DIGITAL FORENSICS TOOLS: DEVELOPMENT AND CONCERNS IN THE CONTEXT OF LAW ENFORCEMENT

FERRAMENTAS DIGITAIS FORENSES: DESENVOLVIMENTO E QUESTÕES NO CONTEXTO DA APLICAÇÃO DA LEI

José Ricardo Marcondes Ramos

Doutorando em ciências jurídico-criminais na Universidade de Coimbra. Mestre em Direito Penal e Graduado em Direito pela USP. Pós-graduado pelo Instituto de Direito Bancário, da Bolsa e dos Seguros. Investigador do Instituto Jurídico da Universidade de Coimbra. Advogado.

Link lattes: http://lattes.cnpq.br/4773621753817164

ORCID: https://orcid.org/0000-0002-2092-2665

jricardo.marcondes@gmail.com

Abstract: Despite its use for criminal misbehaviour, technology is contributing to the improvement of both old and new investigative methods. Combined with the rising incidence of cybercrime, the increasing adoption of new digital devices by society and the enormous amount of digital data produced by them is fostering the development of the new and independent scientific field of digital forensics, specialized on the production, collection and analysis of such data and other computer powered investigative tasks. In this paper, we will focus on forensic investigation methods and digital forensic tools aided by new technologies with an overview of the forensic science and the development of tools and investigative methods powered by computers, as well as the usage and purposes of digital forensic tools.

Keywords: Criminal law – Forensic tools – Digital investigation – Law enforcement.

Resumo: Apesar de seu uso para o desvio de comportamento criminoso, a tecnologia vem contribuindo para o aprimoramento de métodos investigativos antigos e novos. Combinado com a crescente incidência de crimes cibernéticos, a crescente adoção de novos dispositivos digitais pela sociedade e a enorme quantidade de dados digitais produzidos por eles está fomentando o desenvolvimento de um campo científico novo e independente de investigação forense digital, especializado na produção, coleta e análise desses dados e outras tarefas de investigação computadorizadas. Neste artigo, temos como foco os métodos de investigação forense e as ferramentas forenses digitais auxiliadas por novas tecnologias com uma visão geral da ciência forense e o desenvolvimento de ferramentas e métodos investigativos alimentados por computadores, bem como o uso e propósitos de ferramentas forenses digitais.

Palavras-chave: Direito Penal – Ferramentas forenses – Investigação digital – Aplicação da lei.

1. Introduction

Led by the development of new technologies, ranging from autonomous vehicles to all sorts of smart gadgets, the digital transformation of society is changing many aspects of life and introducing new ways of social interaction.[1] While new technologies are facilitating several forms of life interaction, they are also being used to leverage both old and new criminal behaviours, aiding the commitment of different forms of fraud, money laundering and other underground criminal activity, either by tampering or meddling technical and technological mechanisms or by smoothing social engineering schemes in order to exploit personal weaknesses and enable fraud (NIKKEL, 2020, p. 01-02).

If technology may help the commitment of crimes, it is also evolving to help new investigation methods (LOUWERS, 2015, p. 06): on one hand, the growing essentiality of digital gadgets led to the development of a whole new field of digital forensics, which is specialized in the extraction and analysis of data produced, stored and processed within devices (VAN BAAR *et al*, 2014, p. 54). On the other hand, the improvement of capacity of data extraction and analysis enabled by new technological advances is helping to upgrade crime-related forensic methods in diverse areas such as forensic accounting, handwriting analysis and neurocriminology (LOUWERS, 2015, p. 07-08).

In this paper, we will focus on forensic investigation methods and digital forensic tools aided by new technologies. In order to do so, our analysis will begin with an overview of the forensic science and the development of tools and investigative methods powered by computers, as well as the usage and purposes of digital forensic tools. The following part will be dedicated to the analysis of both

legal and procedural concerns related to the application of forensic techniques in the context of law enforcement, examining issues regarding the reliability of the digital forensic tools, the soundness of the investigative process and the fulfilment of the principles of security, privacy and transparency along all steps of data collection, examination, analysis and reporting, and the respect to the principle of equality of arms to all digital evidence.

