DOI: 10.18254/S278229070031781-5 Original paper

The Authentication of Digital Evidence in Criminal Justice: The Latin and Anglo-Saxon Criminal Law Perspective

©2024 Abdulkareem Fahil[a]

[a] Duhok Polytechnic University, Iraq
Fahil.abdulbasit@dpu.edu.krd

Abstract. The emergence of the internet and the widespread use of information systems have led to new challenges for criminal law, both in terms of substance and procedure. Digital evidence has numerous advantages, being scientific evidence that is difficult to dispose of and can be replicated. When it comes to the probative value of this evidence, the criminal judge has significant powers in evaluating digital evidence. For digital evidence to be accepted in court, three conditions must be met: legitimacy of evidence, judge's certainty, and discussion of evidence. The authority of the judge to accept digital evidence depends on the legal system. There are two main legal systems: the Latin system, known as the system of free evidence, and the Anglo-Saxon system, known as the system of restricted evidence.

Keywords: digital forensic evidence, criminal justice, algorithmic criminology, democracy of justice, Iraqi criminal justice system

For citation: Fahil A. 2024. The Authentication of Digital Evidence in Criminal Justice: The Latin and Anglo-Saxon Criminal Law Perspective. *Law & Digital Technologies 4(1): 9—14.*

INTRODUCTION

Forensic evidence is the core of proof and a means of attributing or denying a criminal incident to the defendant. Therefore, it is important at all stages of the trial and through it, the truth is known. Forensic evidence is aimed at proof, and this is defined as the proof of a legally significant fact to the authorities responsible for criminal proceedings using the methods provided by law following the regulations to which it is subject.

Scientific and technological progress has given rise to the information system, with its databases, programs and information, which has reached a large proportion of people in the form of information networks and the undeniable benefits they bring to all cultural, scientific and political levels. On the other hand, it has also opened up a space for considerable risks, as the information system has become a place and a means for committing information crimes (cybercrimes).

For traditional forensic evidence to be accepted in court, it must be specific, direct, and probative to prove the incident. Similarly, digital evidence must meet specific criteria to be accepted in court. This raises the question: What is meant by digital evidence, and what authenticity does it have in Latin and Anglo-Saxon criminal justice systems?

DEFINITION OF DIGITAL EVEDENCE

Definitions of digital forensic evidence have varied between broadening its concept and narrowing it. The Conference of International Investigators defined it as "information and data of potential value to an investigation that is stored or transmitted in digital form. Digital evidence differs from traditional evidence in multiple ways:

a) It is often highly complex, frequently scattered among different physical or virtual locations, and requires expertise and tools to collect.
b) It can easily be altered, accidentally or intentionally, possibly without leaving any trace.
c) It can easily be copied and distributed, presenting challenges to preserving confidentiality.
d) It can be temporary in nature: network logs, Internet browsing history, social media posts, instant messages, cached data and deleted data can be lost if not preserved in a timely manner (CII 2021)".

Digital evidence can be described as information retrieved from computers in the form of magnetic or electrical files or pulses. This data can be collected and analysed using specialised programs, applications, and technology. The findings can then be presented as evidence that is admissible in court. According to Horsman (2023), "Information that originates in the digital world and can be used as evidenc, in a court of law in the form of physical extracts or documentation can be referred to as digital evidence".

CHARACTERISTICS OF DIGITAL EVIDENCE

Digital evidence has many advantages over traditional forensic evidence. It is a type of scientific evidence that is invisible and difficult to dispose of. This evidence can be easily retrieved with a high degree of accuracy (Stoykova 2023). Additionally, digital evidence can be characterised by several features, including those listed below:

a) Invisible evidence refers to data and information in an intangible electronic form (Morelato et al. 2023), which is realised using computer hardware and software systems.

b) Digital evidence is scientific evidence, which means it must adhere to scientific rules. In comparative judiciary, the law seeks justice while science seeks the truth.

c) The evidence in digital form is technical in nature. As technology produces digital pulses, its value lies in the ability to work with the hardware components of the computer (Forte 2003). This data is dynamic, high-speed, and transmitted from one location to another through communication networks.

d) Reproducibility or copying of digital evidence, is a crucial feature that reduces the risk of damaging the original evidence (Choi and Yang 2021). This is because the process of copying is identical to the method of creation, which creates an effective guarantee for preserving the evidence from loss and damage by utilising exact copies of the evidence.

e) Digital evidence is difficult to remove as retrieval programs can recover it even after an order is issued to delete it.

