Analysis of the Content and Characteristics of WIPO Trusted Digital Evidence Service (Post-print)

Authors: Huang Guobin, Chen Li

Date: 2023-04-01T16:02:53+00:00

Abstract

[Objective/Significance] This study aims to dissect the content and characteristics of the WIPO Trusted Digital Evidence Service and propose feasible applications in digital copyright protection. [Methodology/Process] Employing literature review and web-based research methods, this paper retrospectively examines and summarizes relevant research progress on digital evidence. Furthermore, it systematically analyzes the background, development trajectory, service connotation, service content, and service features of WIPO Trusted Digital Evidence, and proposes feasible applications in digital copyright protection. [Results/Conclusion] Current digital evidence research primarily focuses on conceptual clarification, characteristic analysis, legal status and associated legal frameworks, as well as issues of evidence collection and preservation. The WIPO Trusted Digital Evidence Service possesses authoritative organizational status, trustworthy workflows, stable technical support, and stringent management policies and service standards. It can provide trusted timestamp digital evidence for digital work creation processes, bind creator identities to digital works, assist researchers and university libraries in managing scientific data, and help researchers address link rot.

Full Text

Preamble

Analysis of the Content and Characteristics of WIPO Trusted Digital Evidence Service

Huang Guobin, Chen Li Beijing Normal University, Beijing 100875

Abstract: [Purpose/Significance] This study aims to analyze the content and characteristics of the WIPO trusted digital evidence service and propose feasi-

ble applications of this service in digital copyright protection. [Method/Process] Using literature research and network investigation methods, this paper reviews and summarizes the research progress on digital evidence. It further examines the background, development history, service connotation, service content, and service characteristics of WIPO trusted digital evidence, and proposes feasible applications in digital copyright protection. [Result/Conclusion] Current research on digital evidence primarily focuses on conceptual analysis, characteristic analysis, legal status and related legal systems, and issues of evidence collection and preservation. The WIPO trusted digital evidence service features authoritative organizational status, reliable workflows, stable technical support, and strict management policies and service standards. It can provide trusted timestamp digital evidence for digital work creation processes, bind creator identity to digital works, assist researchers and university libraries in managing scientific data, and help researchers address reference rot.

Keywords: WIPO trusted digital evidence; digital evidence; digital copyright protection; scientific data; reference rot

Classification Number: G203; D923.41

---

1. Domestic and International Research Progress

WIPO trusted digital evidence service provides digital evidence of a digital file's existence at a specific point in time, serving as an auxiliary tool for rights confirmation in legal disputes. In December 2020, this study conducted searches in CNKI and Web of Science using keywords such as "trusted digital evidence," "WIPO PROOF," and "trusted digital evidence," yielding limited results. After screening, no studies related to the WIPO trusted digital evidence service were found, prompting further investigation into digital evidence research. The investigation revealed that scholars both domestically and internationally have focused on four main aspects: definition and conceptual analysis of digital evidence, characteristic analysis, legal status and related legal systems, and the evidence collection and preservation process.

1.1 Definition and Conceptual Analysis of Digital Evidence

The term "digital evidence" is translated from the English "digital evidence" and is also rendered by some scholars as electronic evidence or computer evidence, leading to ongoing debates about its connotation and extension in Chinese academia. Scholar Dai Ying [3] argues that digital evidence has a digital form, using binary code symbols as information elements to transmit information through sequences of 0s and 1s. Scholars Zhuang Qianlong et al. [4] believe digital evidence should contain at least two elements: the essential attribute of evidence—digitization—and its current or future existence form—electronization. Scholar C.M. Whitcomb [5] also defines digital evidence as "information of probative value stored or transmitted in digital form," which can

