hosseinian-Far, A. (2019). Evaluation of the Standardised Digital Forensic Investigation Process Model (SDFIPM). DOI: https://doi.org/10.1142/9789811204463_0009.

Montasari, R., Hill, R., Parkinston., S., Peltola, P., Hosseinian-Far, A., & Daneshkhah, A. (2020). Digital Forensics: Challenges and Opportunities for Future Studies, International Journal of Organizational and Collective Intelligence, 10(2). Montasari_etal_IGI_2020_Digital_Forensics_Challenges_and_Opportunities_for_Future_Studies.pdf (northampton.ac.uk)

Montasari, R., Hill, R., Parkinson, S., Peltola, P., Hosseinian-Far, A. & Daneshkhah, A. (2020) Digital Forensics : Challenges and Opportunities for Future Studies. International Journal of Organizational and Collective Intelligence (IJOCI). 10(2), 37-53. DOI: 10.4018/IJOCI.2020040103

Nance, K., Armstrong, H., & Armstrong, C. (2010). Digital forensics: Defining an education agenda, in Proceedings 43rd Hawaii hit. Conf. Syst. Sci., 1-10.

Parkash Soni, V., Williams, A., Garg, L., Savaglio, C. & Bawa, S. (2021). Cloud and Edge Computing-Based Computer Forensics: Challenges and Open Problems. *Electronics*. 10(11), DOI: 10. 10.3390/electronics10111229.

Pato, J.N., & Millett, L.I. (2010). Biometric Recognition: Challenges and Opportunities. National Academies Press, Washington, USA

Pawlaszczyk, D. (2022). Mobile Forensics – The End of a Golden Age? *J Forensic Sci & Criminal Invest,* 15(4): JFSCI.MS.ID.555917 DOI: 10.19080/JFSCI.2022.15.555917

Poston, H. (2021) Popular computer forensics top 19 tools, Available at https://resources.infosecinstitute.com/topic/computer-forensics-tools/

Purnaye, P. & Kulkarni, V. (2021). A comprehensive study of cloud forensics, Arch. Comput. Methods Eng., 29(1):1-14

RTS (2020), Sajber kriminalci sve češće i efikasnije napadaju, važno je reagovati u pravom momentu, https://www.rts.rs/page/stories/sr/story/125/drustvo/4685336/branko-stamenkovic-sajber-kriminal-u-porastu-gradjani-privreda.html

Saini, M. & Kapoor, A.K. (2016). Biometrics in Forensic Identification: Applications and Challenges. *J Forensic Med*, 1(108). DOI: 10.4172/2472-1026.1000108

Shavam, K. (2020). Cloud forensics, Available at https://kumarshivam-66534.medium.com/cloud-forensics-be18e14230de

Soni, V., Garg, L., Bawa, S., & Mercieca, T. (2019). Big data analytics on cloud environment: advantages, limitations and issues. Available at https://www.researchgate.net/publication/338116587_BIG_DATA_ANALYTICS_ON_CLOUD_ENVIRONMENTADVANTAGES_LIMITATIONS_AND_ISSUES

Spellman, A.B., Eldridge, H. & Bieber, P. (2022). Challenges to reasoning in forensic science decisions, Forensic Science International: Synergy, 4, 100-200, https://doi.org/10.1016/j.fsisyn.2021.100200.

Sree, T. R., & Bhanu, S. M. S. (2020). Data Collection Techniques for Forensic Investigation in Cloud. In B. S. K. Shetty, & P. S. H (Eds.), Digital Forensic Science. IntechOpen. https://doi.org/10.5772/intechopen.82013

Stojičić, S., Radovanović, R., Petrović, N., & Srećkoivć, M. (2022). Forensic method for person identification: yesterday, today, tomorrow, Proceedings ETRAN Conference 2022, Novi Pazar, in Serbian

Tanweer, A. (2018). A Reliable Communication Framework and Its Use in Internet of Things (IoT). *Int J S Res CSE & IT*. 2018 May-June; 3(5): 450-456

Trenwith, M.P. & Venter S.H. (2013). Digital Forensic Readiness in the Cloud, 2013 Information Security for South Africa (ISSA 2013) Conference, DOI: 10.1109/ISSA.2013.6641055

Vaishnav, L. (2020). Biometrics - Tool For Identification In Forensic Science, Biometrics - Tool for Identification in Forensic Science (sifs.in) Avaliable at https://www.sifs.in/blog-details/biometrics---tool-for-identification-in-forensic-science/46

Weston, P., & Wolthusen, D.S. (2013). Forensic Entropy Analysis of Microsoft Windows Storage Volumes, 2013 Information Security for South Africa (ISSA 2013) Conference

Yaacoub, A.J., Noura, H., Salman, O. & Chehab, A. (2021). Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations. https://doi.org/10.48550/arXiv.2103.17028

Yadav, J. (2017). The impact of digital Forensics in future. Conference – INCON-RIT 2017 on "Digitalization : Impact on Indian Society"

Zawoad, S. & Hasan, R. (2013). Cloud Forensics: A meta-study of challenges, approaches, and open problems. https://doi.org/10.48550/arXiv.1302.6312