THE COMMON TYPES OF DIGITAL EVIDENCE

1. Digital messages

Written communications between two or more parties have been considered among the most reliable pieces of evidence in the history of law. These communications not only help investigators gain new insights into a crime, but also define relationships between suspects, validate statements, and establish a timeline of events (Sokol et al. 2023). Investigators cannot disregard the source of a digital message, despite their primary interest in its content. A vast range of communication methods may be submitted as evidence in our digital age, including text messages that can be sent through smartphones, social media platforms, instant messaging software, and emails. In addition, digital memos and documents can also serve as communication.

2. Browser and search history

It is a known fact that people spend more than six hours per day on the Internet[1]. This makes browsers a valuable source of evidence for investigators. Every search and website visit leaves a trail that can be followed, and browsing history usually provides the easiest path. Some people may clear their browsing history to protect their privacy, but there are still ways to obtain this information. For instance, several websites and platforms, such as Google, store search history data for each user under their account. A warrant can be obtained data, which can provide a significant amount of information to support an investigation or be used as evidence in a trial.

3. Digital photographs and video footage

Digital images and videos are crucial pieces of evidence in criminal trials. However, this type of evidence is easily manipulated, and people may not be aware that they are doing it. Simple actions such as playing the video with the wrong software, compressing the video to share, or converting the files to a playable format can alter their contents (Pedapudi and Vadlamani 2023). Therefore, agencies and law firms need to follow the correct procedures for acquiring, storing, and presenting evidence.

1 https://www.statista.com/statistics/1258232/daily-time-spent-online-worldwide/

Agencies must obtain and examine original, unmodified digital files as evidence. The sources of evidence generated and stored by law enforcement, such as body-worn and dashboard cameras are particularly valuable as they are under complete oversight. However, third-party sources (Holt and Dolliver 2021), such as digital video files, CCTV cameras, and smartphone camera photographs, must be gathered, stored, and analysed using forensically sound procedures. This ensures that they can be presented objectively in a courtroom (Dolliver et al. 2017).

4. Log files

Computer software typically generates activity logs that document various processes and errors, from operating system functions to video game glitches. Although these logs are primarily intended for maintenance purposes (Dolliver et al. 2017), they can also serve as evidence to confirm the activities of specific individuals or reveal additional information for investigators. The contents and location of each log file can vary depending on the software (Cheng et al. 2021). However, some common examples of digital evidence that are utilised include:

a) Phone logs: Smartphones keep comprehensive records of daily activities, including call frequency and location data. They can also confirm the time a photo or video was captured (Domingues et al. 2021);
b) IP logs: IP addresses are used to identify devices and users accessing a website, and their physical location can be determined using IP logs (Sokol et al. 2020);
c) Transaction logs: These logs are used to track changes made to files, enabling administrators to revert to a previous state. These logs are commonly utilised by servers, databases, and cloud-based document processors such as Google Docs (Choi and Lee 2023);
d) Event logs: Computer software and operating systems maintain event logs to track system activities, identify errors and diagnose crashes. These logs also help to identify whether a human or a computer process triggered a specific event (Khan et al. 2023);
e) Message logs: Most communication software, including messaging and gaming chat, saves conversations for future retrieval (Forte 2004).