exist as text, audio, or images. Scholar Li Binglong et al. [6] contend that digital evidence includes not only common text, graphics, images, and audio-video materials but also system logs, database files, operation records, and real-time chat logs. Some scholars define digital evidence from the perspective of case investigation, such as Wang Fang [7] and Anniwar Mijiali [8], who view digital evidence as data in digital form generated during information digitization that can prove case facts. Scholar Mou Li et al. [9] consider digital evidence to be information and data of value to case investigations that are stored, received, and transmitted by digital devices. Additionally, many scholars have examined distinctions between digital evidence and related concepts; for instance, Xu Xiaotong [10] and Du Zhichun [11] have compared electronic documents with audio-visual materials, computer evidence, digital evidence, electronic data, scientific evidence, and electronic records from different perspectives. Thus, digital evidence is digital material that relies on certain digital devices, has multiple digital forms, and can provide useful information for cases in judicial proceedings. In this study, trusted digital evidence refers to digital evidence with trusted timestamp identification that can assist judicial authorities in confirming rights ownership in cases.

1.2 Characteristic Analysis of Digital Evidence

Based on different definitions, scholars have varying views on digital evidence characteristics, comparing them with traditional evidence. Representative perspectives include: Liao Genwei [12], who believes digital evidence has abstractness and intangibility, perceptual diversity and dependency, dependence and relative independence, coexistence of volatility and recoverability, and precision and fragility of data content. Wang Fang [7] considers high-tech nature and vulnerability to be two accompanying characteristics, along with diversity and openness, rapid transmission, and convenience. Li Binglong et al. [6] argue that compared with traditional evidence, digital evidence has high precision and vulnerability, strong concealment, multimedia characteristics, and advantages of rapid collection, easy preservation, small space occupation, large capacity, and convenient operation. Additionally, Mou Li et al. [9] believe digital evidence also has potentiality and time sensitivity. Synthesizing these definitions and characteristics, this study identifies digital evidence features as: formal diversity, low replication cost, convenient transmission, content precision, and time sensitivity, along with abstractness, vulnerability, and carrier dependence. Trusted digital evidence should additionally possess non-tamperability, easy verifiability, and reliability.

1.3 Legal Status and Related Legal Systems of Digital Evidence

Digital evidence has gained attention with scientific and technological development and widespread use of digital devices, representing a new evidence form distinct from paper documents and audio-visual materials. Currently, relevant laws and regulations on digital evidence are inadequate both domestically and

internationally. Scholar Zhang Lifang [13] argues that China should list digital evidence as an independent evidence form in evidence law and establish corresponding rules for accurate regulation and practice guidance. Cheng Lin [14] proposes improving relevant laws and regulations to enhance digital investigation and evidence collection capabilities, addressing multiple challenges in discovering, collecting, identifying, preserving, and enforcing digital evidence in computer crime investigations. Fan Guanyan [15] examines research findings from North America's "Evidence Law in Digital Environments" project, discussing their applicability in China and comparing digital evidence conditions between China and North America. Foreign scholar O. Kerr [16] believes traditional criminal procedure laws cannot effectively regulate digital evidence investigations, requiring new regulations for digital evidence and its collection methods, and proposes specific content and formulation approaches.

1.4 Digital Evidence Collection and Preservation Process

Digital evidence's vulnerability, replicability, and susceptibility to destruction mean that if the collection process is not standardized or preservation is improper, its integrity and validity as evidence cannot be guaranteed. Scholars Wei Longfei [17] and Zhang Meng [18] discuss digital evidence collection technology and its challenges. Mou Li et al. [9] examine technical methods and considerations for crime scene technicians collecting digital evidence. You Junchen [19] proposes an SSL-based digital evidence protection mechanism from the perspective of protecting confidentiality and information integrity. Chen Baihua [20] analyzes the current status and problems of mobile phone data forensics, designing and implementing an Android-based data collection system to meet market demands. Zhang Junfu [21] designs a universal forensics framework for Android applications, dividing the process into six sub-processes: file capture, file processing, data extraction, data parsing, information association, and result marking. N. Rudolph et al. [22] explore characteristics of digital evidence generated by digital devices and its legal requirements, recommending these requirements be incorporated into device development and evidence creation processes. S. Lee et al. [23] examine general digital evidence collection processes, establishing specific steps to ensure integrity and memory information collection, and propose PKI-based MDC public systems, MAC systems, and public certification systems.

