Forensic Science International: Digital Investigation 59 (2026) 302238



Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi





A study on the standardization of tools and equipment for digital forensics laboratories

Sumin Shin [a, b], Byounghun Moon [a, c], Jihye Jang [a], Gibum Kim [a,*]

[a] Sungkyunkwan University, Department of Forensic Science, Digital Forensics, 25-2 Sungkyunkwan-ro, Jongno-gu, Seoul, 03063, Republic of Korea
[b] Korea Institute for Defense Analyses (KIDA), 37 Hoegi-ro, Dongdaemun-gu, Seoul, 02455, Republic of Korea
[c] Korean Police Investigation Academy, 112 Mugunghwa-ro, Asan-si, Chungcheongnam-do, 31540, Republic of Korea

HIGHLIGHTS

- Establishes a standardized equipment list and budget for Digital Forensic Labs.
- Analyzes 124 practitioner surveys and South Korean RFPs (2015–2025).
- Validates findings via ODA procurement data from five countries (2022 to 2025).
- Provides a practical reference model for global DFL construction.

ARTICLE INFO

Keywords:
Digital forensics
Digital forensics laboratory (DFL)
Digital forensics tools and equipment
Standardization
Focus group interview (FGI)
Survey

ABSTRACT

When developing digital forensic capabilities, building a laboratory to securely acquire and handle digital evidence is a top priority. However, differences in organizational size and characteristics have led to a lack of standardization in budget acquisition and implementation, creating significant challenges. Therefore, this study aims to provide a practical baseline for establishing a composition plan and securing a budget by defining essential tools and equipment for laboratories of varying scales (one-person and five-person configurations). Rather than proposing a new standard, this study presents an implementation baseline that conforms to existing guidance, such as ISO/IEC 17025 and the INTERPOL Global Guidelines for Digital Forensics Laboratories. This study employed a mixed-methods approach. An initial equipment list was derived from focus group interviews with 12 experts, refined through site visits, and validated via a survey of 124 professionals. To ensure feasibility, 62 public requests for proposals were analyzed, and delivery records from ODA projects in five countries (2022–2025) were verified. This study provides practical implementation criteria that address the resource requirements of ISO/IEC 17025 (facilities, environmental conditions, and equipment) and effectively answers the question of how to build a digital forensics laboratory. Rather than rigid regulations, the study suggests a "common baseline configuration" that serves as a practical reference standard. This enables organizations to customize their tools and equipment according to their size and budget while supporting alignment with international standards.

1. Introduction

Digital forensics laboratories (DFLs) are operated not only by investigative agencies such as prosecutors' offices and police agencies but also by private companies (Lyle et al., 2022). These laboratories serve as critical infrastructure for producing reliable results, enhancing the quality of acquired information, and demonstrating the credibility of digital evidence in court (ENFSI, 2015; INTERPOL, 2019). In terms of quality management, non-technical factors such as the management of DFLs can also affect the outcomes of forensic analysis (ENFSI, 2015). The establishment of a DFL requires a comprehensive management system. The system's requirements can be grouped into four broad areas: personnel (skilled staff and competency testing), physical resources (equipment, facilities, and environmental conditions), documentation (reference materials, record-keeping, and methodologies), and quality assurance (process validation, functionality verification (based on tools or personnel), and verification and evaluation of measurement uncertainty)

* Corresponding author.
Email addresses: shin1121@g.skku.edu (S. Shin), sindori1@naver.com (B. Moon), jihye01@g.skku.edu (J. Jang), kgb02@skku.edu (G. Kim).

https://doi.org/10.1016/j.fsidi.2026.302238
Received 10 May 2025; Received in revised form 24 August 2026; Accepted 24 October 2026
2666-2817/© 2026 Elsevier Ltd. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

(INTERPOL, 2019; SWGDE, 2017, 2010; International Organization for Standardization, 2017).

The standard most commonly applied to DFLs is ISO/IEC 17025, which sets out general requirements for the competence of testing and calibration laboratories. This standard specifies environmental requirements for building DFLs, including facilities and environmental conditions (Section 6.3) and equipment (Section 6.4) (International Organization for Standardization, 2017). Of course, organizations intending to operate digital laboratories face various challenges beyond equipment and facilities, such as securing skilled personnel, budgets, and physical space. In many cases—excluding investigative agencies—DFLs function as part of a larger organization and are generally not large in scale. Therefore, the primary aim of this work is to curate a baseline list of the tools and equipment and associated budget estimates necessary for the establishment of a DFL. This study provides an implementation baseline that maps practitioner-validated tool and equipment requirements onto existing guidance, including ISO/IEC 17025, the INTERPOL Global Guidelines, and SWGDE and ENFSI best practices (International Organization for Standardization, 2017; INTERPOL, 2019; SWGDE, 2010; ENFSI, 2015). The scope of the analysis is specifically centered on small-scale operations, distinguishing between laboratories comprised of a single staff member and those with a capacity of up to five personnel. Acknowledging the variability in financial allocation and operational mandates across different organizations, this study calculates the maximum resource demands for each scale, factoring in these limitations. In Chapter 2, a review of existing literature concerning the criteria for identifying and selecting tools and equipment for DFLs is presented. Chapter 3 details the research methodology—comprising focus group interviews, on-site visits, and surveys—utilized to determine the necessary resources for laboratories with the specified staffing levels. Chapter 4 refines and validates the derived items and budgets. This validation process entails three components. First, prices are verified by digital forensic service providers. Second, purchase lists for digital forensic tools and equipment are comprehensively reviewed in Request for Proposals (RFPs) issued in Korea between 2015 and 2025. Third, actual delivery records from ODA projects in five countries (Vietnam, Indonesia, Mongolia, Bangladesh, and Nepal) are comparatively analyzed. Chapter 5 discusses the implications and future directions, and Chapter 6 concludes the study with its limitations.

2. Related work

2.1. Tool evaluation and selection

SWGDE defines minimum test requirements for digital and multimedia forensic tools (SWGDE, 2024). It categorizes functions into critical (preservation, acquisition, hashing, wiping), OS-related, analysis, multimedia, and administrative components, providing a baseline for tool assessment. NIST SP 800-101 R1 emphasizes mandatory validation and revalidation of tools after updates, noting that defects such as failed recovery or inconsistencies undermine evidentiary reliability (Ayers et al., 2014). It identifies usability, comprehensiveness, accuracy, determinism, verifiability, and testability as core criteria. NIST SP 800-35 supports procurement and operational alignment through lifecycle management and SLAs, while NIST IR 8354 highlights usability, software reliability, and processing speed as key test factors (Grance et al., 2003; Lyle et al., 2022). ISO/IEC 17025:2017 strengthens reproducibility and accreditation readiness through requirements for impartiality, traceability, validation, and documentation (International Organization for Standardization, 2017). ISO/IEC 27037:2012 formalizes procedures for evidence identification, collection, preservation, and chain of custody (International Organization for Standardization, International Electrotechnical Commission, 2012). O'Connor identified technical, managerial, and legal criteria for tool selection through expert interviews (O'Connor, 2005). Hibshi et al. highlighted usability issues such as user experience, GUI/CLI preferences, reporting features, and workflow design (Hibshi et al., 2011). Karabiyik and Karabiyik modeled tool selection as a game-theoretic decision problem, applied to file-carving tools (Karabiyik and Karabiyik, 2020). Friedl et al. integrated an expanded tool typology with the Analytic Hierarchy Process (AHP) to generate structured rankings (Friedl et al., 2023). Guo et al. proposed a function-oriented validation and verification framework for forensic tools, grounded in requirements specification and reference test sets (Guo et al., 2009). Horsman further documented persistent tool-testing and reliability challenges that such evaluation regimes must address (Horsman, 2019). Stoykova et al. identified documentation and methodological gaps in 124 Norwegian cases (Stoykova et al., 2022), while Nordvik et al. designed a reproducibility assessment framework for file-system interpretation (Nordvik et al., 2021).

2.2. Tool and equipment lists and budget estimation

Lawrence et al. conducted a study to support budget planning for DFLs (Lawrence et al., 2018). They identified the minimum set of tools and equipment required to establish a small laboratory for one or two personnel and presented estimates for acquisition and maintenance costs. Their analysis distinguished between computer forensics and mobile forensics, incorporating both commercial and open-source products. The estimated acquisition costs ranged from USD 8575 to USD 22,052, while annual maintenance costs ranged from USD 2478 to USD 6419. Nodeland and Belshaw supplemented this perspective through telephone surveys with Texas law-enforcement agencies, outlining the equipment categories, startup cost ranges, and general cost estimates for the computers, hardware, and software required to establish law-enforcement and university cyber laboratories (Nodeland and Belshaw, 2020). Buchanan-Wollaston et al. empirically compared the data-recovery performance of commercial forensic suites and lower-cost mass-market recovery tools, revealing material functional differences across price tiers (Buchanan-Wollaston et al., 2013). Hildebrandt et al. proposed a common evaluation scheme that combines legal and technical criteria and applied it to the imaging tools dcfldd and EnCase (Hildebrandt et al., 2011). Gupta et al. proposed an instructional framework for digital forensics training laboratories, incorporating real-case scenarios, core forensic procedures, tool selection, technical compatibility, and the minimization of image-file size (Gupta et al., 2022). In this framework, digital forensic tools were primarily selected from open-source alternatives to reduce cost, excluding commercial products such as Cellebrite and Aid4Mail; for commercial tools, the authors recommended relying on trial licenses when possible.

2.3. Tool and technology classification

The NIST Computer Forensic Tool Catalog enables vendors to directly register the technical parameters of their products and allows users to search tools and equipment based on functional capabilities (National Institute of Standards and Technology, 2026c). Wu et al. surveyed the digital forensic tool landscape across approximately 800 studies published between 2014 and 2019, classifying released tools by functional category and proposing a centralized catalog to improve tool discoverability and maintenance transparency (Wu et al., 2020). The Forensic Science Standards Library integrates dispersed standards and guidance documents, including ISO/IEC, ASTM, SWGDE, and the OSAC Registry, providing a consolidated resource to support laboratory SOP alignment and regulatory compliance (International Organization for Standardization, 2017; SWGDE, 2010; ENFSI, 2015). Mahmood et al. categorized IoT forensic frameworks by type and noted persistent limitations, including insufficient incorporation of compliance requirements (e.g., ISO standards and chain-of-custody procedures) and weak experimental validation (Mahmood et al., 2024) (Table 1).