2. From forensic science to digital forensics

Because of the difficulty to unveil the circumstances in which a crime may have occurred and the reliance on confessions or witnesses testimony to identify the offender, the field of forensic science developed a series of techniques and methods to aid the investigative process by acquiring, analysing and interpreting evidence through a coordinated process in order to base scientifically investigative conclusions (V. RAJIČ *et al*, 2020, p. 2094). Ever since the introduction of the fingerprinting method, the first significant investigation technique, forensic science developed a series of scientific processes to assist investigators identify and enquire information and objects related to a crime scene (a mute witness of the crime) and collect relevant evidence such as stains, hair or DNA samples, soil and so on (V. RAJIČ *et al*, 2020, p. 2094).

The development of new applied research and new technologies helped forensics science to improve its methods as well as to advance its techniques for interviewing and interrogation, handwriting analysis, data analysis and others (LOUWERS, 2015, p. 07; WU *et al*, 2020, p. 04). For instance, regarding the interviewing and interrogation processes, currently techniques use neurocriminology instruments, which can identify if someone is lying or telling the truth based on areas of the brain displayed as active when the person is confronted with evidences of the crime (neural mapping), instead of the old lie-detection techniques previously based on alterations in breathing, blood pressure, pulse rate and sweat, measured by the polygraph (LOUWERS, 2015, p. 07-08). Similarly, handwriting analysis, which used to be made personally by experts, is now made by algorithms that examine pen pressure, letter dimensions and other features (LOUWERS, 2015, p. 07). Finally, the emergence of new data processing capacities, arising from the development of data mining and data analysis techniques,[2] is improving the fight against corporate fraud and money laundering, throughout statistical tools for fraud detection, as well as against corruption, using word mapping software to identify bribery-related terms (BOLTON et al, 2002, p. 236; LOUWERS, 2015, p. 08).

Although various tools for forensic investigation and its techniques are not actually new – e.g., the polygraph machine was created around the 1880s (idem, p. 07) – it was only by the end of the 20th century that the use of computers to perform investigative tasks contributed to the development of the digital forensics field (V. RAJIČ, 2020, p. 2094-2095; FERGUSON *et al*, 2020, p. 259;). In spite of the enhanced performance to undertake forensic tasks such as hair or DNA analysis, however, it was only with the adoption of new digital devices and the rising incidence of cybercrime that the digital forensics field was highly developed (Idem).

Even recognizing that the increasing use of new communication devices and informational technologies is fostering new investigative techniques and data sources for old crimes – as the remarkable example of the usage of information from the Apple Watch app to investigate and unveil the disappearance and assassination of Saudi dissident Jamal Khashoggi in Turkey (FERGUSON et al, 2020, p. 259; LEE, SOH, 2020, p. 01) – it is important do recognize that the development of digital forensics as a new and independent field,[3] specialized in the understanding of how this data is produced and how it can be collected and analysed, is being fostered by the enormous amount of digital data increasingly produced by new digital devices (VAN BEEK *et al*, 2020, p. 01-02; VAN BAAR *et al*, 2014, p. 54).

As a branch of forensic science, digital forensics is responsible for the process of identification, collection, processing and interpretation of digital data from any given device (V. RAJIČ, 2020, p. 2095; LEE, SOH, 2020, p. 01, 04) and, as such, can be understood as "the process of applying scientific methods to analyze stored information and to determine the events of a particular incident, thus making evidence usable in court" (OLIVEIRA JÚNIOR *et al*, 2020, p. 01). It must de mentioned, though, that digital investigation's appliance is not restricted to judicial controversies, also being commonly used in the corporate ecosystem as a preventive and investigative tool related to behavioral and disciplinary concerns (FERGUSON *et al*, 2020, p. 262; V. RAJIČ *et al*, 2020, p. 2097). However, even though digital forensics has several applications within the legal frameworks – namely, public sector operation and security as well as corporate investigations – it is important to recall that the "main purpose of digital evidence is to support or rebut a thesis or argument on which court decision is based on" (Idem, p. 2096). As a consequence, and considering that its main application is associated with criminal investigations, there are operational and legal concerns related to digital investigations, topic that we shall address next.