2. Background and Development History of WIPO Trusted Digital Evidence Service

WIPO trusted digital evidence is an emerging intellectual property service and an online business service for digital works. Developed within WIPO's existing intellectual property protection system, it represents a new tool for digital copyright protection. This study systematically collected information on its background and development through network investigation.

2.1 Background

WIPO's mission is to lead the development of a balanced and effective international intellectual property system that enables innovation and creativity for the benefit of all [24]. To provide simple, economical intellectual property protection for enterprises and individuals worldwide, WIPO has launched a series of global intellectual property services, including the Patent Cooperation Treaty (PCT) for international patent protection, the Madrid System for international trademark protection, and the Hague System for registering industrial designs in multiple member states with minimal formalities and cost. WIPO has also established an Arbitration and Mediation Center to provide neutral, international, non-profit alternative dispute resolution (ADR) services for intellectual property and technology disputes. Furthermore, WIPO emphasizes intellectual property data management, having established multiple databases containing vast amounts of intellectual property information, including PATENTSCOPE, the Global Brand Database, and the Global Design Database, all freely accessible online.

With the digital era, economic activities worldwide are increasingly digitized. Industrial production and technological R&D increasingly rely on technology, big data, and global collaboration for innovation and creativity enhancement. However, existing WIPO intellectual property systems cannot fully meet national, enterprise, and individual needs for digital work protection. International copyright law stipulates that creators automatically obtain copyright when fixing creative works in tangible media (e.g., digital files) without requiring any action, making evidence of a work's existence at a specific time crucial in litigation. Providing evidence of digital asset rights ownership is key to winning intellectual property infringement lawsuits, and ensuring evidence authenticity, legality, and integrity is critical. Traditional digital evidence integrity proof methods almost universally fail to bind time identifiers to digital evidence. Recent intellectual property litigation cases have increasingly adopted timestamps to preserve electronic evidence, using trusted timestamps on digitally signed files to resolve legal issues. WIPO trusted digital evidence service was developed under these circumstances, supplementing WIPO's existing intellectual property services and providing another tool for users to strategically manage intellectual assets [25].

2.2 Development History

WIPO launched the trusted digital evidence service on May 27, 2020. On July 31, 2020, WIPO announced Spanish and French versions. According to WIPO news reports, as of September 15, 2020, visitors from over 150 countries and regions had accessed the service online, with users from 117 countries and regions having used it. Mexico, Switzerland, Spain, Russia, and France were the most frequent users, with the United States, India, and Italy also using it multiple times. By December 2020, the service offered nine language versions including English, Chinese, Japanese, Spanish, French, Korean, Russian, German,

and Portuguese, enabling users to more easily obtain written evidence in the language of the jurisdiction where legal disputes arise [26].

3. Basic Connotation and Main Characteristics of WIPO Trusted Digital Evidence

3.1 Service Connotation

WIPO trusted digital evidence is a new online digital business service that provides date and timestamp digital fingerprints for any digital file, quickly generating tamper-proof evidence to prove the file's existence at a specific point in time [27]. Using industry-leading security technology, the service generates globally recognized digital fingerprints—called WIPO trusted digital evidence tokens—for users' intellectual assets within seconds, adding date and timestamp upon token creation. Tokens remain valid indefinitely, are securely stored for five years, and consistently align with evolving encryption technology. Anyone can verify tokens online through WIPO to prove a tokened digital file's existence at any time, effectively preventing intellectual asset abuse and misappropriation and serving as auxiliary evidence in legal disputes.

3.2 Service Content

WIPO trusted digital evidence service offers two categories: paid and free. Paid services include: (1) Token creation: The token is a date-and-time-stamped digital fingerprint of a digital file, permanently valid and stored for five years, with an option to extend storage before expiration. (2) Premium certificate application: Based on obtained tokens, users can apply for premium certificates stamped and signed by WIPO [Figure 1: see original paper] to assist in proving digital file ownership and existence at a specific time. WIPO currently provides certificates in multiple languages. Additionally, the service offers free token verification, allowing users to verify a digital file's existence at a determined time to help resolve digital copyright disputes [28].