2.4. Comparative studies on digital forensic tools

Ghazinour et al. analyzed tool attributes using a matrix-based comparison and demonstrated scenario-dependent tool performance (Ghazinour et al., 2017). Padmanabhan et al. compared open-source

Table 1
Summary of research Themes and Representative References.

Category	Key Content Summary	Representative References
Tool/Cost List	• Minimum tool/equipment sets and acquisition/maintenance cost ranges. • Cost–benefit analysis of quality programs. • Cost-saving training sets (open-source + trial versions).	(Lawrence et al., 2018; Hibshi et al., 2011; Council of Europe, 2017; INTERPOL, 2019; Nodeland and Belshaw, 2020; Supreme Prosecutors' Office, 2021; Hughes et al., 2022; Gupta et al., 2022)
Tool Selection/ Evaluation	• Functional parameter catalogs; CFTT testing. • Attribute-based comparison; compliance considerations. • Dataset-based evaluation (e.g., MDP metrics). • Metrics: accuracy, completeness, reliability, traceability. • Error typologies and legal relevance.	(National Institute of Standards and Technology, 2026c; SWGDE, 2024, 2010; O'Connor, 2005; Wu et al., 2020; Guo et al., 2009; Hildebrandt et al., 2011; Ghazinour et al., 2017; Padmanabhan et al., 2016; Stoykova et al., 2022; Voigt et al., 2025; Nordvik et al., 2021; Mahmood et al., 2024; Rzepka et al., 2025; Horsman, 2024b)
Tool Comparison	• Functional/speed/accuracy comparison across domains. • Scenario-based extraction variations; multi-tool workflows. • Anti-forensic limitations; cross-validation needs. • Systematic reviews on rooting, encryption, cloud/IoT constraints.	(Ghazinour et al., 2017; Padmanabhan et al., 2016) (Mahmood et al., 2024; Rzepka et al., 2025; Riadi et al., 2023; Bhat et al., 2021; Almuqren et al., 2024; Malik et al., 2024; Patel and Mann, 2025; Dubettier et al., 2023; Hargreaves et al., 2024b; Dubey et al., 2023; Sinaga et al., 2026; Glisson et al., 2013; Buchanan-Wollaston et al., 2013)
Facility/Space/etc	• Zoning and Workflows according to Laboratory Scale. • Environmental, security, documentation, accreditation requirements.	(Jang, 2017; Hassan, 2019; Watson and Jones, 2024; Council of Europe, 2017; INTERPOL, 2019)

(Autopsy, SIFT) and commercial (MOBILedit!, UFED) tools, showing that open-source tools may complement commercial suites (Padmanabhan et al., 2016). Prior studies have further proposed evaluation metrics for forensic tools, including speed, accuracy, completeness, reliability, and repeatability (Guo et al., 2009; Hughes and Karabiyik, 2020). Sinaga et al. comparatively evaluated Cellebrite UFED, MSAB XRY, and Magnet AXIOM in terms of artifact-extraction performance and usability (Sinaga et al., 2026), and Glisson et al. provided early empirical evidence of substantial variation in the data recovered by commercial mobile forensic toolkits (Glisson et al., 2013). Riadi et al. and Sunardi et al. analyzed MiChat and Facebook Messenger artifacts, confirming the need for multi-tool use (Riadi et al., 2023; Ardiningtias, 2022). Dubettier et al. reported inconsistencies in hidden-content processing across file-type identification tools (Dubettier et al., 2023). Bhat et al. emphasized cross-validation due to anti-forensic detection failures (Bhat et al., 2021). Additional comparative research includes Android tools (Almuqren et al., 2024), mobile extraction suites (Patel and Mann, 2025), disk-image metrics (Voigt et al., 2025), and memory-acquisition benchmarking (Rzepka et al., 2025). Collectively, these studies highlight integrity, performance, and compatibility as central metrics while noting persistent limitations in dataset availability, repeatability, and encrypted/cloud scenarios.

2.5. Digital forensics laboratory design

Jang derived the standard design for the digital evidence analysis room using police data, focus group interviews, workshops, field visits, and surveys. They established standards for each facility and environmental condition, with layouts adjusted based on personnel size (Jang, 2017). Hassan outlined physical facility requirements, environmental controls, hardware, software, furniture, consumables, validation procedures, documentation, and accreditation considerations (Hassan, 2019). Watson and Jones highlighted building selection, physical security, internal zoning, power requirements, UPS planning, and shared forensic equipment considerations (Watson and Jones, 2024). The Council of Europe (CoE) presented a basic guide to the management and procedures of DFLs. The guide describes the foundational elements necessary for operating DFLs, including budgeting, staff welfare, and the office environment. It also provides step-by-step processes for acquiring, processing, analyzing, and presenting reports on evidence from computers and mobile devices. Additionally, it addresses office equipment, such as chairs and desks, as well as hardware and software used for digital forensic analysis. Through an appendix, it provides a list of components for a device carrying case intended for field response (Council of Europe, 2017). INTERPOL has provided international standard guidelines for DFLs. Along with standards for physical security, personnel, and equipment management, it offers comprehensive standard operating procedures for evidence collection, examination, analysis, and quality assurance, as well as laboratory accreditation. Digital forensic equipment is categorized as software, hardware, tools, or accessories, and a "basic DFL equipment checklist" is provided (INTERPOL, 2019). Both the CoE and INTERPOL share the goal of ensuring the reliability and legal validity of electronic evidence by systematizing DFL operations, management, and the processes of evidence collection, analysis, and reporting. They define essential hardware and software as core resources necessary for conducting digital forensics and regard the acquisition and management of these resources as fundamental aspects of laboratory operations. However, while the CoE focuses on the selection and practical use of equipment, such as comparisons between software products or field-portable equipment sets, INTERPOL places greater emphasis on providing technical specifications and standardized equipment lists to ensure the reliability of analysis procedures.

3. Research design

3.1. Research framework

This study employed a mixed-methods research framework that integrates both qualitative and quantitative approaches. Based on the review of previous research, it begins by identifying the key factors necessary for the selection of digital forensic tools and equipment. A focus group interview was then conducted to gather additional considerations. Subsequently, on-site inspections were carried out at five institutions where DFLs had already been established (complemented by one additional practitioner interview). Following the site visits, a questionnaire was distributed to 200 current and former professionals in the field of digital forensics, resulting in 124 valid responses. Based on the findings from the focus group interview, site visits, and survey results, a draft standard list of tools and equipment along with corresponding budget estimates was developed. This draft was subsequently reviewed and refined through expert consultation with two industry professionals who had direct experience in establishing DFLs, as shown in Fig. 1.

3.2. Research methods and procedures

3.2.1. Focus group interview

The focus group interview is a qualitative research methodology in which a small group of participants engages in discussion on a specific topic to elicit a range of perspectives. The resulting data are often used to develop survey instruments and inform research design (Morgan, 1998). For this study, participant homogeneity was ensured by selecting individuals who were actively engaged in the digital forensics field at the time of the research and had experience using tools or performing

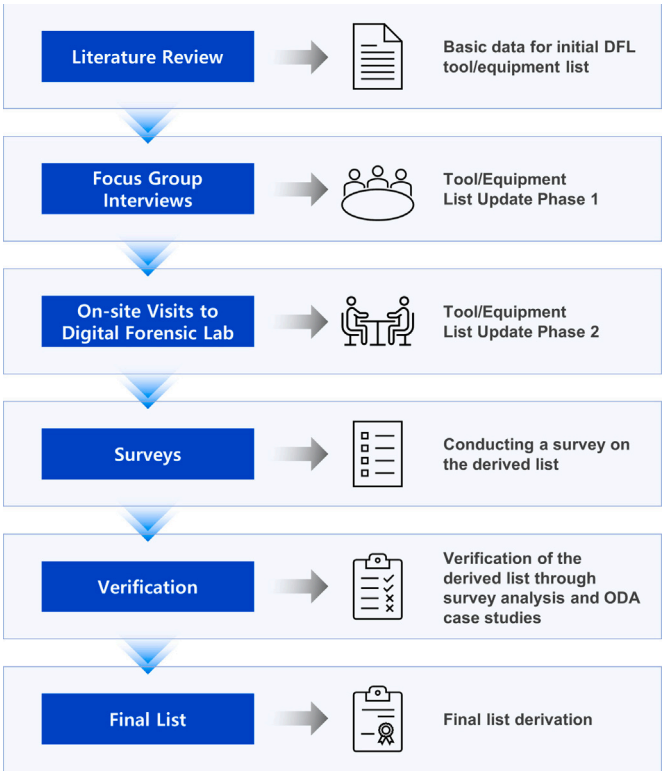


Fig. 1. Research process Overview.

Table 2
General information on FGI Participants.

