A Digital Forensics Approach for Validating Screen Captures in Legal Proceedings

Claudia Greco[1], Michele Ianni[1], Antonella Guzzo[1] and Giancarlo Fortino[1]

[1]*University of Calabria*

Abstract

In today's hyper-digitalized world, digital content often plays a central role in the resolution of legal proceedings. However, its reliability is frequently called into question, as screenshots, recordings, and other forms of digital evidence can be easily manipulated, compromising their integrity, authenticity and admissibility in court. To address this issue, we present a novel framework for certifying the authenticity and integrity of digital content, including screenshots, audio and video recordings, and web interactions. The proposed approach is centered around a modified web browser instance specifically designed to prevent alterations to displayed content, thereby ensuring the integrity of captured material. Users can securely access this browser via a remote interface, enabling them to capture and certify digital content in a controlled and verifiable manner. The certification process integrates several security mechanisms, including metadata collection, digital signatures for certification packages, and encrypted communication protocols to preserve both the integrity and confidentiality of the certified data. By combining server-side and client-side technologies, the proposed framework offers a scalable and robust solution for enhancing the credibility of digital evidence. Ultimately, this approach strengthens the legal admissibility and reliability of digital content in legal proceedings and other domains where data integrity is of paramount importance.

Keywords

Digital Evidence, Content Certification, Legal Admissibility

1. Introduction

The rapid progress in technology has deeply impacted daily life, with digital technologies becoming essential for healthcare, education, commerce, communication, and more. However, increased online activity has also led to a surge in cyber-crimes, including the spread of fake news, cyber-bullying, cyber-stalking, online defamation, creation of fake profiles, revenge porn, and other illicit activities [1, 2, 3]. The effects of these cyber-crimes can be profound, not only on individual victims but also on industries [4, 5] and society as a whole. They erode trust in online communities, perpetuate fear and anxiety, and contribute to a culture of misinformation and distrust.

Addressing cybercrime requires a multidisciplinary approach, integrating legal reforms, technological tools, and public awareness. Digital forensics is especially critical, enabling the collection and analysis of electronic evidence to support legal proceedings [6]. The advent

SEBD 2025: 33rd Symposium on Advanced Database System, June 16-19, 2025 - Ischia, Italy

claudia.greco@unical.it (C. Greco); michele.ianni@unical.it (M. Ianni); antonella.guzzo@unical.it (A. Guzzo); giancarlo.fortino@unical.it (G. Fortino)

0000-0003-4929-2289 (C. Greco); 0000-0003-0562-7462 (M. Ianni); 0000-0003-3159-0536 (A. Guzzo); 0000-0002-4039-891X (G. Fortino)

of artificial intelligence (AI) has further complicated this landscape, as AI technologies are increasingly utilized to automate and enhance cyber-attacks, making them more sophisticated and harder to detect [7, 8]. Forensics and legal systems work synergistically—laws define offenses and consequences, while forensic methods provide the means to enforce them. To be legally admissible, forensic evidence must meet stringent standards. A key issue is the evidentiary value of screenshots, particularly in cases involving social media chats—often the only available proof for victims. Yet, screenshots are easily manipulated and lack inherent reliability, complicating their use in court. Surprisingly, academic literature on the legal admissibility of screenshots is limited. The most relevant study focuses on Ukrainian civil procedures, discussing challenges in identifying perpetrators and the role of electronic signatures [9].

In their analysis, the authors debate the use of screenshots obtained from social networks and the challenges associated with identifying individuals involved in disseminating information. The authors also address the use of electronic digital signatures and their significance in the acceptance of electronic evidence under Ukrainian law.