3.3 Service Characteristics

3.3.1 Authoritative Organizational Status The World Intellectual Property Organization (WIPO) is the global forum for intellectual property services, policy, information, and cooperation. Established in 1967, it currently has 193 member states [29]. At the 59th Assembly of Member States in October 2019, WIPO's 193 member states unanimously approved the launch of the WIPO trusted digital evidence project. WIPO trusted digital evidence tokens can be used in countries that recognize digital timestamps as legal evidence. To overcome potential authentication limitations of local Time Stamp Authorities (TSAs) in different jurisdictions, WIPO's timestamp service creates identical evidence for each jurisdiction with potential legal disputes, making the service jurisdiction-independent, with a single token sufficient as admissible evidence in courts accepting digital evidence.

3.3.2 Reliable Workflow Anyone can access WIPO trusted digital evidence's secure online website to request tokens for specific digital files. The token creation workflow comprises: (1) User access: Users access the service website via browser (wipo-proof.wipo.int) and must register a WIPO account. (2) Token request: Users select one or more digital files of any format; the system generates digital fingerprints (hashes) without uploading files, storing only the hash values to maximize personal information and data protection. (3) Token creation: The backend system timestamps the hash values, creates digital signatures, and generates tokens. (4) Token download: Users can directly download created tokens.

3.3.3 Stable Technical Support WIPO trusted digital evidence service employs mature digital authentication technology—PKI technology—to provide compliant digital evidence accepted by most countries. PKI, based on public-key cryptography and digital signatures with digital certificates at its core, has become the security foundation platform for network applications [30]. PKI comprises public-key certificates, certificate authorities, certificate management systems, and related hardware, software, and legal foundations, providing basic services supporting public-key cryptography applications. Its core function is solving trust issues in information networks, establishing the uniqueness, authenticity, and legality of various actors in cyberspace to protect security interests [31], with characteristics of information confidentiality, authentication, integrity, and non-repudiation [32]. PKI uses certificates for public-key management, binding user identity information with public keys through third-party Certificate Authorities (CAs). The WIPO service's digital authentication process is completely tamper-proof, making it a digital equivalent of a notary public.

The service also complies with the ISO/IEC 27001 information security management standard, which specifies requirements for establishing, implementing, maintaining, and continually improving information security management systems within organizations, including risk assessment and treatment according to international standards [35]. Furthermore, the timestamp service complies with ETSI EN 319 421 (Electronic Signatures and Infrastructures; Policy and Security Requirements for Trust Service Providers issuing Time-Stamps), which aims to meet international requirements for trust services in electronic transactions, including more specific provisions for qualified Trust Service Providers (TSPs) issuing qualified timestamps [36].

3.3.4 Strict Management Policies and Service Standards WIPO trusted digital evidence service complies with the eIDAS (electronic Identification, Authentication and Trust Services) regulation [33], one of the world's most comprehensive and stringent electronic trust service regulations. The EU regulation establishes rules for electronic identification and trust services, including technical standards based on the European Telecommunications Standards Institute (ETSI) [34]. eIDAS allows citizens, enterprises, and public administrations to use electronic identification means and trust services

(electronic signatures, seals, timestamps, registered electronic delivery, and website authentication) for online services and electronic transaction management. eIDAS features include: (1) Transparency and accountability: clearly defining minimum obligations and responsibilities of trust service providers; (2) Credibility and security: ensuring service credibility and security requirements; (3) Technical neutrality: avoiding requirements that only specific technologies can meet; (4) Market rules and standardization certainty. Compliance advantages include better user experience, higher security and accountability, and greater efficiency gains through process cycle reduction, large-scale automation, simplified task execution, and lower overall costs while maintaining quality [33].

3.4 Comparison with Domestic Digital Evidence Services

In recent years, China has seen digital evidence services based on blockchain technology. Ant Group's Ant Blockchain is China's first legally recognized blockchain evidence platform, offering "trusted deposit services" based on blockchain and AI technology with characteristics of full-process traceability, full-link credibility, and full-node witnessing [37]. The service charges monthly/annually, with a minimum purchase of 50,000 deposit services for 30,000 RMB per month, better suited for enterprises or groups with high deposit demands. Ant Blockchain also developed the "Quezhao Digital Copyright Service Platform," which provides deposit, verification, network monitoring, and on-chain evidence collection services. While deposit fees are low (only 5 RMB per instance), network monitoring and on-chain evidence collection are expensive. The platform requires uploading files with size and format restrictions, stores files for only three years, and requires users to preserve originals [38].