3. Legal and procedural concerns regarding digital investigation processes

From a procedural and legal point of view, as any sort of investigation, the application of digital forensics techniques in the context of law enforcement is limited by a series of concerns stemming from broad investigative limitations and specific procedures precautions (FERGUSON *et al*, 2020, p. 260; WU *et al*, 2020, p. 08). In order to guarantee that the digital evidence used to understand and reconstruct the criminal activity is both legal and valid, there are several issues that must be addressed, ranging from the reliability of the digital forensic analysis tool to the forensic soundness of the whole process used to gather the evidences, as well as the respect to legal constrains and privacy affairs, the fulfilment of demands from diverse stakeholders and the respect to the principle of equality of arms to all digital evidence (VAN BEEK *et al*, 2020, p. 01 and 05; FERGUSON *et al*, 2020, p. 262-263).

Within the context of digital forensic analysis, the initial concern is to ensure that the tool used in the process of data collection, analysis and report is both reliable and suited for the task and for the associated data source from which digital material is extracted – be it a software, a hardware or a combination of both (V. RAJIČ *et al*, 2020, p. 2095; WU *et al*, 2020, p. 04; Netherlands Register of Court Experts, 2016, p. 06). By being very technical in nature,[4] the investigation of crimes and felonies involving different sorts of technologies imply different types of analysis of hardware, software systems, malware, network protocols, APIs and cryptography (NIKKEL, 2020, p. 06). Even though there are different criteria to classify digital forensics tools, the diversity of data sources and the need for expertise on the underlying technology is the base for its taxonomy, which separates the digital forensics in different subfields such as computer forensics,

software forensics, multimedia forensics,[5] device forensics, network forensics, malware forensics and memory forensics, as shown in Figure 1.

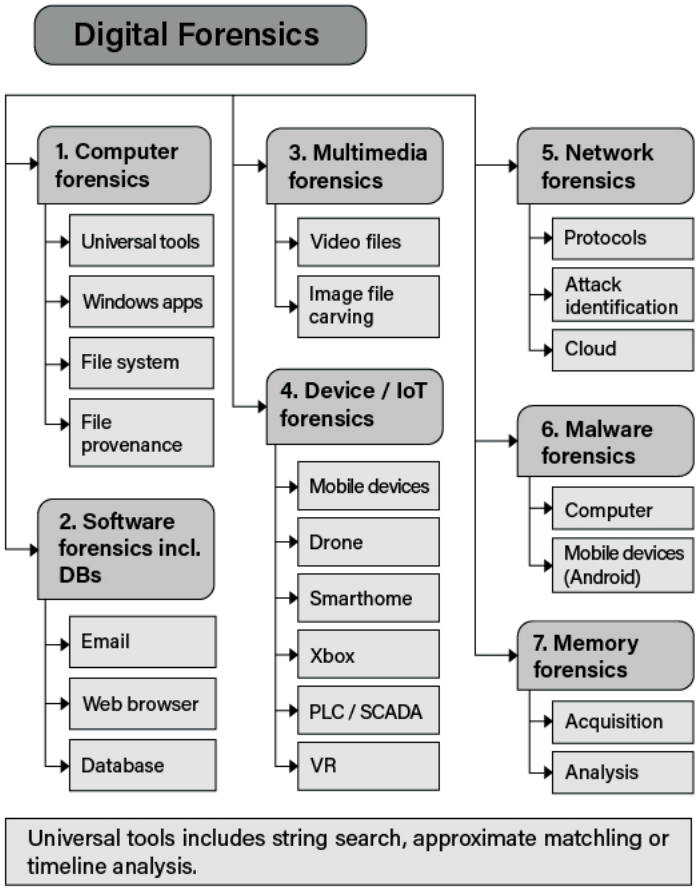

Fig. 1. Digital forensics tool taxonomy.

Source: Wu, Tina; Breitinger, Frank; O'Shaughnessy, Stephen (2020). Digital forensic tools: Recent advances and enhancing the status quo. *Forensic Science International: Digital Investigation*, 34, p. 05.