THE BASIC CONDITIONS OF DIGITAL EVIDENCE

The criminal judge is obligated to meet three basic conditions in assessing digital evidence as scientific (technological) evidence before the criminal court:

a) The first condition for digital evidence to be considered legitimate is that it must be obtained through legal means within the criminal system. If the procedures used to obtain the digital evidence are not based on a legal basis, they will be invalidated, and the evidence will not be considered legitimate. For example, using physical or moral coercion, or fraudulent methods against the perpetrator, such as deceiving them to reveal their entry code to their system, will make the evidence invalid. The legality of evidence is deemed an essential aspect of the criminal procedure reform movement. Recommendation No. 18 of the Fifteenth International Conference of the International Penal Law Association, held in Brazil in September 1994, states that: "Any evidence obtained by violation of a fundamental right, including any derivative evidence thereof, is invalid and inadmissible with respect to any stage of the procedure" (Fifteenth International Conference 2015). The principle of legitimacy is crucial when investigating digital evidence in both information crimes as well as traditional and hybrid crimes in the digital environment. Any violation of this principle will render the procedure invalid. Additionally, this principle determines the responsibility of law enforcement officers for their actions under the law.
b) The second condition for digital evidence is the judge's level of certainty when convicting an offender. It is constitutionally crucial for a judge to have a high level of certainty, regardless of whether the evidence is traditional, digital, or a combination of both. According to Article 19, paragraph 5 of the Iraqi Constitution of 2005, when there is doubt in a criminal case, it is always interpreted in favour of the accused. To reach a state of certainty in traditional crimes, a judge can scrutinise the evidence, analyse it, and draw a conclusion. However, when it comes to digital crimes, the judge must possess technical knowledge of information matters to determine certainty. Without

sufficient technical knowledge, the judge may have doubts about the digital evidence, which could lead to the release or acquittal of the defendant. Therefore, any defendant in a digital case can benefit from doubts generated by the judge. According to the majority of comparative criminal law experts, computer outputs are considered to have a high level of certainty. This is why the American criminal justice system recognises copies of data extracted from computers as evidence with significant probative value.

c) The third condition for digital evidence is that it should be presented and discussed during court sessions. This means that the evidence must have a legal basis established in the case papers, and the parties involved must be given sufficient opportunity to view and discuss it. This applies to all types of evidence, as stated in article 212 of the Iraqi Criminal Procedure Code 23 of 1971. The discussion of digital evidence follows two fundamental rules. Firstly, the opponents have the right to access and respond to the digital evidence until a legal decision is reached, guaranteed by articles 123 and 124 of the Iraqi Criminal Procedure Code 23 of 1971. This statement emphasises the importance of allowing individuals to have the right to defend themselves and confront the evidence presented against them. Secondly, for the judge's verdict to be legally valid, the evidence must originate from official case documents.

THE JUDGE'S DISCRETION IN THE ADMISSION OF DIGITAL EVIDENCE

The admissibility of digital evidence is at the discretion of the criminal judge and depends on the prevailing evidence system (Bhadu 2021). These systems include the Latin system and the Anglo-Saxon system:

a) The Latin System is a legal framework where the legislature does not specify the evidence and means of proof but rather leaves the judge free to establish their judgment at their discretion without imposing any specific evidence requirements. With the advancement of scientific and digital evidence, judges in this system have to deal with new kinds of evidence to discover crimes. As a result of this principle, the judge is not bound by the evidence presented by the parties to the case because they have the right to independently initiate and take all necessary measures to gather evidence to form their conviction (Tatulych 2020). To obtain digital evidence, the individual in charge, typically the criminal judge, can issue orders to the internet service provider. These orders may require the collection of information related to the websites that the accused person visited, the files and conversations in which they participated, as well as the messages they sent and received. Furthermore, the person in charge may instruct the system operator to provide them with the necessary details to access the system, including passwords and codes for various programs. They may also order an inspection of the computer in question. However, the criminal judge must ensure that any evidence they accept is valid and credible according to the relevant laws before admitting it. Both Algerian and Egyptian legislations, in addition to French legislation, have adopted this system (Oparnica 2016).

b) The Anglo-Saxon System is also known as the system of specific proof or the system of legal evidence. In this system, the legislator determines the evidence in advance and the judge is not allowed to deviate from it. Therefore, if the evidence is available for conditions that were specified and restricted by the legislator, the judge is obligated to establish his ruling even if the judge is not convinced. The evidence in this system is governed by two rules: The first is the rule of excluding hearing testimony, and the second is the rule of best evidence (Bierekoven et al. 2014).