Compared with Ant Blockchain, WIPO trusted digital evidence service offers broader applicability: (1) Authority: Ant Blockchain is only recognized under Chinese law, while WIPO evidence is valid in all countries recognizing digital timestamps; (2) Stability: Ant Blockchain relies on blockchain technology, which remains exploratory in digital copyright management with issues like resource waste, lack of unified standards, originality judgment deficiencies, and frequent smart contract vulnerabilities [39]. WIPO's PKI infrastructure, based on cryptography, digital signatures, data integrity mechanisms, digital envelopes, and dual digital signatures, is more mature and stable; (3) Security: Ant Blockchain requires uploading digital files, while WIPO never accesses local files, storing only generated hash values to better protect digital assets and reduce information leakage risk; (4) Convenience: While Ant Blockchain primarily serves domestic users with Chinese and English interfaces, WIPO provides multiple language versions for global accessibility; (5) Cost-effectiveness: WIPO offers single and bundled purchase options at moderate prices, better suited for individual users with limited deposit needs.

4. Applications of WIPO Trusted Digital Evidence in Digital Copyright Protection

WIPO defines copyright as "a legal term describing the rights creators have over their literary and artistic works." Copyright applies to broad creative outputs, from books, music, paintings, sculpture, and films to computer programs, databases, advertisements, maps, and technical drawings [40]. Copyright grants creators economic and moral rights. Under the Berne Convention [41], works are automatically copyrighted in most countries without registration. However, when copyright disputes arise, concrete evidence of a work's existence at a specific time is crucial—precisely what WIPO trusted digital evidence provides.

4.1 Providing Trusted Timestamp Digital Evidence for Digital Work Creation

WIPO trusted digital evidence tokens provide timestamped digital proof that creators developed works before a certain time, helping establish existence at specific points. China's Copyright Law has been implemented for nearly 30 years, forming a relatively complete legal system with continuous amendments and administrative regulations. Policies like the "Administrative Measures for Internet Copyright Protection" and "Regulations on the Protection of Information Network Transmission Rights" specifically address digital copyright, yet public awareness remains weak, particularly regarding protection during the creation process. Due to digital works' characteristics and the internet's borderless, public, and interactive nature, creators increasingly publish and disseminate works online, but copyright infringement has become more severe. Creators cannot simultaneously achieve knowledge sharing and prevent abuse or misappropriation, making it essential to enhance protection awareness and prepare in advance. In digital evidence research, scholars have identified timestamp synchronization as a challenge requiring trusted timestamp services [18], and noted that current integrity proof methods fail to bind time identifiers to digital evidence [42]. Linking works to their existence time is also critical in copyright disputes. WIPO trusted digital evidence helps copyright owners generate tamper-proof, timestamped tokens from a work's initial creation, providing trusted evidence when disputes arise while enhancing protection awareness.

4.2 Binding Creator Identity to Digital Works

Core to digital copyright protection is rights confirmation—establishing the relationship between author and work. In network environments, due to digital resources' replicability and vulnerability, unregistered works published and disseminated online make ownership difficult to determine when disputes arise. Therefore, linking creator identity to digital works before publication is crucial. Creators can use WIPO trusted digital evidence to apply for tokens linking their identity to works. The service also allows creators to create separate tokens for partial works (lyrics, melodies) and final complete works, recording and protecting each component. Music, film, and video works often involve multiple

collaborators, and distinguishing contributions helps resolve future authorship disputes. With low cost, simple operation, and free verification services, WIPO trusted digital evidence minimizes the time and financial costs of binding works to creator identity.