No.	Gen	Age	Affiliation	Position	Exp.	Rnd
1	M	30s	Private Company	CEO	15	1
2	M	30s	Financial Supervisory Service.	Senior	9	1
3	M	40s	National Police Agency	Researcher	10	2
4	M	40s	District Prosecutors' Office	Investigator	13	2
5	M	40s	Private Company	Executive Director	14	2
6	M	40s	Provincial Police Agency	Senior Inspector	25	3
7	M	40s	Provincial Police Agency	Inspector	9	3
8	F	40s	Provincial Police Agency	Inspector	11	3
9	M	40s	Public Institution	Manager	7	4
10	M	30s	Local Government	Inspector	1	4
11	M	30s	Railway Police Unit	Inspector	4	4
12	M	40s	Railway Police Unit	Inspector	2	4

Note: Exp. = Experience (years), Rnd = Round.

forensic analysis. Recruitment was based on a list compiled by the research team, which identified candidates who met the criteria, and participation was confirmed through phone calls and emails. Drawing on practical and essential considerations, the optimal number of participants for a focus group is typically between 6 and 12 individuals. Ultimately, 12 experts were selected for this study (Morgan, 1997). Fifteen experts were initially recruited for the tool- and equipment-derivation phase of this project, as reported in our preliminary study (Shin et al., 2022). Twelve of them participated in the main focus group sessions analyzed here, while the remaining three served instead as expert reviewers of the survey instrument (see Section 3.2.4). The interviews were conducted over four sessions, held on August 10, 12, 26, and 27, 2021. The 12 experts were assigned across the four sessions, with two to four participants per session, as shown in Table 2.

The interviews were conducted remotely via video conferencing (WebEx), with informational materials shared in advance to ensure that participants were familiar with the content beforehand. The interview sessions followed a structured sequence: an explanation of the study's purpose and background, participant introductions, an overview of relevant prior research, guidance on the interview process, and then the interview itself. Each session lasted approximately two hours and was structured around nine key topics: personal tools and equipment, network configuration, analyst workstations, dedicated software, imaging devices, open-source software, tools and accessories, shared tools/equipment, and other considerations. The discussion continued until thematic saturation was reached, at which point the sessions were concluded (Shin et al., 2022). Participants in the FGI indicated that open-source software (OSS) and freeware can serve as cost-effective alternatives for underfunded organizations and complement the functionalities of commercial tools. However, some organizations were unsure about officially adopting these tools due to variations in individual preferences, rapid technological advancements, and concerns about the tools' stability and reliability that may arise during legal consultations. Despite these limitations, the most widely used tools in the field are FTK Imager for imaging, Everything for file retrieval, HashMyFiles for calculating hashes, Sysinternals Procmon for process monitoring, and SQLite for database analysis. Table 3 presents these baseline OSS/freeware tools in comparison with the corresponding commercial suite options by functional category. Prior research suggests that open-source tools, when subjected to the same validation procedures, can meet the same evidentiary standards as commercial tools (Carrier, 2002; Manson et al., 2007; Ismail and Ariffin, 2025).

Table 3
Baseline OSS/Freeware tools versus commercial Suite Options by functional category.

Function	Baseline OSS/ Freeware (License)	Commercial Suite Options
Disk/forensic imaging	FTK Imager (freeware, Exterro)	EnCase and X-Ways Forensics (built-in acquisition); Magnet AXIOM (AXIOM Process); hardware duplicators (e.g., Falcon-Neo)
File search and triage	Everything (freeware, voidtools)	X-Ways Forensics, EnCase (indexed search), Intella, Nuix, Magnet AXIOM (keyword/filter search)
Hash computation and verification	HashMyFiles (freeware, NirSoft)	Hashing functions integrated in EnCase, FTK, and AXIOM
Process and behavior monitoring	Process Monitor (freeware, Microsoft Sysinternals)	No like-for-like real-time monitoring counterpart among the surveyed commercial products
SQLite/database analysis	DB Browser for SQLite (OSS); sqlite3 CLI (public domain)	Magnet AXIOM, MD-RED, Oxygen (embedded database parsers)
Integrated analysis platform	Autopsy/The Sleuth Kit (OSS)	EnCase, FTK, Magnet AXIOM, X-Ways Forensics, Belkasoft Evidence Center

Note: Entries indicate category-level coverage rather than feature equivalence and are representative (survey-period product names), not exhaustive; a single product may cover multiple functions. OSS/freeware tools require the same validation as commercial tools under ISO/IEC 17025 before casework use (see Table 14); licensing terms for organizational use of freeware should be verified. Sources: focus group interview results (Section 3.2) and (Carrier, 2002; Manson et al., 2007; Padmanabhan et al., 2016; Ismail and Ariffin, 2025) (Hargreaves et al., 2024a).

3.2.2. Derivation of the tool/equipment pool

Through the focus group interviews, a comprehensive pool of tools and equipment required for establishing a DFL was derived. The division of tools/equipment into categories was based on the possession by individuals and teams, with the categories being computers and mobiles. Items that should be held at the organizational level were listed separately. The list includes items that individual organizations want but are restricted by budget and operational issues. It also includes products that require support from higher institutions if necessary. Common items reflect tools and equipment available to all analysts in the DFL.

Table 4
On-Site visits to DFLs and interview Summary.

No.	Type	Age	Date	Members	Method
1	LEA	30s	2021.06.18	5	On-site/Int.
2	AAA	30s	2021.09.15	4	On-site/Interview
3	LEA	40s	2021.09.17	4	Interview
4	LEA	40s	2021.09.24	4	On-site/Interview
5	LEA	40s	2021.10.11	20+	On-site/Interview
6	LEA	40s	2021.10.27	4	On-site/Interview

Note: LEA = Law Enforcement Agency, AAA = Analysis Appraisal Agency.

On-site deployment kits and imaging devices were identified during the interviews as being assigned to individuals in small organizations. However, as a result of the discussion, many people thought that they should be shared. Other items considered included evidence storage, network equipment, safety/security equipment, office equipment, facilities equipment and other items (Shin et al., 2023).

3.2.3. On-site visits and practitioner interviews in digital forensics laboratories

To understand the current state of tools and equipment in practice, on-site visits and practitioner interviews were conducted with six digital forensic organizations—five of which were examined through on-site visits, while one participated through an interview only. Five of these organizations consisted of approximately one to five personnel, and one larger organization with more than 20 members was also included, as shown in Table 4. The interview questions focused on the status of tools and equipment based on the size of the organization. The results showed that most organizations used HDD docking stations, while the use of J-Tag and Chip-Off was infrequent, being checked on an annual basis.

With the support for file-level encryption in smartphones, J-Tag and Chip-Off have become less significant. Most agreed that using J-Tag and Chip-Off in organizations with one or two personnel could be considered a waste of the budget. The use of write-blockers varied depending on whether the organization used portable or built-in devices, with some using both types, others using only portable devices, and some primarily using built-in devices. Imaging devices were typically allocated one per person, and monitors were generally in the range of 24 to 32 inches, with 2 to 4 units in use. Workstations, recently introduced, typically used Xeon Silver to Gold series processors, with higher-end models preferred. Memory was typically 128 GB, and hard drives ranged from 512 GB to 1 TB, with an additional 10 TB used separately. The cost for these systems ranged from $4666.7 to $8666.7. Some labs used USIM readers to verify phone model information during mobile analysis or maintained the information in the form of evidence reports. Most labs conducted mobile analysis, making mobile multi-chargers a requirement. Other mobile accessories, such as MD series or Cellebrite products, were either utilized when purchased or bought separately with allocated budgets. General accessories were preferred to be static-free and low wear. Tools with specialized features, such as Nuix, Chainalysis, I2, and Sentinel, were not commonly owned. Some institutions offered a digital forensics tool/equipment rental service. Field response kits were equipped with tools and devices based on support requests and the incident summary, or pre-packaged and prepared according to various operational methods. Evidence photography was conducted using camcorders or GPS watches, and some institutions operated self-made evidence authentication systems or used personal mobile phones for this purpose. Safety bags (shield packs) and anti-static bags were commonly possessed and utilized by most institutions, while Faraday bags were not available in some. Seals and labels were used to secure evidence in storage boxes, or specific areas were designated as evidence storage zones for management. NAS (Network-Attached Storage) was universally used, with institutions adapting it to their needs for storing image files or analysis results. Some institutions used self-developed digital forensics tools, and most specialized investigative agencies used CFT and DFT (64-bit). The interview results suggested a need for a contact point when supporting digital forensics work at the Supreme Prosecutor's Office. Such a contact point would provide guidance on analysis methods, CFT/DFT distribution, sharing of self-developed tools, NDFaaS, and other related matters concerning DFLs (Supreme Prosecutors' Office, 2021).

3.2.4. Survey

The questionnaire was developed based on the digital forensic tool and equipment list pool and the interview content, incorporating information from the NIST CFTT's computer forensic tools and technology catalog. For this study, two statistics specialists and three digital forensics researchers were asked to evaluate the questionnaire's validity. During the survey, data were collected on readability, the time required, fatigue from question selection and other inconveniences. This led to supplementary measures such as rearranging questions, adjusting the page layout and modifying the questionnaire. The experts reviewed the appropriateness, clarity and representativeness of each question, providing specific feedback which the researchers then used to revise the initial questionnaire. Subsequently, three rounds of final discussions were held to refine the questionnaire and ensure the reliability and validity of its content. The survey targeted individuals with experience in operating digital forensics tools and equipment, and this was reflected in the demographic questions. The survey items were structured around five primary themes: (1) preference for commercial digital forensics software, (2) preference for commercial imaging devices, (3) digital forensics tools and equipment needed at the individual level, (4) tools and equipment needed for a five-person team, and (5) the extent of digital forensics tool usage by function. To verify the content validity of the instrument, the draft questionnaire was first sent to a statistical expert for initial review and revision. A second round of evaluation was then conducted with the experts who had participated in the focus group interview. Based on the feedback received, a second revision was completed, after which the research team conducted an internal review and finalized a third round of modifications.