1) The hearsay evidence rule states that testimony cannot be used as evidence if the witness only heard it and did not observe or experience it firsthand. Such testimony is usually collected outside the court and thus excluded from being used as evidence. However, there are some exceptions to this rule, especially when it comes to data and information obtained through a computer. The English judiciary has accepted this type of evidence on numerous occasions. For instance, the case of R v. Wood (1983) (Harvey, 2019) showed that direct evidence produced by a computer is not subject to the hearsay rule and can be accepted as direct testimony.

2) The best evidence rule requires the original writing, recording, or photograph to prove its contents. In the United States, this rule has been approved as part of the Evidence Act (Rule 1002

n.d.), which allows electronic materials to receive the same recognition as other forms of evidence. Furthermore, the American legislation recognizes that electronic writings are equivalent to original documents. This means that copies, such as printouts or other outputs, are considered original if they accurately reflect the data (Rule 1003 n.d.). Therefore, electronic documents do not conflict with the rule of best evidence.

CONCLUSION

Digital evidence is legally highly suitable for use in criminal cases due to its strong probative value, despite being intangible and easily concealed. However, using digital evidence in cases involving multiple countries can present a challenge due to conflicts in jurisdiction. The situation becomes even more complicated when the countries involved have different criminal justice systems, as each country will adhere to its judicial sovereignty. There is a need for technical expertise, especially judges and investigators, in the field of justice due to the digital reality. Additionally, the Iraqi criminal system lacks legislative provisions for investigating digital crimes and handling digital evidence. Our research has focused on identifying the types, characteristics, and basic requirements of digital evidence. It is worth mentioning that the Iraqi criminal legislator has adopted the free evidence system in its penal approach, which is based on the Latin system.

We urge the Iraqi criminal legislature to update its system to accept digital evidence as original and reliable evidence that cannot be challenged except through illicit means (illegitimacy). We also recommend incorporating modern technical requirements into the Iraqi criminal system, specifically by creating a legal mechanism for investigation and collection procedures for analysing digital evidence. This is necessary to prevent digital criminals from acting with impunity.

REFERENCES

1. Bierekoven, C., P. Bazin, and T. Kozlowski. 2014. Electronic Signatures in German, French and Polish Law Perspective. Digital Evidence and Electronic Signature Law Review 1(0). https://doi.org/10.14296/deeslr.v1i0.1719
2. Cheng, C. C.-C., C. Shi, N. Z. Gong, and Y. Guan. 2021. LogExtractor: Extracting digital evidence from android log messages via string and taint analysis. Forensic Science International: Digital Investigation 37: 301193. https://doi.org/10.1016/j.fsidi.2021.301193
3. Choi, H., and S. Lee. 2023. Forensic analysis of SQL server transaction log in unallocated area of file system. Forensic Science International: Digital Investigation 46: 301605. https://doi.org/10.1016/j.fsidi.2023.301605
4. Choi, J. P., and S. Yang. 2021. Investigative journalism and media capture in the digital age. Information Economics and Policy 57: 100942. https://doi.org/10.1016/j.infoecopol.2021.100942
5. Dolliver, D. S., C. Collins, and B. Sams. 2017. Hybrid approaches to digital forensic investigations: A comparative analysis in an institutional context. Digital Investigation 23: 124–137. https://doi.org/10.1016/j.diin.2017.10.005
6. Domingues, P., L. M. Andrade, and M. Frade. 2021. Microsoft's Your Phone environment from a digital forensic perspective. Forensic Science International: Digital Investigation 38: 301177. https://doi.org/10.1016/j.fsidi.2021.301177
7. Fifteenth international congress of penal law (Rio de Janeiro, 4 – 10 September 1994). 2015. Revue internationale de droit penal 86(1-2): 369-390. https://www.cairn.info/revue-internationale-de-droit-penal-2015-1-page-369.htm
8. Forte, D. 2003. Principles of digital evidence collection. Network Security 2003(12): 6–7. https://doi.org/10.1016/s1353-4858(03)00006-0
9. Forte, D. 2004. The importance of text searches in digital forensics. Network Security, 2004(4): 13–15. https://doi.org/10.1016/s1353-4858(04)00067-4
10. Franco, D. 2023. The Importance of Research in Forensic Sciences and Digital Forensics in Contemporary Society. International Journal of Forensic Sciences 8(4): 1–2. https://doi.org/10.23880/ijfsc-16000336
11. Harvey, D. J. 2019. Digital Evidence Admissibility: Some Issues. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3505611
12. Holt, T., and D. S. Dolliver. 2021. Exploring digital evidence recognition among front-line law enforcement officers at fatal crash scenes. Forensic Science International: Digital Investigation 37: 301167. https://doi.org/10.1016/j.fsidi.2021.301167
13. Horsman, G. 2023. Digital evidence strategies for digital forensic science examinations. Science & Justice 63(1): 116–126. https://doi.org/10.1016/j.scijus.2022.11.004
14. Khan, S., S. Parkinson, and C. Murphy. 2023. Context-based irregular activity detection in event logs for forensic investigations: An itemset mining approach. Expert Systems with Applications 233: 120991. https://doi.org/10.1016/j.eswa.2023.120991