4.3 Assisting Researchers and University Libraries in Managing Scientific Data

Scientific data, also called research data, refers to original foundational data generated in scientific research activities [43], including observational, statistical, survey, and experimental data. Research institutions, universities, and corporate R&D departments generate valuable scientific data daily that may lead to new products and discoveries. While researchers may use tools to capture and manage these digital assets, these tools cannot prove scientific data's existence at specific times. Scientific data is continuously updated and accumulated during research, producing multiple versions requiring documentation and preservation. WIPO trusted digital evidence can prove digital assets' existence at specific times and help researchers create multi-version histories for software code, experimental data, and research notes to reduce future misappropriation risks. As information resource aggregators, organizers, managers, and knowledge guides, university libraries are responsible for providing disciplinary services, institutional repository construction, and scientific data management support. Using WIPO trusted digital evidence, libraries can develop effective scientific data management plans that protect digital copyright and help faculty and students manage scientific data, reducing potential copyright dispute risks.

4.4 Helping Researchers Address Reference Rot

Network citations are references in academic papers whose sources are network information—essentially, network information used as citations [44]. References are crucial components of academic papers, forming a complete expression of rigorous scientific research together with the main text and serving as important factors in core journal and academic evaluations [45]. However, network information resources are numerous and rapidly updated, with many experiencing link rot or content drift over time, making it impossible to prove referenced content's authenticity and existence after citation—highly inconvenient for researchers. WIPO trusted digital evidence can help address this: researchers can screenshot URLs and web content of cited resources, save complete web pages as digital files, and obtain tamper-proof timestamped tokens for these files. The tokens and digital files together serve as evidence of network citations' existence at specific times, helping researchers prepare for reference rot.

Limitations and Conclusion

As a new service, WIPO trusted digital evidence's framework and functions remain under development with certain limitations: (1) The service currently

provides tamper-proof evidence proving digital files' existence at specific times, serving as an auxiliary means for rights confirmation and helping manage future copyright disputes. However, it cannot yet provide legally guaranteed intellectual property protection like global registration systems (PCT, Madrid, Hague), which are based on international treaties among member states and simplify cross-jurisdictional protection applications. WIPO trusted digital evidence can be considered an intellectual property protection measure but does not provide actual protection or registration, nor can it replace registration systems. (2) The service does not access users' local files, reducing information leakage and infringement risks during service use. However, it does not provide data storage; users must preserve original files used for token applications without any modifications. When disputes arise, users must provide original files for verification, which is inconvenient, especially for large digital files like digital library resources or enterprise big data that cannot be easily stored locally.

WIPO trusted digital evidence serves as an effective tool for creating evidence of digital files' existence at specific dates and times. Users can retain generated tokens as digital evidence to reduce potential legal disputes. The service can assist in proving intellectual property ownership and help individuals and enterprises protect digital asset content, whether or not they become formal intellectual property. This represents significant development in digital copyright protection services, advancing intellectual property protection into the digital world. Currently, the global economy is undergoing a massive transformation from industrialization to digitization. According to WIPO statistics, digital and information technology-related patent applications are increasing annually. While most intellectual property systems were developed for the industrial era, traditional protection does not necessarily cover all types, especially for digital works and data. WIPO trusted digital evidence marks a major step forward in providing intellectual property services for the digital economy. This study examined the service's basic connotation, 梳理了其主要特征 based on the fundamental concepts and characteristics of "trusted digital evidence," compared it with domestic digital evidence services for digital copyright protection, summarized its outstanding features, and proposed feasible applications from a practical perspective.

References

[1] Xie Jingjing. Research on digital copyright protection in network environments [J]. Legal System and Society, 2014(30): 276-277.

[2] World Intellectual Property Organization. Introducing WIPO PROOF: an interview with Francis Gurry [EB/OL]. [2020-11-11]. https://www.wipo.int/wipo_{magazine}/en/2020/02/artic

[3] Dai Ying. Analysis of electronic evidence and related concepts [J]. Chinese Criminal Law Journal, 2012(3): 73-77.

[4] Zhuang Qianlong, Zhu Tengfei. Conceptual analysis of criminal electronic data evidence in the big data era [J]. Journal of Henan Judicial Police Vocational

College, 2019, 17(4): 75-81.