The literature on forensic analysis of web pages is relatively limited as well, reflecting a narrow focus within the scientific community. On the other hand, several studies address digital forensics in relation to other aspects of the online experience, including web content forensics, web-based communication forensics, and web tracking and privacy forensics, while a few papers in the scientific literature discuss novel proposal to help managing digital crimes [10, 11, 12]. Vidya et al. [13] proposed an automated system designed for the forensic acquisition of websites. The system aims to comprehensively capture all content from live websites, allowing the acquisition of webpages content, such as media and scripts, and the analysis of the acquired data. The acquisition software developed by Vidya et al., however, operates locally, meaning that the security guarantees depend heavily on the trustworthiness and integrity of the individual using the software. This constraint necessitates the involvement of trusted entities such as law enforcement agencies, investigators, or other legal authorities to ensure the credibility of the acquired digital evidence. The need for trusted personnel limits the accessibility and usability of the software to specific professionals and scenarios, potentially delaying the acquisition process.

In this paper, we propose a comprehensive framework for the validation of digital content, such as screenshots, audio and video recordings, and web interactions. Our framework centers on a customized web browser that online users can securely access to capture and authenticate digital content and that prevents the alteration of web content. In order to guarantee the integrity of collected data, the process we present encompasses gathering metadata, digitally signing certification packages, and encrypting communication.

The rest of this paper is organized as follows. Section 2 provides an overview of the laws and standards that regulate the evidential validity within a legal trial of evidence collected through forensic analysis. Additionally, it delves into a technical explanation of the features of digital signatures, which form a crucial component of our proposal. Section 3 explains the reasoning behind our proposal and underscores the pressing need to devise solutions for validating screen captures. Section 4 describes the inner working and the technical implementation of our proposed framework. Finally, in Section 5 we draw conclusions about our findings and discuss future work.

2. Background

Digital evidence in forensic analysis is governed by international conventions, technical standards, and national regulations, which vary across jurisdictions. One of the most relevant international conventions is the Budapest Convention on Cybercrime [14], adopted in 2001 and effective from 2004. It facilitates international cooperation in combating cybercrime and mandates that digital evidence be handled using methods that preserve its originality and prevent alteration, thus maintaining its probative value—i.e., its authenticity, attribution, integrity, and non-repudiation in legal contexts. Complementing this, technical standards from the ISO/IEC define procedures for acquiring, analyzing, and presenting digital evidence. Specifically, the ISO/IEC 27037:2012 [15] outlines best practices for identifying, collecting, acquiring, and preserving digital evidence, offering a technical framework for forensic procedures regardless of legal context. However, national laws significantly influence the legal interpretation and admissibility of digital evidence. One central issue is the legal status of electronic documents. The eIDAS Regulation (EU No. 910/2014) [16], effective since 2016, establishes criteria for electronic identification, authentication, and trust services, including the definition and recognition of electronic documents and digital signatures.

In the forensic context, digital signatures are used to ensure that electronic documents presented as evidence are authentic and unaltered. The validity of digital signatures is established in accordance with the provisions of the eIDAS Regulation and relevant national laws, which set specific requirements for the use and validity of electronic signatures.

2.1. Cryptographic keys

Digital signatures use cryptographic methods to ensure the integrity and authenticity of electronic documents, confirming the content is unchanged and verifying the signer's identity. They are based on asymmetric (public-key) cryptography, which uses a mathematically linked key pair: a private key, known only to the signer, and a public key, which can be shared openly. Data encrypted with one key can only be decrypted with the other. To sign a document, the signer applies their private key to generate a unique digital signature—a string derived via a mathematical algorithm from the document's content.

The use of cryptographic keys within the legal context is motivated by certain inherent properties they present:

Ensuring integrity - To verify the authenticity and integrity of the digital signature, the recipient of the document uses the signer's public key to decrypt the signature. If the resulting decrypted signature matches the document's content, it confirms that the document has not been altered since it was signed and that it was indeed signed by the holder of the corresponding private key.

Establishing Authenticity - Digital signatures ensure the integrity of electronic documents by providing a means to detect any unauthorized alterations. Even a small change in the document's content would result in a completely different digital signature, alerting recipients to the tampering attempt.