From September 27 to November 8, 2021, the survey was distributed to approximately 200 digital forensics professionals nationwide, and a total of 124 responses were collected. Among the respondents, 107 were male and 17 were female, showing a significantly higher proportion of males. The age distribution of respondents was as follows: 15 respondents in their 20s (12.1%), 50 in their 30s (40.3%), 51 in their 40s (41.1%), and 8 in their 50s (6.5%). The majority of respondents were in their 30s and 40s. Regarding educational background, 2 respondents held an associate degree (1.6%), 58 had a bachelor's degree (46.8%), 55 had a master's degree (44.4%), and 9 held a doctoral degree (7.3%). Thus, most respondents held either a bachelor's or master's degree. With respect to affiliation, 81 respondents (65.3%) were from investigative agencies, including the police, prosecution service, special judicial police units, the military, and the coast guard; 11 (8.9%) were from public-sector examination or supervisory institutions outside investigative agencies; 29 (23.4%) were from the private sector, including digital forensic service providers and accounting and law firms; and 3 (2.4%) were from academia. Among the respondents from investigative agencies, 55 worked in the police. For the group comparisons reported in this study, the former two categories were combined into an investigative/public-sector group ($n = 92$) and the latter two into a private-sector group ($n = 32$). In terms of digital forensics experience, 17 respondents (13.7%) had less than one year of experience; 21 (16.9%) had between one and three years; 21 (16.9%) had between three and five years; 30 (24.2%) had between five and ten years; 31 (25.0%) had between ten and twenty years; and 4 (3.2%) had twenty years or more of experience. The largest groups were those with 5–10 years and 10–20 years of experience. The collected data were analyzed using Python 3.9 (specifically, the Statsmodels and SciPy libraries). The detailed analysis procedure is as follows: First, frequency and descriptive statistical analyses were conducted to identify the general characteristics of the respondents. Additionally, a one-way analysis of variance (ANOVA) was performed to

verify differences between the investigative/public-sector and private-sector groups in the perceived necessity of tools and equipment for the one-person and five-person configurations. Homogeneity of variance was assessed with the median-centered (Brown–Forsythe) Levene test, and Welch's t-test was used for items violating the assumption. Post-hoc testing with the Scheffé test (or Dunnett's T3 for heterogeneous items) was then conducted to identify specific differences between groups. To explain the practical significance of the differences, in addition to statistical significance, effect sizes were calculated, specifically Cohen's d and Eta-squared (η^2). Inferential and multivariate analyses were also applied to identify the effects of demographic characteristics (job role and experience) on tool preference. To test for independence between the variables, a Chi-square test (χ^2) was conducted. Furthermore, a binary logistic regression analysis was performed to analyze the simultaneous effects of job role and experience on tool selection, resulting in the calculation of odds ratios. All statistical significance levels were set at $\alpha = .05$.

3.3. Survey analysis

3.3.1. Digital forensic tool/commercial imaging device preferences

The preference evaluation for digital forensic tools was conducted based on frequency averages (46.5%) and preference averages (3.27), using quadrant analysis. The digital forensic tools were categorized as follows: (1) EnCase, (2) FTK, (3) X-Ways, (4) AXIOM, (5) CFT, (6) UFED, (7) MD-Next, (8) MD-RED, (9) MacQuisition (Cellebrite Digital Collector), (10) BlackLight (Cellebrite Inspector), (11) Intella, (12) Nuix, (13) Belkasoft Evidence Center, (14) Passware Kit, (15) Final Forensic, (16) Final Mobile Forensic, (17) XRY, (18) Oxygen, (19) Forensic Explorer, (20) Sanderson Forensics, DFAS, DTsearch, Relativity. The analysis revealed that tools with high usage frequency and high preference (upper-right quadrant group) were: (1) EnCase, (2) FTK, (3) X-Ways, (4) AXIOM, (7) MD-Next, and (8) MD-RED, as shown in Fig. 2.

Considering the scatter plot, tools located near the intersection of the reference lines in the upper-right quadrant were difficult to assign significance, and thus were excluded from the list of preferred tools. The preference evaluation for commercial imaging devices was conducted using the same quadrant analysis. However, because the usage-frequency distribution was strongly skewed by a single dominant device (mean frequency rate: 33%), a fixed majority-usage threshold (50%) was applied to the frequency axis, together with the mean preference score of the evaluated devices (3.31). The commercial imaging devices were categorized as follows: (1) Falcon (Neo), (2) TX-1, (3) TaskForce, (4) TD-3, (5) SuperImager, (6) CFID, (7) PC-3000, (8) Solo (3, 4, 5), and (9) Magicube.

The analysis revealed that the device with both a high usage frequency and a high preference (upper-right category) was **Falcon (Neo)**, as shown in Fig. 3.

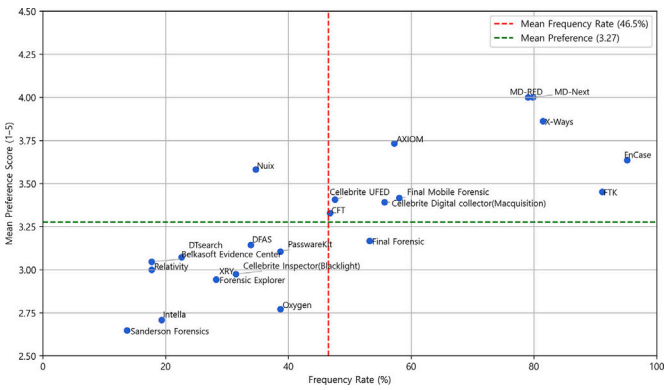


Fig. 2. Overall digital forensic tool preferences.

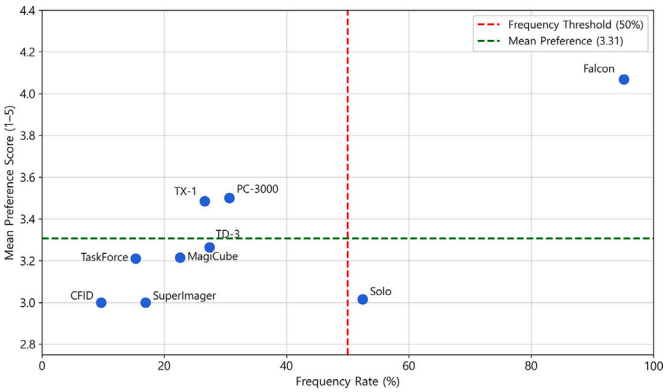


Fig. 3. Imaging device preference.

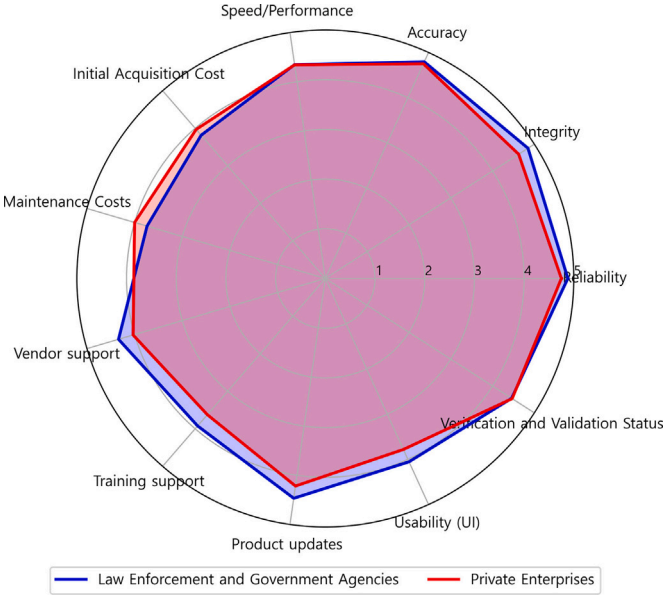


Fig. 4. Considerations when selecting digital forensics SW.

3.3.2. Evaluation factors for purchasing/adopting digital forensic software

The survey respondents were categorized into law enforcement/public sector and private sector groups to analyze the importance of evaluation factors when purchasing or adopting digital forensic software. The evaluation factors were categorized into eleven items: Speed/Performance, Accuracy, Integrity, Reliability, Verification and Validation Status, Usability, Product Updates, Training Support, Vendor Support, Maintenance Cost, and Initial Acquisition Cost. According to the survey results, the most important factors were **reliability**, **integrity**, and **accuracy**, in that order, as shown in Fig. 4.

3.3.3. Tool preference by job role

The preference for digital forensic tools was analyzed based on the respondents' job roles. As respondents were allowed to select multiple job roles they had experienced, the total number of responses in Table 5 exceeds the total number of respondents (N = 124). The categories of job roles were defined as follows: (A) Policy & Planning, (B) Consulting & Advisory, (C) Budget Management, (D) Procurement & Equipment Management, (E) Digital Forensic Analysis, (F) Education & Lecture, and (G) Research & Development, as shown in Table 5.

Digital forensic tools were categorized as follows: (1) EnCase, (2) FTK, (3) X-Ways, (4) AXIOM, (5) CFT, (6) UFED, (7) MD-Next, (8) MD-RED, (9) Cellebrite Digital Collector (MacQuisition), (10)

Table 5
Job roles of survey respondents (multiple responses allowed).

Job role	People	Percent (%)
Policy Planning	15	6.6%
Digital Forensic Analysis	93	40.6%
Consulting & Advisory	14	6.1%
Education & Lecture	47	20.5%
Budget Management	4	1.7%
Research & Development	35	15.3%
Procurement & Equipment Management	21	9.2%
Total	229	100.0%

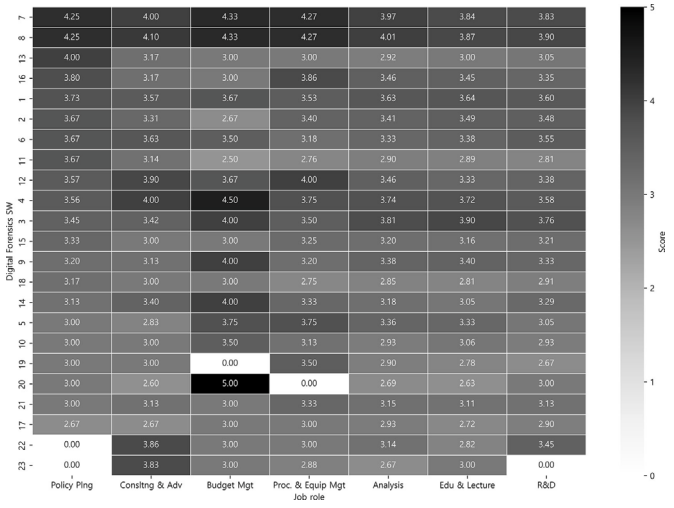


Fig. 5. Average digital forensic tool preferences by job role.