[5] WHITCOMB C M. Forensic aspects of digital evidence: contributions and initiatives by the National Center for Forensic Science (NCFS) [J]. Proceedings of spie-the international society for optical engineering, 2002(4709): 111-120.

[6] Li Binglong, Wang Lu, Chen Xingyuan. Digital forensics technology and its development trends [J]. Information Network Security, 2011(1): 52-55.

[7] Wang Fang. Nature and related rules of digital evidence [J]. Law Science, 2004(8): 72-79.

[8] Jia Mali. Brief discussion on digital signatures and digital evidence [J]. Fujian Computer, 2004(2): 7-8.

[9] Mou Li, Zhong Hongfei, Yang Min. Digital evidence crime scene investigation [J]. Guangdong Public Security Science and Technology, 2013, 21(4): 22-25.

[10] Xu Xiaotong, Xiao Qiuhui. Comparison and evolution analysis of concepts related to electronic documents and evidence law [J]. Archives Science Bulletin, 2019(2): 23-28.

[11] Du Zhichun, Liao Genwei. Conceptual comparison and analysis of digital evidence, electronic evidence, scientific evidence, and electronic records [J]. Chinese Journal of Forensic Sciences, 2011(4): 64-68.

[12] Liao Genwei. Concept and characteristic analysis of digital evidence [J]. Jianghuai Tribune, 2010(3): 136-139.

[13] Zhang Lifang. Research on the legal status and applicable rules of digital evidence [D]. Sichuan University, 2004.

[14] Cheng Lin. Strengthen computer digital forensics research to improve digital crime investigation capabilities [J]. Journal of Chinese People's Public Security University (Social Sciences Edition), 2012, 28(6): 1-8.

[15] Fan Guanyan. Electronic evidence rules in digital environments: comparative research based on LEDE project [J]. Archives Science Study, 2017(S1): 100-107.

[16] KERR O. Digital evidence and the new criminal procedure [J]. Columbia law review, 2005, 105(1): 279-318.

[17] Wei Longfei. Research on computer digital forensics technology based on information security protection [J]. China New Telecommunications, 2015, 17(20): 99.

[18] Zhang Meng. Analysis of challenges in digital forensics in mobile cloud environments [J]. Police Technology, 2015(5): 42-44.

[19] You Junchen. SSL-based security solution for digital evidence protection mechanism [J]. Mianyang Normal University Journal, 2008(5): 93-97.

[20] Chen Baihua. Implementation of Android mobile phone data collection system [D]. Xiamen University, 2017.

[21] Zhang Junfu. Design of universal framework and system for Android application forensics [D]. Southeast University, 2019.

[22] KUNTZ E, RUDOLPH C, ALVA A, et al. On the creation of reliable digital evidence [C]//IFIP international conference on digital forensics. Springer Berlin Heidelberg, 2012, 383: 3-17.

[23] LEE S, KIM H, LEE S, et al. Digital evidence collection process in integrity and memory information gathering [C]//International workshop on systematic approaches to digital forensic engineering. TAIPEI: IEEE, 2005: 236-247.

[24] World Intellectual Property Organization. What is WIPO? [EB/OL]. [2020-11-09]. https://www.wipo.int/about-wipo/en/index.html.

[25] World Intellectual Property Organization. Trusted digital evidence for your intellectual assets [EB/OL]. [2020-11-09]. https://wipo-proof.wipo.int/wdts/.

[26] World Intellectual Property Organization. WIPO PROOF now available in French and Spanish; in nine languages by year-end [EB/OL]. [2020-11-10]. https://www.wipo.int/wipo-proof/en/news/2020/news_{0002}.html.

[27] World Intellectual Property Organization. WIPO PROOF—Trusted digital evidence [EB/OL]. [2020-11-09]. https://www.wipo.int/wipo-proof/en/.

[28] World Intellectual Property Organization. WIPO PROOF services & pricing [EB/OL]. [2020-11-28]. https://wipo-proof.wipo.int/wdts/services-pricing.xhtml.

[29] World Intellectual Property Organization. Inside WIPO [EB/OL]. [2020-11-28]. https://www.wipo.int/about-wipo/en.