Non-repudiation - Digital signatures also provide non-repudiation, meaning that the signer cannot later deny having signed the document. The mathematical link between the signature

and the private key ensures that only the signer could have generated the signature.
Integration with Trusted Certificate Authorities - To further enhance trust in digital signatures, they are often issued and verified by trusted certificate authorities (CAs). These authorities verify the identity of individuals or organizations before issuing digital certificates, which contain the public key and other identifying information. Recipients can then rely on these certificates to validate digital signatures.
Legal Recognition - In many jurisdictions, digital signatures have legal recognition equivalent to handwritten signatures, provided they meet certain criteria outlined in relevant laws and regulations.

3. Motivation

In the digital age, criminal activities such as cyberbullying, cyberstalking, and revenge porn have found a fertile ground within the confines of social network chats. These platforms, originally created to connect people over long distances, have unintentionally become hubs for malicious activities because they are easy to access and provide anonymity. One of the most concerning aspects of these crimes is the ease with which they can be perpetuated, since within the virtual realm of social network chats, perpetrators can operate with relative impunity. This presents a double-edged sword: While victims can collect evidence of the abuse they receive by capturing the chat's content through screenshots, proving the authenticity of an unaltered screenshot can be challenging, making it difficult to use it as valid proof in legal proceedings.

In general, using screenshots as legal evidence poses several problems and challenges that require careful consideration.
Authenticity - One of the primary concerns is the authenticity of screenshots. Since they can be easily manipulated or falsified, it is essential to ensure that a screenshot presented in court is genuine and unaltered.
Chain of Custody - Proper documentation of the chain of custody is crucial to demonstrate that a screenshot has not been tampered with or modified after its initial capture. Without adequate chain of custody documentation, the validity of the screenshot may be called into question.
Relevance and Admissibility - Another issue is the relevance of the screenshot in the context of the legal proceeding. It may be necessary to assess whether the screenshot is pertinent to the matter under discussion and whether it can be effectively used to support a particular argument.
Protection of Personal Data - In some jurisdictions, such as the European Union, there are strict regulations regarding the protection of personal data (e.g., GDPR). This raises concerns about the collection and presentation of screenshots that may contain sensitive or identifiable information.

Jurisdictions around the world propose different solutions to address the problem of validating and authenticating screenshots. In the EU, the use of screenshots as legal evidence is subject to regulations on the protection of personal data, such as the GDPR. In the United States, the Federal Rules of Evidence provide guidelines on the admissibility of digital evidence, including

screenshots. In the UK, laws such as the Civil Evidence Act 1995 and the Criminal Justice Act 2003 regulate the use of digital evidence, including screenshots. Sworn testimony and technical analysis can be used to authenticate screenshots.

Regardless of the individual legislation, the common approach requires the proponent of the evidence to "produce sufficient evidence to support the conclusion that the item is what the proponent claims it to be" [17]. This process, inherently labor-intensive, often becomes long and tedious and leaves the jury with the responsibility of deciding on the true authenticity and probative value of the evidence. Additionally, obtaining testimony of authenticity (e.g., from an institutional authority, a policeman, or a notary) can sometimes become impossible due to the volatile nature of the evidence itself, as digital contents could be removed or become inaccessible. As a result, different courts may reach different conclusions regarding the authenticity of the same piece of evidence. For example, in United States v. Vayner [18], the U.S. Court of Appeals for the Second Circuit reversed a district court's decision to admit screenshots of a social media profile that contained the name, photo, and work history of the defendant. Lawyers offering social media evidence at trial must "over-authenticate" their evidence by laying a foundation that substantially eliminates the possibility that an impostor created the content. While technological evolution brings new challenges, it also offers powerful means of establishing the authenticity of evidence by design. This can ensure that evidence is irrefutable and, above all, fairly presented, thereby enhancing the integrity of the judicial process.