Cellebrite Inspector (BlackLight), (11) Intella, (12) Nuix, (13) Belkasoft Evidence Center, (14) Passware Kit, (15) Final Forensics, (16) Final Mobile Forensics, (17) XRY, (18) Oxygen, (19) Forensic Explorer, (20) Sanderson Forensics, DFAS, DTsearch, and Relativity.

The survey allowed respondents to select multiple tools for the same item, and the average tool preference by job role was calculated and compared, as shown in Fig. 5.

Blank spaces in the table represent "Never used," indicating that no preference score was assigned to that item. The tool preferences by job role are summarized below:

- **Policy & Planning**: (7) MD-Next, (8) MD-RED, (13) Belkasoft Evidence Center, (16) Final Mobile Forensics, (1) EnCase
- **Consulting & Advisory**: (8) MD-RED, (4) AXIOM, (7) MD-Next, (12) Nuix, DTsearch
- **Budget Management**: (20) Sanderson Forensics, (4) AXIOM, (7) MD-Next, (8) MD-RED, (3) X-Ways
- **Procurement & Equipment Management**: (7) MD-Next, (8) MD-RED, (12) Nuix, (16) Final Mobile Forensics, (4) AXIOM
- **Digital Forensic Analysis**: (8) MD-RED, (7) MD-Next, (3) X-Ways, (4) AXIOM, (1) EnCase
- **Education & Lecture**: (3) X-Ways, (8) MD-RED, (7) MD-Next, (4) AXIOM, (1) EnCase
- **Research & Development**: (8) MD-RED, (7) MD-Next, (3) X-Ways, (1) EnCase, (4) AXIOM

Upon reviewing tool preference priorities across job role categories, it was observed that the following tools consistently emerged as preferred across multiple domains: **(8) MD-RED, (7) MD-Next, (4) AXIOM, (3) X-Ways, and (1) EnCase**.

3.3.4. One-person vs. Five-person tool/equipment analysis

The tool and equipment preferences for one-person and five-person teams were examined using frequency analysis and variance analysis. In the frequency analysis, responses were converted to numerical values: "Very necessary" (5), "Necessary" (4), "Neutral" (3), "Not necessary" (2), and "Hardly necessary" (1). Average scores and rankings were then calculated. For one-person requirements, the workstation for evidence collection and analysis produced the highest average score (4.80), while the office laptop yielded the lowest (3.38). For five-person teams, the same workstation type showed the highest score (4.53), whereas the office desktop PC showed the lowest score (3.72), as summarized in Table 6.

Levene's test for homogeneity of variance was first conducted to assess variance equality. For items that satisfied the assumption, a one-way analysis of variance (ANOVA) was performed; for items violating the assumption, independent-samples *t*-tests were applied. When the *p*-value was below 0.05, Scheffé or Dunnett's T3 post-hoc tests were employed to control for multiple comparison errors in Table 7.

Based on the ANOVA and Scheffé post-hoc results, the investigative/public-sector group reported significantly higher perceived necessity than the private-sector group for several tools: office desktop PC ($F = 8.77$, $p = 0.004$, $\eta^2 = 0.067$), damaged video/CCTV recovery and analysis ($F = 15.79$, $p < 0.001$, $\eta^2 = 0.115$), and Hex Editor ($F = 5.63$, $p = 0.019$, $\eta^2 = 0.044$). These findings suggest that such tools are essential in the preprocessing stages of frontline investigations. The same analytical procedure was applied to the five-person laboratory configuration. For the item "Shared evidence-collection/analysis laptop," Levene's test indicated heterogeneity of variances; thus, an independent-samples *t*-test was conducted, revealing a significant difference ($p = 0.043$). Dunnett's T3 post-hoc test showed that the private-sector group expressed relatively greater perceived necessity than the investigative/public-sector group ($t = -2.057$). For the items "air purifier, color laser printer, temperature–humidity control unit, dryer (mobile-device drying), air

Table 6
Frequency analysis of required Tools/Equipment (Individual versus Five-member Teams).

Category	Individual							5-Member Teams						
	A	B	C	D	E	Avg	Rank	A	B	C	D	E	Avg	Rank
Workstation for Evidence Collection and Analysis	102	19	3	0	0	4.80	1	84	27	9	3	1	4.53	1
Laptop for Evidence Collection and Analysis	66	42	15	0	1	4.39	6	68	37	9	7	3	4.29	5
PC for Evidence Collection and Analysis	61	30	20	5	8	4.06	7	58	34	17	10	5	4.05	7
Office Laptop	22	32	51	9	10	3.38	9	44	32	27	13	8	3.73	8
Office Desktop PC	28	35	47	7	7	3.56	8	44	33	24	14	9	3.72	9
Monitor	90	23	10	0	1	4.62	5	53	43	16	8	4	4.07	6
Computer Forensic Analysis Software	102	19	2	0	1	4.78	4	69	37	14	3	1	4.37	3
Mobile Evidence Acquisition Software	104	15	4	1	0	4.79	2.5	72	34	13	4	1	4.39	2
Mobile Evidence Analysis Software	104	15	4	1	0	4.79	2.5	71	33	15	4	1	4.36	4

Response categories: A = "Very necessary" (5), B = "Necessary" (4), C = "Neutral" (3), D = "Not necessary" (2), E = "Hardly necessary" (1); cell values are response counts (N = 124 per configuration), and Avg is the mean of the coded values.

Table 7
ANOVA and Post-hoc test results for perceived necessity of Tools/Equipment: Investigative/Public-Sector vs. Private-Sector Groups.

Item	Mean (M)		F/t	Post-hoc	Diff.	S.E.	*p*	95% CI		Cohen's *d*	η^2	Effect *f*
	A	B			(A–B)			L	U			
Required Tools/Equipment per Person												
Office Desktop PC	3.73	3.09	8.773*	S	0.63	0.21	.004*	0.21	1.06	0.608	0.067	0.268
Damaged Video/CCTV Recovery SW	4.17	3.31	15.793*	S	0.86	0.22	<.001*	0.43	1.29	0.816	0.115	0.360
Hex Editor	4.27	3.78	5.634*	S	0.49	0.21	.019*	0.08	0.90	0.487	0.044	0.215
Required Shared Tools/Equipment for Five People												
Laptop (Evidence Collection/Analysis)	4.20	4.56	−2.057*	D	−0.37	0.18	.043*	−0.72	−0.01	−0.372	0.026	0.164
Air Purifier	4.34	3.75	9.924*	S	0.59	0.19	.002*	0.22	0.96	0.647	0.075	0.285
Color Laser Printer	4.07	3.59	6.354*	S	0.47	0.19	.013*	0.10	0.84	0.517	0.050	0.228
Temp. & Humidity Control Device	4.02	3.56	5.562*	S	0.46	0.19	.020*	0.07	0.84	0.484	0.044	0.214
Hair Dryer (Mobile Phone Drying)	3.72	3.25	4.770*	S	0.47	0.21	.031*	0.04	0.89	0.448	0.038	0.198
Air Compressor	3.57	3.16	4.452*	S	0.41	0.19	.037*	0.03	0.79	0.433	0.035	0.191
Electric Driver	4.25	3.81	5.768*	S	0.44	0.18	.018*	0.08	0.80	0.493	0.045	0.217
JTAG Emulator	4.02	3.38	9.216*	S	0.65	0.21	.003*	0.23	1.07	0.623	0.070	0.275
Soldering Equipment Set	3.75	3.28	4.251*	S	0.47	0.23	.041*	0.02	0.92	0.423	0.034	0.187
Chip-Off Device	3.84	3.19	8.068*	S	0.65	0.23	.005*	0.20	1.10	0.583	0.062	0.257
Chip Reader	3.92	3.44	5.026*	S	0.49	0.22	.027*	0.06	0.92	0.460	0.040	0.203

Note: M = Mean; A = Investigative/public-sector group; B = Private-sector group; F/t = *F* statistic for ANOVA items (Scheffé post-hoc) or *t* statistic for items analyzed with independent-samples *t*-tests (Dunnett T3); Post-hoc: S = Scheffé, D = Dunnett T3; Diff. = Mean Difference (A–B); SE = Standard Error; CI = Confidence Interval (L = Lower, U = Upper); * $p < .05$. All statistics were recomputed from the raw survey responses: variance homogeneity was assessed with the median-centered (Brown–Forsythe) Levene's test; homogeneous items were analyzed with one-way ANOVA (Scheffé), heterogeneous items with Welch's *t*-test (Dunnett T3); Cohen's *d* uses the pooled standard deviation, $\eta^2 = SS_{between}/SS_{total}$, and effect $f = \sqrt{\eta^2/(1-\eta^2)}$.

Table 8
Required number of Workstations, Laptops, and PCs (Individual vs. Five-member Teams).

Item	Individual						5-Member Teams					
	A	B	C	D	E	Avg	A	B	C	D	E	Avg
(1)	3	13	56	51	1	1.726	32	31	40	17	4	2.565
(2)	1	1	14	104	4	1.121	30	20	40	25	9	2.298
(3)	1	3	17	85	18	1.065	35	20	32	23	14	2.315
(4)	1	0	3	86	34	0.774	20	9	28	52	15	1.734
(5)	1	0	4	104	15	0.935	20	8	25	53	18	1.669

Item definitions: (1) = Workstations for Evidence Collection & Analysis, (2) = Laptops for Evidence Collection & Analysis, (3) = PCs for Evidence Collection & Analysis, (4) = Office Laptops, (5) = Office PCs. Response categories: A = "4 or more" (coded 4), B = "3", C = "2", D = "1", E = "not needed" (coded 0); cell values are response counts (N = 124 per configuration), and Avg is the mean of the coded values.

Table 9
Paired t-test and Cohen's D results (Individual vs. Five-Member Teams).