As all digital forensic tools[6] share the common goals of making the digital evidence available to investigators as quickly possible, maximizing coverage of seized material and providing "a service that processes high volumes of digital material in a forensic context and gives easy and secure access to the results" (VAN BEEK *et al*, 2020, p. 01), the validity of the tool itself is tested by the satisfaction of the Daubert standard.[7] Arising from a rule of evidence which establishes the admissibility of the testimony of expert witnesses, the Daubert test requires that the tool and its underlying methodology should be subjected to peer review, should disclosure its known error rate and should be kept updated (FERGUSON *et al*, 2020, p. 260). It should, in short, answer to the following questions: can and has the procedure been tested? Is there a known error rate of the procedure? Has the procedure been published and subject to peer review? Is the procedure generally accepted in the relevant scientific community? (WU *et al*, 2020, p. 02).

A second scope of challenges for digital forensics is related to the access of devices associated to criminal behaviour by investigators, when there could be legal and technical problems related to privacy concerns (FERGUSON *et al*, 2020, p. 261). Under the legal standpoint, the access to digital devices to undertake investigative actions is constrained by law which, to protect individual freedoms and rights, requires judicial approval and overview of surveillance activities and data confidentiality breakage (idem, p. 263). From the technical perspective, on the other hand, the rising awareness regarding the vulnerability of devices is leading to the increasing adoption of built-in privacy and security systems, creating a scenario where while the use of add-on privacy-respecting tools is impairing hackers' malicious intent, it is also hampering official investigations (idem, p. 262-263).

Once investigators managed to have access to the digital devices at stake, a third source of issues arises from the forensic process itself. Because one of the main concerns of the investigative process is to acquire unbiased evidence related to the criminal activity, the soundness of both the investigative process and whole chain of data custody are essential for the digital evidence to be considered reliable and, as such, be accepted in court (V. RAJIČ *et al*, 2020, p. 2095-2096). In order to do so, the digital forensic investigation methodology applied must fulfil the principles of security, privacy and transparency along all steps of data collection, examination, analysis and reporting, assuring, first, that the extraction process was not subject to contamination, that the evidence was carefully handled and "documented from the moment when identified, acquired, processed, interpreted and presented in the court" (V. RAJIČ *et al*, 2020, p. 2095) in a trustworthy chain of custody and, finally, that the digital evidence traces to the original material, guaranteeing the provenance of traces with a clear chain of evidence (VAN BEEK *et al*, 2020, p. 05). As described by Van Baar *et al* (2014, p. 58), the digital forensic investigation process usually adopt the following path (Figure 2):

> the first task is to create forensic copies of the digital devices (*collection and authentication*). ... images are copied to a central storage, processed (*examined*) using a standard set of tools, ranging from tools that extract file systems, files and carve unallocated space, to tools that parse chat logs, Internet history and mail databases. The results of these tools are stored (*harvested*) in a centralized database. After storing these traces, they can be queried (*reduced* and *analyzed*) using multiple methods. ... This makes it possible to *identify*, *classify*, *organize* and *compare* the traces within seconds, based on *hypotheses* and questions the investigators have. This can be done at any time during the investigation.

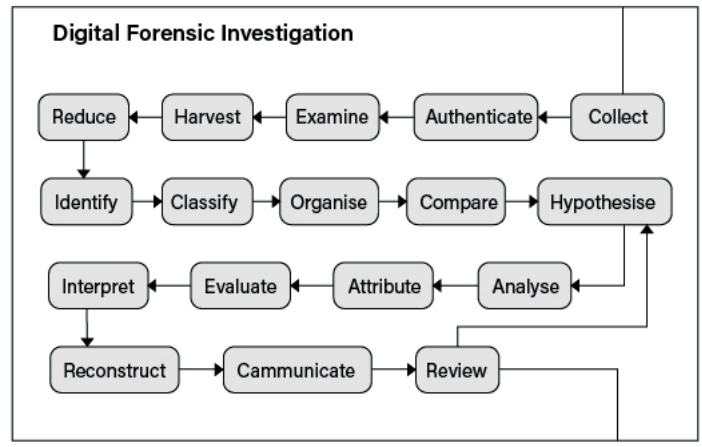

Fig. 2 Digital forensic investigation process.