4. Proposal

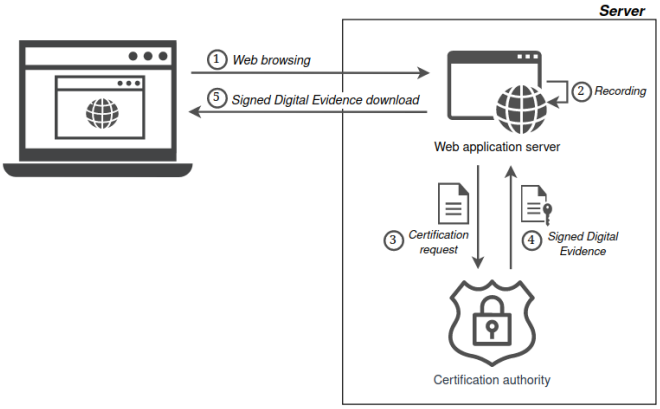

Figure 1: Digital Evidence Certification Process

In this section, we present our framework (Figure 1) for certifying the validity of screenshots and other web interactions. At its core is a Certification Authority (CA), which manages the certification process using a modified web browser designed to block content manipulation. This secure environment ensures captured screenshots and metadata accurately reflect the original web page at the time of capture.

Key components of our framework include:

- *Modified Browser Instance*: Employed by the CA, this browser disables developer tools and prevents content edits, ensuring screenshots remain tamper-proof.
- *Remote Access Interface*: A web application allows users to remotely access the browser, navigate web pages, capture screenshots, and initiate certification.
- *Certification Process*: When a user captures a screenshot, the CA collects metadata—URL, IP address, timestamp, page source, and more—bundling it with the screenshot into a certification package, which is digitally signed.
- *Digital Signatures*: Each package is signed with the CA's private key, enabling authenticity verification via its public key.

The implementation of the proposed framework focuses on the modified browser and remote interface to support secure user interaction and certification. Below, we outline the technical details and key components of our implementation:

Modified Browser Instance In our implementation, we opted to modify the Midori web browser[1]. This decision was made after careful consideration of various browser options, including Chromium and Firefox. Midori was selected for its lightweight nature, open-source architecture, and flexibility, making it well-suited for customization to meet our specific requirements. The modifications to the Midori browser were aimed at enhancing security and preventing users from modifying web content, thus ensuring the integrity of captured screenshots. These modifications include disabling access to developer tools to prevent tampering and restricting the execution of JavaScript code that could alter page content. By leveraging the lightweight and customizable nature of Midori, we were able to tailor the browser to our needs while maintaining compatibility with web standards and protocols. The modified browser is executed through a web-based remote access interface. As shown in Figure 2, the instance of the modified browser is running inside a regular browser as a normal web application. The figure shows a Wikipedia page within the modified Midori browser, and both the page and the modified browser containing it are presented as a web application to the user accessing it via their own browser (Firefox).

Remote Access Interface Our remote access interface uses a web-based frontend as a Remote Desktop Protocol (RDP) client, allowing users to interact with the modified browser on the CA server directly from their browsers, with no need for extra software or plugins. RDP functionality is enabled via JavaScript libraries that convert user input (mouse, keyboard) into RDP commands sent to the backend. A Node.js server handles RDP connections, user authentication, and communication between the frontend and the remote browser. It uses secure WebSocket connections for real-time, bidirectional data exchange between the frontend and backend components. When a user connects to the remote access interface, they are prompted to authenticate themselves using username and password credentials. Optionally,

[1]https://astian.org/midori-browser

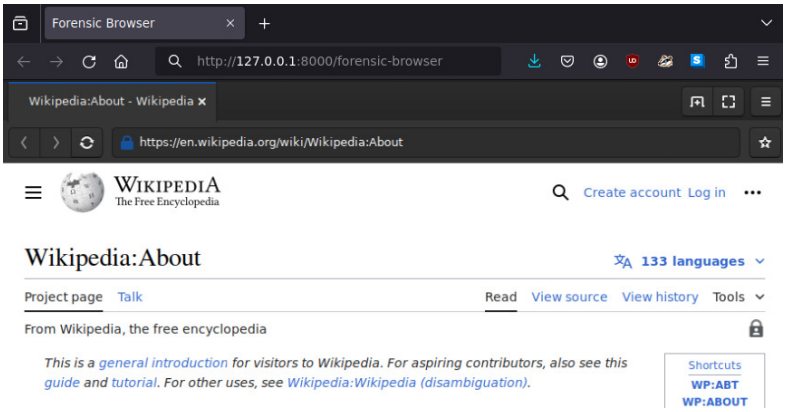

Figure 2: Modified Browser instance running inside a regular browser as a web application