Item Pairs	Mean Diff	p-value	Cohen's d	Effect Size
1P-01 vs 5P-01	−0.839	<.001	-0.666	M
1P-02 vs 5P-02	−1.177	<.001	-0.984	L
1P-03 vs 5P-03	−1.250	<.001	-0.992	L
1P-04 vs 5P-04	−0.960	<.001	-0.783	M~L
1P-05 vs 5P-05	−0.734	<.001	-0.581	M

1P = one-person criterion, 5P = five-person criterion. Effect size categories: S = small, M = medium, L = large (Cohen's d).

compressor, electric screwdriver, JTAG emulator, soldering kit, chip-off device, and chip reader," the homogeneity assumption was satisfied. ANOVA followed by Scheffé post-hoc tests indicated that the investigative/public-sector group assigned higher importance to these tools, reflecting their greater need for controlled preprocessing environments when handling digital evidence. The corresponding η^2 values reflected medium-sized effect magnitudes. A post-hoc power analysis was conducted using G*Power 3.1, based on the total sample of 124 respondents (investigative/public-sector group = 92; private-sector group = 32). With a medium effect size ($f = 0.29$, $\eta^2 = 0.08$) and $\alpha = 0.05$, the statistical power ($1 - \beta$) was approximately 0.87. This indicates that the significant results obtained in this study are supported by sufficient statistical power.

Frequency analysis was also conducted on the number of required workstations, laptops, PCs, office laptops, and office PCs for one-person and five-person teams, as shown in Table 8.

The results indicated that, based on the most frequently selected response category for each item, two analysis workstations were required. One analysis laptop was required for one-person setups and two for five-person teams. One analysis PC was required for one-person setups and four or more for five-person teams. One office laptop and one office PC were required for both configurations. Average scores for each item were compared between one-person and five-person teams in Table 9.

All items showed significantly higher average scores for the five-person configuration ($p < 0.001$). In particular, differences in the number of evidence collection and analysis laptops and PCs between one-person and five-person setups demonstrated Cohen's d values of −0.984 and −0.992, respectively, indicating very large effect sizes. These findings suggest a substantially higher demand for shared equipment in five-person teams.

For digital forensic tools required by a single practitioner, the survey used a multiple-response format. EnCase recorded the highest selection frequency (116 responses), followed by X-Ways, FTK, and AXIOM, as illustrated in Fig. 6. Respondents also recommended the inclusion of external analysis utilities not listed in the survey. For mobile forensic tools, MD-RED, MD-Next, Final Mobile Forensic, UFED, and AXIOM were the most frequently selected.

3.3.5. Tool usage by analysis target and function

The usage of digital forensic tools by analysis target and functional category was examined. The analysis categories were derived from the NIST *Computer Forensics Tools & Techniques Catalog*, as summarized in Table 10.

- Analysis Targets: Image Forensics (Video & Graphics), Mobile Forensics (Acquisition, Analysis, Triage), Social Media Forensics, Video (Film) Analysis Forensics, VoIP Forensics, Communication & Account Forensics.
- Functions: Hardware Write Blocking, Image Analysis (Video & Graphics), Video Format Conversion.

Post-analysis revealed significant differences across several analysis targets and tool functions, as shown in Table 11. The Remote

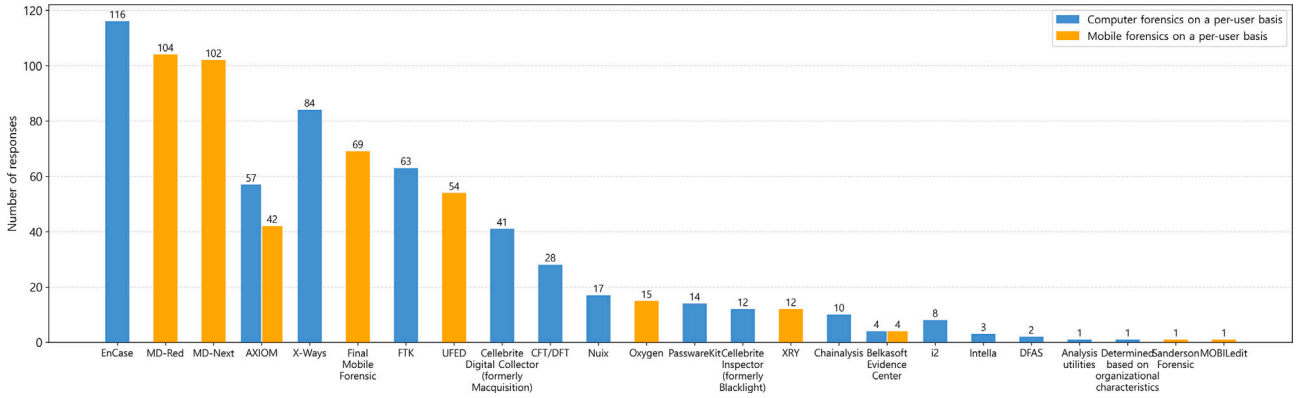


Fig. 6. Digital forensic SW to be provided to individuals.

Table 10
Categorization of tools and equipment by analysis targets and functions.

Analysis Targets	Functions
• Cloud Service Forensics • Database Forensics • Drone Forensics • Computer Forensics (Mac) • Computer Forensics (Windows) • GPS Forensics • Image Forensics (Video & Graphics) • Infotainment & Vehicle Forensics • Instant Messenger Forensics • Mobile Forensics (Acquisition, Analysis, Triage) • P2P Forensics • Social Media Forensics • Video (Film) Analysis Forensics • VoIP Forensics • Cryptocurrency Forensics • Communication & Account Forensics	• Data Analysis • Deleted File Recovery • Disk Cataloging • Disk Imaging • Email Parsing • File Carving • Forensic File Copying • Hardware Write Blocking • Software Write Blocking • Hash Analysis • Image Analysis (Video & Graphics) • Incident Response Forensics • Live Response Forensics • Complete Media Erasure/Drive Reuse • Memory Capture & Analysis • File Password Recovery • Remote Forensics • Steganography Analysis • String Search • Video Format Conversion • Web Browser Analysis • WiFi Analysis • Windows Registry Analysis • Forensic Boot Environment (Live CD/USB)

Function/Remote Forensics function was used more by the private sector group than the law enforcement group. Overall, the law enforcement/investigation group was found to use digital forensic analysis tools for image, mobile, social media, VoIP, and communication/account forensics more frequently than the private sector group. In the image forensics category, the results indicated that the investigative/public-sector group demonstrated a significantly higher perceived need for the relevant tools compared with the private-sector group ($F = 8.024$, $p = 0.005$, $\eta^2 = 0.062$). In mobile forensics, the difference between the two groups was statistically significant ($t = 2.311$, $p = 0.026$, $\eta^2 = 0.062$). The investigation/examination agency group tended to require slightly more tools. In video analysis forensics in particular, Cohen's $d = 0.969$ indicated a substantial effect size, with $F = 22.308$, $p < 0.001$, and $\eta^2 = 0.155$. This supported the conclusion that the investigation/examination agency group's need for tools was significantly higher than that of the private group. Conversely, in remote function/remote forensics items, private groups tended to use more tools than investigation/examination agency groups, with statistically significant differences ($t = -2.132$, $p = 0.039$, Cohen's $d = -0.496$). This suggests that private groups utilise certain tools more frequently. Therefore, investigation/examination agency groups tend to use image forensics, mobile forensics, social media forensics, VoIP forensics, and communication and account forensics relatively more than private groups. These results suggest that the investigative/examination agencies make essential use of digital forensic tools in the pre-processing stage, indicating that the private groups tend to use fewer of these tools.

3.3.6. Analysis of tool preferences by role and experience

As a result of multivariate logistic regression analysis and Chi-square tests, preferences for digital forensics tools tended to be largely categorized into 'universal standard tools' and 'job and career-dependent tools', as shown in Table 12.

Universal Standard Tools: A statistically significant correlation with job or career variables was not shown for major tools with high market shares, such as EnCase ($p = 0.568$), AXIOM ($p = 0.799$), and Cellebrite UFED ($p = 0.673$). This suggests that these tools are essential regardless of the analyst's proficiency or the nature of their tasks (analysis versus administration). Therefore, the absence of role- or experience-dependent variation indicates that the high usage frequency of these tools reflects their function as de facto common equipment regardless of laboratory type, which supports their prioritization in baseline budgeting.

Job and Experience-Based Preference Tools: Certain tools exhibited distinct preference differences based on respondents' job roles. The "Technical Analyst" group demonstrated a statistically significant preference for the file system deep analysis tool, X-Ways Forensics (Coefficient = 1.655, $p < 0.05$), and the mobile data acquisition tools, MD-Next/RED (Coefficient $\approx$ 1.3, $p < 0.05$). In contrast, Relativity, an eDiscovery and review platform, exhibited a negative coefficient (Coefficient = −1.728, $p < 0.05$), indicating a relatively higher preference within the "Administrative and Planning" group. These results highlight the different equipment characteristics required for high-level analysis tasks versus data management and review tasks. Furthermore, experience-based preference tools, such as X-Ways Forensics, DFT, and Oxygen Forensics, showed significant positive correlations with career variables ($p < 0.05$); DFT is omitted from Table 12, which reports selected significant items only. This suggests that these tools require high proficiency or offer advanced features favored by experienced analysts.

4. Research results

4.1. Digital forensic tools and equipment lists for one-person and five-person teams

The final lists of required tools and equipment for one-person and five-person digital forensic teams were derived from the analyses presented in the previous sections. These lists are intended to assist organizations in establishing or upgrading DFLs. Table 13 presents the consolidated items.

Items that can be bundled together or exhibit minimal cost differences at the procurement stage were grouped into set configurations.

Table 11
ANOVA and Post-hoc test results by analysis Target and analytical Function: Investigative/Public-Sector vs. Private-Sector Groups.