Source: van Baar, R.B.; Van Beek, H.M.A.; van Eijk, E.J., Digital Forensics as a Service: A game changer. *Digital Investigation*, 2014, 11, p. 58.

Alongside the soundness and transparency of the whole digital forensics investigation process, there is still another challenge faced by the forensic investigator, namely, the scope of the investigation. As a result of privacy concerns, there are several digital traces out of investigator's reach, such as communications between the defendant and his/her lawyers and data outside the express boundaries of the judicial approval (VAN BEEK *et al*, 2020, p. 05). Aiming to overcome these challenges, the process of data collection is usually guided by *white list* traces that determine which data can be included in the investigation. Considering that it is not always possible to seize solely legitimate materials, it is possible to apply other filters restricting the trace collection, such as *black list* traces that exclude from the trace collection elements that are not allowed to integrate the investigation (for example, privileged communication regarding medical or legal files), creating a so called *partial clone* to which investigators are authorized to access (idem, p. 05). Obviously, it is clear that these solutions may not be perfect and that there will eventually be false positives as well as false negatives.

Finally, the last legal concern associated to forensic investigation lies on the use of the digital evidence within legal procedures and the fulfilment of demands from its stakeholders, which include not only case investigators and case analysts but also lawyers, prosecutors and judges (idem, p. 01). Here, the main issue is the assessment of the digital evidence in court and the possibility to access it for evaluation and investigation purposes, allowing it to be contradict within the legal procedure, in respect to the principle of equality of arms to all digital evidence (idem, p. 08). As Van Beek *et al* (2020, p. 08) advocate, this demand may be answered by "giving defense attorneys/suspects direct access to digital evidence via DFaaS [Digital Forensics as a Service] implementations", although such access might be limited depending on the content of the material and the type and context of the case.

4. Conclusions

As a branch of forensic science, the application of digital forensic techniques for law enforcement goals is limited by concerns and issues related to the reliability of the digital forensic analysis tool, the forensic soundness of the investigative process, the respect to legal constrains and privacy affairs and the fulfilment of the principle of equality of arms to all digital evidence. While the reliability of the forensic tool can be assured by the satisfaction of the Daubert standard, legal issues can be complied by the respect to the legal constrains that protect individual freedoms and rights. Under the procedural standpoint, the forensic soundness of the investigative process can be assured by a trustworthy chain of custody and of evidence guided by *white* and *black list* traces, which guarantee the respect to the principles of security, privacy and transparency along. Finally, the respect to the principle of equality of arms can be fulfilled by assuring that all stakeholders have direct access to the digital evidence during legal procedures.

Notas

[1] Revisão aos cuidados do autor.

[2] The attribute that distinguishes both techniques is that unlike data analysis, data mining does not test a previously set hypothesis. As Sunder Gee describe, "data mining is the searching of large amounts of computerized data to find trends, patterns, or relationships without testing a hypothesis" and "data analytics starts with a hypothesis that is to be confirmed or proven to be false. A conclusion is made based on inference from the findings". Gee, 2015, p. 10-11.

[3] As Ferguson *et al* (2020, p. 260) explain "the field of digital forensics, though relatively young, has earned the right to call itself a discipline, and that law enforcement and educational institutions are developing training to ensure that effective investigations can indeed be carried out in the digital world to support law enforcement".

[4] As Bruce Nikkel (2020, p. 03-05) explains, considering solely financial frauds, there are many kinds of criminal activities exploiting different technological bases such, as ATMs or card payment attacks, phishing, rogue mobile banking apps, online banking trojans, online money laundering, extortion and ransom attacks, online social engineering attacks, among others. Just as the crime could be committed throughout different technological means, so must the investigative vary.