multi-factor authentication mechanisms may be employed to enhance security. Upon successful authentication, the frontend initiates an RDP session through the backend, which connects to the CA's remote browser. During the RDP session, user inputs captured by the frontend interface, such as mouse movements and keyboard inputs, are transmitted to the backend server over the WebSocket connection. The backend server forwards these input events to the remote browser instance, allowing users to interact with the browser environment in real-time. Similarly, graphical output generated by the browser instance, including rendered web pages and captured screenshots, is transmitted back to the frontend interface and displayed to the user within their web browser. To ensure the security and integrity of the remote access interface, we implement encryption mechanisms such as Transport Layer Security (TLS) to encrypt communication between the client and server, protecting sensitive data from interception or tampering.

Certification Process The certification process in our framework ensures the integrity and authenticity of digital content, including screenshots captured via the remote browser instance. It involves several steps to collect metadata, verify content authenticity, and provide cryptographic proof of integrity. When a screenshot is captured, metadata is collected, including the URL, IP address, timestamp, and session/browser info. The framework also supports recording web interactions, allowing multimedia (e.g., audio, video) on the page to be included in the certification. The modified browser then combines the screenshot with the metadata to form a certification package, representing the content and context needed to verify authenticity. Before finalizing the certification package, the browser instance digitally signs the package using the private key of the CA. This digital signature provides cryptographic proof of the CA's approval and serves as a tamper-evident seal, ensuring that the content has not been altered or manipulated since the time of capture. Once signed, the package is returned to the user via the remote access interface, where it can be downloaded and validated using the CA's public key, stored in trusted channels for verification.

Security considerations Cross-Site Scripting (XSS) poses a significant threat to digital evidence, as attackers can inject malicious scripts into web pages to alter content or steal sensitive data [19]. Our framework addresses this with two key mitigations. First, it records all interactions with the web page, including server requests, enabling the detection of any injected JavaScript. This allows security experts to analyze the recorded data or use existing XSS detection systems to identify unauthorized modifications. Second, the framework limits JavaScript execution within the modified browser instance to only essential functions needed for the page's functionality. This minimizes the attack surface for XSS vulnerabilities. Additionally, enforcing strict content security policies restricts where JavaScript code can be loaded from, providing further protection. Together, these measures ensure the integrity and reliability of captured digital evidence.

Case Studies To demonstrate the practical applications and effectiveness of our framework, we present case studies in various contexts. In legal proceedings, it captures and certifies web content as court evidence, ensuring its integrity and authenticity. In digital forensics, it assists investigators by providing tamper-proof evidence from screenshots, video recordings, and web interactions. For online content verification, journalists and fact-checkers can use our framework to authenticate social media posts or news articles, quickly capturing and certifying content to confirm or debunk online claims. In protecting intellectual property, our framework helps capture and certify digital content to address plagiarism or unauthorized use of copyrighted material, providing certified evidence for legal actions. Additionally, in corporate compliance, businesses can use our framework to ensure adherence to digital content regulations, capturing and certifying records of web interactions that demonstrate regulatory compliance, such as with data privacy laws. These case studies showcase the diverse and practical applications of our framework, underscoring its utility in ensuring the integrity and reliability of digital content across various domains.

5. Conclusions

In this paper we presented a framework for content certification [20], which represents a significant step towards enhancing the integrity and authenticity of digital evidence in various contexts, including legal proceedings, investigations, and digital forensics. By leveraging a modified web browser instance and a secure remote access interface, we have provided users with a reliable means of capturing and certifying digital content, including screenshots, audio recordings, video recordings, and web interactions. The certification process, incorporating metadata collection, digital signatures, and encryption mechanisms, ensures the integrity and reliability of certified content, bolstering its admissibility and credibility in legal proceedings and other contexts where integrity is paramount.