Item	Mean (M)		F/t	Post-hoc	Diff.	S.E.	*p*	95% CI		Cohen's *d*	η^2	Effect *f*
	A	B			(A–B)			L	U			
Analysis Targets												
Image Forensics (Video & Graph.)	3.43	2.72	8.024*	S	0.72	0.25	005*	0.22	1.22	0.581	0.062	0.256
Mobile Forensics (Acq/Anal/Tri)	4.65	4.09	2.311*	D	0.56	0.24	026*	0.07	1.05	0.584	0.062	0.258
Social Media Forensics	3.23	2.62	4.290*	S	0.60	0.29	040*	0.03	1.18	0.425	0.034	0.188
Video (Film) Analysis Forensics	3.70	2.47	22.308*	S	1.23	0.26	<.001*	0.71	1.74	0.969	0.155	0.428
VoIP Forensics	2.22	1.78	4.202*	S	0.44	0.21	043*	0.01	0.86	0.421	0.033	0.186
Comm. & Account Forensics	2.70	2.16	2.179*	D	0.54	0.25	033*	0.05	1.03	0.408	0.031	0.180
Functions												
Hardware Write Blocking	4.40	3.97	4.088*	S	0.43	0.21	045*	0.01	0.86	0.415	0.032	0.183
Image Analysis (Video & Graph.)	3.85	2.94	12.785*	S	0.91	0.25	001*	0.41	1.41	0.734	0.095	0.324
Remote Forensics	2.27	2.81	−2.132*	D	−0.54	0.25	039*	−1.05	−0.03	−0.496	0.046	0.219
Video Format Conversion	3.03	2.31	7.518*	S	0.72	0.26	007*	0.20	1.24	0.563	0.058	0.248

Note: M = Mean; A = Investigative/public-sector group; B = Private-sector group; F/t = *F* statistic for ANOVA items (Scheffé post-hoc) or *t* statistic for items analyzed with independent-samples *t*-tests (Dunnett T3); Post-hoc: S = Scheffé, D = Dunnett T3; Diff. = Mean Difference (A–B); SE = Standard Error; CI = Confidence Interval (L = Lower, U = Upper); * $p < .05$. All statistics were recomputed from the raw survey responses using the same procedure as in Table 7.

Table 12
Statistical analysis results of tool preferences by experience and role (Selected significant Items).

Tool Name	Chi-Square Test		Logistic Regression Analysis			
	p-value	Cramer's V	Exp. *p*-value	Role *p*-value	Role Coef.[a]	Interpretation
***Standard Tools** (No Significant Differences)*						
EnCase	0.755	0.146	0.841	0.568	−0.327	Universal
AXIOM	0.396	0.204	0.694	0.799	0.151	Universal
Cellebrite UFED	0.308	0.220	0.098	0.673	−0.272	Universal
Tools with Significant Dependencies						
X-Ways Forensics	0.057	0.294	**0.005****	**0.012***	1.655	Analyst/Senior
MD-Next	0.418	0.200	0.921	**0.028***	1.307	Analyst Pref.
MD-RED	0.364	0.210	0.831	**0.032***	1.271	Analyst Pref.
Relativity	0.778	0.142	0.522	**0.031***	−1.728	Manager Pref.
Nuix	**0.025***	0.321	0.082	0.125	−0.963	Exp. Dependent
Oxygen Forensic	0.087	0.278	**0.033***	0.808	−0.302	Exp. Dependent

[a]Positive Coefficient (+) indicates preference by Technical Analysts; Negative (−) indicates Administrative/Managers.
* $p < 0.05$, ** $p < 0.01$.

Although not every item may be necessary for all institutions, the lists were designed to capture a broad and standardized range of requirements applicable to both one-person and five-person laboratory environments. Open-source tools, which do not incur licensing costs, were excluded from the cost estimates. During the analysis process, unit prices were verified, and the reliability of market estimates was enhanced through validation by two domestic industry experts. The results indicated that the estimated construction costs were approximately USD 300,794.8 for a one-person laboratory and USD 585,699.9 for a five-person laboratory (based on an exchange rate of 1 USD = 1500 KRW).

Furthermore, to mitigate the limitations of the survey, actual procurement data (RFP/ODA) were analyzed to filter out theoretical items lacking practical delivery records. This empirical approach identified the essential tools and equipment for actual laboratory construction and facilitated the definition of five maturity levels (Levels 1–5). Level 1 refers to a state requiring new construction; Level 2, where only space has been secured; Level 3, where furniture and basic materials are provided; Level 4, where partial computer equipment has been acquired; and Level 5, where full infrastructure is established. Based on the necessity of introducing equipment at each stage, items were prioritized as Mandatory, Recommended, or Optional.

4.2. Application case comparison and validity assessments

To verify the effectiveness of the derived items, the actual procurement details of state agencies were analyzed. Specifically, 62 cases of Requests for Proposals (RFPs) related to the construction of DFLs and the supply of equipment, announced by the Korea Public Procurement Service (KONEPS) from January 2015 to December 2025, were collected. Survey results were cross-referenced with these procurement lists. Items common to both datasets were incorporated into the final list, while items identified in the survey lacking a history of actual delivery were excluded to ensure realism. The analysis revealed that public orders primarily consisted of lab construction, IT equipment, furniture, and dedicated tools, ordered either individually or in integrated forms. To validate global applicability, the delivery details of ODA DFL construction projects in five countries (Vietnam, Indonesia, Mongolia, Bangladesh, and Nepal) were also analyzed. As illustrated in Fig. 7, this study employed a **triangulation verification method** to map these empirical datasets against the derived items and international standards. The analysis visualized the flow from the procurement timeline and organizations to specific equipment categories, grouping them into seven major domains (e.g., Computer Forensics, Mobile Forensics, Lab Facility). This process confirmed that the derived items have been consistently demanded by major public agencies over the past decade. Furthermore, the final list was mapped against twelve international standards and guidelines, including ISO/IEC 17025, the NIST SP series, and SWGDE, to ensure compliance with global quality and procedural requirements.

5. Discussion and implications

5.1. Implications

5.1.1. Budgetary implications

When budgeting for a digital forensics environment, it is important to consider not only cost efficiency, but also whether the proposed tools and equipment meet legal evidence capability requirements. Legal

Table 13
Detailed Specification and price analysis.

Group	Category	Item	Unit	Price (USD)	Individual		5-Member		DFL Level					Ref.
					Qty	Amt	Qty	Amt	1	2	3	4	5	
Section A: Computer Domain														
1	Computer HW	Workstation (Write Blocker)	EA	10,000.0	2	20,000	5	50,000	M	M	M	R	R	(1,3,4,7,9,11,12)
		Monitor (Privacy Filter)	EA	266.7	6	1600.2	15	4000.5	M	M	M	R	R	(2,6,11,12)
		Office Desktop PC (OS, Office)	EA	666.7	2	1333.4	3	2000.1	M	M	M	R	R	(1,9,11,12)
		Office Laptop (OS, Office)	EA	2000.0	2	4000	3	6000	M	M	M	R	R	(1,9,11,12)
	Computer Forensic SW	EnCase	Copy	5333.3	1	5333.3	1	5333.3	M*	M*	M*	M*	M*	(4,7,9)
		AXIOM	Copy	7333.3	1	7333.3	1	7333.3	M*	M*	M*	M*	M*	(4,7,9)
		X-Ways	Copy	3066.7	1	3066.7	1	3066.7	M*	M*	M*	M*	M*	(4,7,9)
		FTK	Copy	5666.7	0	0	1	5666.7	M*	M*	M*	M*	M*	(4,7,9)
	Support	VMware	Copy	533.3	2	1066.6	2	1066.6	M	M	M	M	M	(10,12)
	Accessories	Driver Kit	Set	146.7	1	146.7	3	440.1	M	M	M	M	M	(3,11,12)
		Docking Station (HDD, M.2)	EA	‡	1	113.4‡	3	273.5‡	M	M	M	M	M	(3,9,12)
		Cables	Set	33.3	1	33.3	3	99.9	M	M	M	M	M	(3,11,12)
		HDD (Evidence, TB)	EA	‡	5	1283.5‡	20	3234‡	M	M	M	M	M	(4,9,11,12)
		External SSD (TB)	EA	366.7	4	1466.8	10	3667	M	M	M	M	M	(3,9,11,12)
		USB Drive (GB)	EA	66.7	20	1334	20	1334	M	M	M	M	M	(5,9,12)
		DVD/ODD/KVM Switch	Set	‡	1	483.3‡	3	1249.9‡	M	M	M	M	M	(1,5,9)
Section B: Mobile Domain														
2	Mobile Forensic SW	MD-Next	Copy	22,000	1	22,000	2	44,000	M*	M*	M*	M*	M*	(4,5)
		MD-RED	Copy	56,666.7	1	56,666.7	2	113,333.4	M†	M†	M†	M†	M†	(4,5)
		Cellebrite UFED	Copy	19,333.3	1	19,333.3	2	38,666.6	M†	M†	M†	M†	M†	(4,5)
		Final Mobile Forensic	Copy	66,666.7	1	66,666.7	2	133,333.4	M†	M†	M†	M†	M†	(4,5)
		Analysis Tools (On-Site)	Copy	30,000	1	30,000	2	60,000	M†	M†	M†	M†	M†	(5,9)
	Accessories	Cables/Reader/Multi-Charger	Set	266.7	1	266.7	3	800.1	M	M	M	M	M	(9,11,12)
Section C: Special and Common Domain														
3	Field Kit	Laptop/Tools/Bags/Media	Set	4666.7	2	9333.4	4	18,666.8	M	M	M	R	R	(3,9,11,12)
4	Special	IoT/Crypto/AI Tools	Set	$+\alpha$	–	–	–	–	R	R	R	R	R	(3,4)
5	Photo	Camcorder/GPS/Lighting	Set	1733.3	1	1733.3	1	1733.3	M	M	R	R	R	(9,11,12)
		Evidence Display/Capture Board	EA	266.7	1	266.7	1	266.7	M	M	R	R	R	(9,11,12)
	Imaging	Falcon Neo	EA	5866.7	1	5866.7	3	17,600.1	M†	M†	R†	R†	R†	(3,4,7,9,10,11,12)
		TX-1	EA	4333.3	1	4333.3	2	8666.6	M†	M†	R†	R†	R†	(3,4,7,9,10,11,12)
	Reception	Faraday, Anti-Static, Labels, etc.	Set	1433.3	1	1433.3	1	1433.3	M	M	M	M	M	(3,5,9,10,11,12)
	Storage	Evidence Storage Boxes	Set	100	1	100	3	300	M	M	M	M	M	(3,9,10,11,12)
		Evidence Cabinets	EA	400	1	400	3	1200	M	M	M	M	M	(1,9)
		Tool Cabinets	EA	400	2	800	4	1600	R	M	M	M	M	(1)
		Fireproof Safe	EA	533.3	1	533.3	2	1066.6	M	M	M	M	M	(1,9)
6	IT/Network	Switch/Router/Rack	Set	3666.6	1	3666.6	1	3666.6	M	M	R	R	R	(1,7,9)
		NAS (with HDD)	Unit	3333.3	1	3333.3	1	3333.3	M	M	R	R	R	(7,8,9,10,11,12)
		Color Printer	Unit	400	1	400	3	1200	M	M	M	R	R	(1,12)
	Security	CCTV (Camera/Monitor/NVR)	Set	1933.4	1	1933.4	1	1933.4	M	M	R	R	R	(1,6,12)
		Door Lock	Unit	200	2	400	2	400	M	M	R	R	R	(1,6,12)
7	Observation	LED TV (Included KB/Mouse)	Unit	2733.4	1	2733.4	1	2733.4	M	M	R	O	O	(1,9)
		Video Switch	Unit	2000	1	2000	1	2000	M	M	R	O	O	(1)
	Office	Desk (Forensic Main/Assistant)	Set	600.0	2	1200	10	6000	M	M	R	O	O	(1,11,12)
		Chairs (Office/Conference/Observation)	EA	266.7	6	1600.2	21	5600.7	M	M	R	O	O	(1,11,12)
		Table (Conference/Observation)	EA	266.7	1	266.7	2	533.4	M	M	R	O	O	(1,11,12)
		Large TV (Conference)	EA	2666.7	0	0	1	2666.7	M	M	R	O	O	(1,11,12)
		Refrigerator/Air purifier/Etc	Pkg	‡	‡	1600‡	‡	4866.6‡	M	M	R	O	O	(1,11)
	Interior	Interior/Network Construction	Pkg	13,333.3	1	13,333.3	1	13,333.3	M	M	R	O	O	(1,9)
Total Prices (USD)						**300,794.8**		**585,699.9**						