[5] This taxonomy is proposed by Tina Wu *et al* (2020) as an updated version of the distinction made by the Netherlands Register of Court Experts (NRGD, 2016. Standards 008.0 Digital Forensics. Technical Report Netherlands Register of Court Experts, p. 08). As the authors describe, their version has two central differences: first, "due to the lack of available database forensic tools", the data bases subfield is placed under the software category; and, second, the taxonomy was extended to include the categories of malware and memory forensics. Wu *et al*, 2020, p. 04.

[6] As mentioned by Lee and Soh (2020, p. 02-03), there are several integrated digital forensic tools available in the market, such as EnCase, the FTK (Forensic Tool Kit), the Forensic Explorer, the X-Ways Forensics and the BlackLight, to name a fill.
The other tool that is worth mentioning, the Hansken platform from the Netherlands Forensic Institute, is analysed in detail in van Beek, H.M.A.; van den Bos, J.; Boztas, A.; van Eijk, E. J.; Schramp, R.; Ugen, M. Digital forensics as a service: Stepping up the game. *Forensic Science International: Digital Investigation*, Volume 35, 2020.

[7] Despite of the lack of international standard certification for forensic tools, the ISO 17025 is applied as an international standard to certify laboratories that develop such tools. van Beek *et al*, 2020, p. 08. As Tina Wu *et al* (2020) describe, "Sec. 7.2.2 of ISO 17025 requires that the laboratory validate non-standard methods to the necessary extent to meet the needs of the given application or field of application. Validation requires that the laboratory implement robust testing methods through variation of controlled parameters, comparison of results achieved with other validated tools and inter- laboratory comparisons. Furthermore ISO 17025 Sec. 7.7 requires that laboratories have procedures for ensuring and monitoring the validity of their results".

Referências

Bolton, R. J., Hand, D. J., Provost, F., Breiman, L., Statistical Fraud Detection – A Review, Statistical Science, Vol. 17, No. 3 (2002), Institute of Mathematical Statistics, p. 235-249.

Ferguson, R.I., Renaud, K., Wilford, S. and Irons, A. PRECEPT: a framework for ethical digital forensics investigations, *Journal of Intellectual Capital*, 2020, Vol. 21 No. 2, p. 257-290.

Gee, Sunder. *Fraud and fraud detection: a data analytics approach*. New Jersey: Ed. Wiley, 2015.

Kumari Tiwari, Reshma; Debnath, Jasojit (2017). Forensic accounting: a blend of knowledge. Journal of Financial Regulation and Compliance, 25(1), 73–85.

Lee, Jae-Ung; Soh, Woo-Young. Comparative analysis on integrated digital forensic tools for digital forensic investigation. *IOP Conference Series: Materials Science and Engineering*, 2020, 834.

Louwers, Timothy J. (2015). The past, present, and future (?) of crime-related forensic accounting methodology. Accounting Research Journal, 28(1), 4–9.

Netherlands Register of Court Experts NRGD, 2016. Standards 008.0 Digital Forensics. Technical Report Netherlands Register of Court Experts.

Nikkel, Bruce. Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, (2020).

Oliveira Júnior, Edson; Zorzo, Avelino F.; Neu, Charles Varlei (2020). Towards a conceptual model for promoting digital forensics experiments. *Forensic Science International: Digital Investigation*, 35.

V. Rajič, M. Milenković and G. Vojković. Digital forensics appliance in corporate ecosystem considering limitations in the EU legal framework, 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), 2020, p. 2094-2100.

van Baar, R.B.; van Beek, H.M.A.; van Eijk, E.J. (2014). Digital Forensics as a Service: A game changer. Digital Investigation, 11, S54–S62.

van Beek, H.M.A.; van den Bos, J.; Boztas, A.; van Eijk, E. J.; Schramp, R.; Ugen, M. Digital forensics as a service: Stepping up the game. *Forensic Science International: Digital Investigation*, Vol. 35, 2020.

Wu, Tina; Breitinger, Frank; O'Shaughnessy, Stephen (2020). Digital forensic tools: Recent advances and enhancing the status quo. *Forensic Science International: Digital Investigation*, 34.

Recebido em: 30.06.2022 - Aprovado em: 05.09.2022 - Versão final: 11.10.2022