Acknowledgement

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] J. Juvonen, E. F. Gross, Extending the school grounds?—bullying experiences in cyberspace, Journal of School health 78 (2008) 496–505.

[2] E. Whittaker, R. M. Kowalski, Cyberbullying via social media, Journal of school violence 14 (2015) 11–29.

[3] J. Peterson, J. Densley, Cyber violence: What do we know and where do we go from here?, Aggression and violent behavior 34 (2017) 193–200.

[4] G. Fortino, C. Greco, A. Guzzo, M. Ianni, Identification and prediction of attacks to industrial control systems using temporal point processes, Journal of Ambient Intelligence and Humanized Computing 14 (2023) 4771–4783.

[5] G. Fortino, C. Greco, A. Guzzo, M. Ianni, Neural network based temporal point processes for attack detection in industrial control systems, in: 2022 IEEE international conference on cyber security and resilience (CSR), IEEE, 2022, pp. 221–226.

[6] S. Raghavan, Digital forensic research: current state of the art, Csi Transactions on ICT 1 (2013) 91–114.

[7] C. Greco, G. Fortino, B. Crispo, K.-K. R. Choo, Ai-enabled iot penetration testing: state-of-the-art and research challenges, Enterprise Information Systems 17 (2023) 2130014.

[8] G. Beltrano, C. Greco, M. Ianni, G. Fortino, Deep learning-based detection of csrf vulnerabilities in web applications, in: 2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), IEEE, 2023, pp. 0916–0920.

[9] N. Golubeva, K. Drogoziuk, Web-page screenshots as an evidence in civil procedure of ukraine, Masaryk University Journal of Law and Technology 13 (2019) 87–114.

[10] S. Sultana, M. Deb, A. Bhattacharjee, S. Hasan, S. R. Alam, T. Chakraborty, P. Roy, S. F. Ahmed, A. Moitra, M. A. Amin, et al., 'unmochon': A tool to combat online sexual harassment over facebook messenger, in: Proceedings of the 2021 CHI conference on human factors in computing systems, 2021, pp. 1–18.

[11] T. Tun, B. Price, A. Bandara, Y. Yu, B. Nuseibeh, Verifiable limited disclosure: reporting and handling digital evidence in police investigations, in: 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW), IEEE, 2016, pp. 102–105.

[12] M. Huber, M. Mulazzani, M. Leithner, S. Schrittwieser, G. Wondracek, E. Weippl, Social snapshots: Digital forensics for online social networks, in: Proceedings of the 27th annual computer security applications conference, 2011, pp. 113–122.

[13] V. Vidya, K. Saly, C. Balan, Forensic acquisition and analysis of webpage, in: 2022 2nd International Conference on Intelligent Technologies (CONIT), 2022, pp. 1–6. doi:10.1109/CONIT55038.2022.9848303.

[14] O. E. COUNCIL, Convention on cybercrime, Budapest, November 23 (2001).

[15] ISO/IEC 27037, 2012. URL: https://www.iso27001security.com/html/27037.html, [Online; accessed 19-February-2025].

[16] EUR-lex, Regulation (eu) no 910/2014 of the european parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec, 2014. Https://eur-lex.europa.eu/eli/reg/2014/910/oj [Accessed: April 12, 2024].

[17] D. C. D. V. W. O. K. G. Clifford C. Histed, Desiree F. Moore, Bot or not? authenticating social media evidence at trial in the age of internet fakery, The National Law Review (2020).

[18] N. Y. S.-F. J. Council, United states v. vayner, 769 f.3d 125, 131 (2d cir. 2014), 2014. The New York State-Federal Judicial Council https://nys-fjc.ca2.uscourts.gov.

[19] J. Grossman, XSS attacks: cross site scripting exploits and defense, Syngress, 2007.

[20] C. Greco, M. Ianni, G. Seminara, A. Guzzo, G. Fortino, A forensic framework for screen capture validation in legal contexts, in: 2024 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE, 2024, pp. 127–132.