15. Makulilo, A. B. 2016. The admissibility of electronic evidence in Tanzania: new rules and case law. Digital Evidence and Electronic Signature Law Review 13. https://doi.org/10.14296/deeslr.v13i0.2302
16. Morelato, M., L. Cadola, M. Bérubé, O. Ribaux, and S. Baechler. 2023. Forensic intelligence teaching and learning in higher education: An international approach. Forensic Science International 344: 111575. https://doi.org/10.1016/j.forsciint.2023.111575
17. Oparnica, G. 2016. Digital evidence and digital forensic education. Digital Evidence and Electronic Signature Law Review, 13. https://doi.org/10.14296/deeslr.v13i0.2305
18. Pedapudi, S. M., and N. Vadlamani. 2023. Digital forensics approach for handling audio and video files. Measurement: Sensors 29: 100860. https://doi.org/10.1016/j.measen.2023.100860
19. Bhadu, P. 2021. Admissibility And Perplexity Of Digital Evidence: An Overview. Legal Research Development 5(IV): 10–20. https://doi.org/10.53724/lrd/v5n4.03
20. Rule 1002. n.d. "Requirement of the Original". https://www.law.cornell.edu/rules/fre/rule_1002
21. Rule 1003. n.d. "Admissibility of Duplicates". https://www.law.cornell.edu/rules/fre/rule_1003
22. Scanlon, M., F. Breitinger, C. Hargreaves, J.-N.Hilgert, and J. Sheppard. 2023. ChatGPT for digital forensic investigation: The good, the bad, and the unknown. Forensic Science International: Digital Investigation 46: 301609. https://doi.org/10.1016/j.fsidi.2023.301609
23. Sokol, P., Ľ. Antoni, O. Krídlo, E. Marková, K. Kováčová, S. Krajči. 2023. Formal concept analysis approach to understand digital evidence relationships. International Journal of Approximate Reasoning 159: 108940. https://doi.org/10.1016/j.ijar.2023.108940
24. Sokol, P., L. Rózenfeldová, K. Lučivjanská, and J. Harašta. 2020. IP Addresses in the Context of Digital Evidence in the Criminal and Civil Case Law of the Slovak Republic. Forensic Science International: Digital Investigation 32: 300918. https://doi.org/10.1016/j.fsidi.2020.300918
25. Stoykova, R. 2023. The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. Computer Law & Security Review 49: 105801. https://doi.org/10.1016/j.clsr.2023.105801
26. Tatulych, I. 2020. Electronic evidence as a means of evidence in civil proceedings. Law Review of Kyiv University of Law 1: 215–219. https://doi.org/10.36695/2219-5521.1.2020.43