[30] Gu Yunhua, He Yanxiu. PKI/PMI security model and its application in digital copyright trading platforms [J]. Journal of Wuhan University of Technology, 2010, 32(16): 80-83.

[31] Yang Yu. Research and implementation of PKI-based identity authentication system [D]. University of Electronic Science and Technology, 2009.

[32] Li Yunlong. Design and implementation of PKI-based digital certificate management system [D]. Huazhong University of Science and Technology, 2015.

[33] European Commission. eIDAS for SMEs [EB/OL]. [2020-11-10]. https://ec.europa.eu/digital-single-market/en/eidas-smes.

[34] European Telecommunications Standards Institute. About us [EB/OL]. [2020-11-10]. https://www.etsi.org/about.

[35] International Organization for Standardization. ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements [EB/OL]. [2020-11-10]. https://www.iso.org/standard/54534.html.

[36] European Telecommunications Standards Institute. Electronic signatures and infrastructures (ESI); Policy and security requirements for trust service providers issuing time-stamps [EB/OL]. [2020-11-25]. https://www.etsi.org/deliver/etsi_{en}/319400_{319499}/319421/01.01.01_{60}/en_{319421v010101p}.pdf

[37] Ant Blockchain Trusted Deposit Product Overview [EB/OL]. [2021-03-18]. https://antchain.antgroup.com/docs/11/130331.

[38] Quezhao Digital Copyright Service Platform [EB/OL]. [2021-03-18]. https://www.mydcs.com/pages/index.

[39] Lai Lina, Li Yongming. Opportunities, challenges, and development paths of digital copyright protection under blockchain technology [J]. Rule of Law Research, 2020(4): 127-135.

[40] World Intellectual Property Organization. What is copyright? [EB/OL]. [2020-11-25]. https://www.wipo.int/copyright/en/.

[41] World Intellectual Property Organization. Berne Convention for the Protection of Literary and Artistic Works [EB/OL]. [2020-11-25]. https://wipolex.wipo.int/en/text/283698.

[42] Wang Jun. Research on digital evidence integrity proof methods—Secure, auditable digital timestamp proof method [J]. Journal of Sichuan Police College, 2007(6): 58-62.

[43] Si Li, Xing Wenming. Investigation of foreign scientific data management and sharing policies and implications for China [J]. Information and Documentation Services, 2013, 34(1): 61-66.

[44] Ren Jing, Sun Jianjun. Review of network information utilization in journal literature—From the perspective of network citations [J]. Modern Information, 2012, 32(4): 174-177.

[45] Wang Xiaoyan, Lu Hong. Reflections on standardization of network information resource citation in references [J]. Modern Information, 2005(5): 6-7.

Author Contributions:

Huang Guobin: Conceived the research topic, proposed research ideas and outline, and guided writing and revision.

Chen Li: Collected and organized research materials and wrote the paper.

Academic Integrity Statement for Authors of *Library and Information Service*

Library and Information Service has always upheld the mission of publishing excellent academic research and promoting scholarly exchange, while committed to purifying the academic publishing environment and creating a healthy

academic ecosystem. In 2013, the journal took the lead in formulating, publishing, and implementing the "Joint Statement on Upholding Academic Ethics and Purifying the Academic Environment by Library Science Journals" (the "Statement") (see: http://www.lis.ac.cn/CN/column/item202.shtml). Subsequently, it led the formulation and publication of the "Joint Action Plan for Chinese Library and Information Science Journals to Resist Academic Misconduct" (the "Joint Action Plan") (see: http://www.lis.ac.cn/CN/column/item247.shtml). To implement this philosophy, the journal hereby declares that, effective immediately, all submitting authors must commit to: complying with the above "Statement" and "Joint Action Plan," consciously adhering to academic ethics, and resolutely resisting academic misconduct. *Library and Information Service* maintains zero tolerance for all forms of academic misconduct, including plagiarism and appropriation, and will implement corresponding punitive measures.

Library and Information Service Editorial Office

Note: Figure translations are in progress. See original paper for figures.