Special: Nuix, Relativity, Amped Five·Authenticate, Magnet Witness (DVR Examiner), Chainalysis, X1 Search, Cyber Triage, Passware Kit, etc. / ‡ Prices and quantities vary by item. **DFL Level: Level 5 (Isolated Lab)** - Fully equipped office retrofitted for an isolated network and independent security environment; **Level 4 (Shared IT)** - Furnished space with general IT, utilizing shared building infrastructure; **Level 3 (Shared Furnished)** - Furnished space utilizing shared infrastructure (requires IT); **Level 2 (Shared Basic)** - Empty secured space utilizing shared infrastructure (requires furniture/IT); **Level 1 (New)** - Newly constructed facility from scratch. **Legend:** M (Mandatory): Essential for operations—initial procurement for new labs (L1–L3) or critical renewals/consumables for existing labs (L4–L5); R (Recommended): Improves efficiency—leveraging shared infrastructure (L4) or replacing aging equipment (L5); O (Optional): Budget-dependent expansion; * (Cross-validation): Select 1–2 items within the category to ensure analytical reliability (e.g., Computer Forensics); †(Alternatives): Select at least 1 item among alternatives due to cost or functional overlap (e.g., Mobile Forensics). **References:** (1) ISO/IEC 17025, (2) ISO/IEC 27002, (3) ISO/IEC 27037, (4) NIST CFTT, (5) NIST SP 800-101r1, (6) NIST SP 800-53 (PE), (7) NIST SP 800-86, (8) NIST SP 800-88r1, (9) SWGDE Best Practices, (10) NIST SP 800-201, (11) INTERPOL Global guidelines for DFL, (12) Council of Europe, A Basic Guide for the Management and Procedures of a DFL.

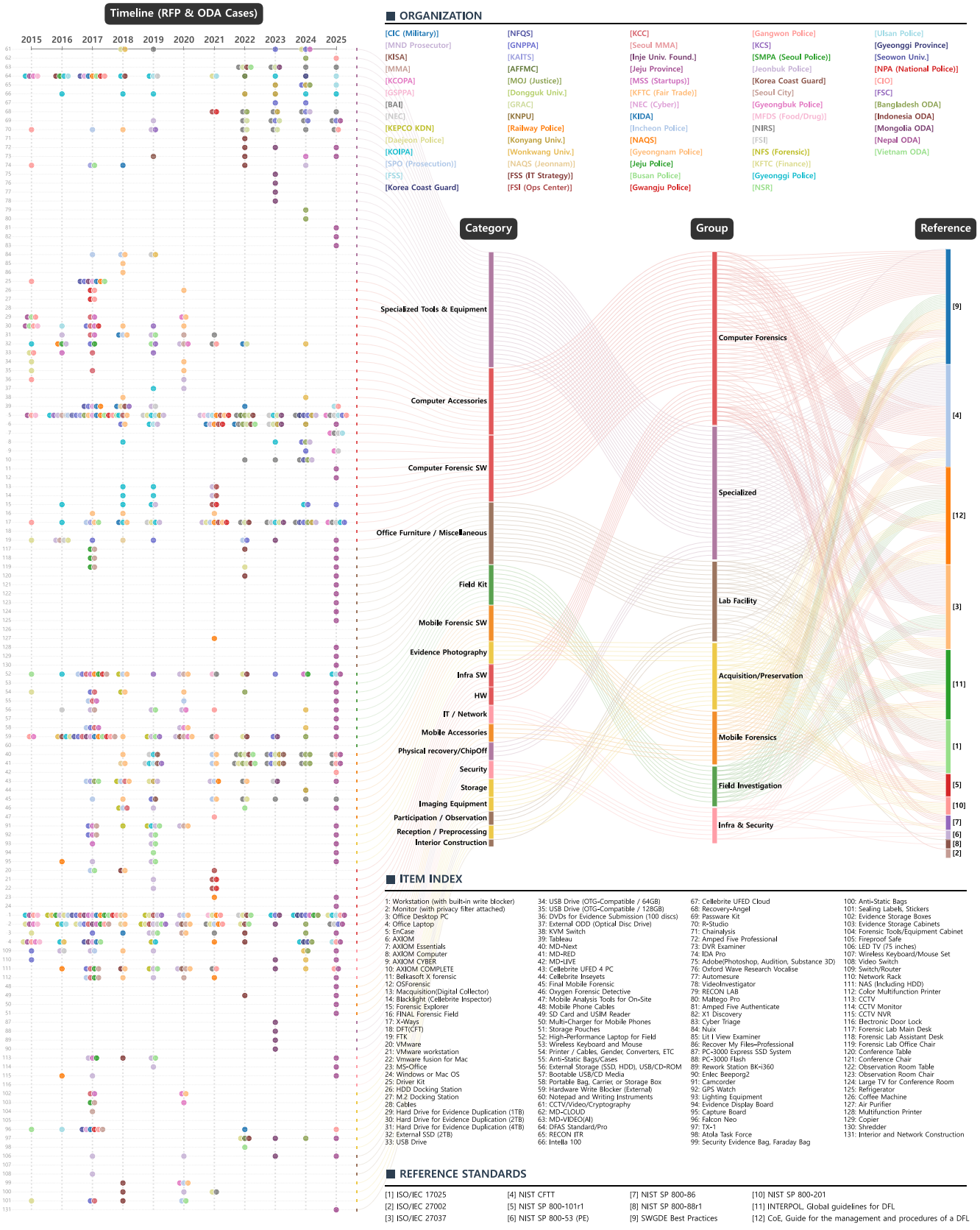


Fig. 7. Visualization of the triangulation verification method mapping procurement data (2015–2025) and ODA cases to derived equipment categories and international standards.

admissibility guarantees the reliability, integrity and accuracy of the evidence. To secure this, a secure lab space and proven, reliable tools and equipment are necessary. Therefore, when establishing the DFL, those responsible for establishing and enforcing the budget must consider allocating appropriate resources to meet both technical reliability and legal requirements, while being fully aware of these requirements. In this study, the standard list of tools and equipment is calculated to be larger in terms of cost than the amount actually built because it covers items available in the public and private sectors. Therefore, organizations should select and implement items from the derived list based on their specific scale, mission, and role. Additionally, pricing policies for commercial digital forensics products within the Korean market may differ somewhat from prices available for overseas purchases. For instance, it should be recognized that domestic pricing is set somewhat higher than overseas prices due to varying domestic margin rates influenced by exchange rates. Price fluctuations relative to the amounts at the time of the study must also be considered. Furthermore, for equipment such as office furniture/other items, given the vast variety and the inability to select a specific product unlike digital forensics tools, the average price range for the existing product category was calculated. Therefore, when considering the purchase of tools or equipment, it is advisable to check the latest prices and maintenance contract terms through the official supplier or authorized reseller for each item.

5.1.2. Strategies for tool selection

The evaluation criteria for purchasing and implementing digital forensic tools were analyzed in the preceding survey. The findings confirmed that the most important criteria are, in order of priority, reliability, integrity and accuracy. EnCase, which is used in court, can therefore be considered a reliable option. Integrity and accuracy are fundamental to digital forensic tools, ensuring that copies of evidence are identical to the original by using hash values. Analysis of the types of digital forensic tools, conducted through interviews with professionals and a survey, confirmed that computers and mobile tools represent a significant proportion. The scope of digital forensic tools is expanding beyond computer and mobile forensics to include drones, automobiles, the cloud and artificial intelligence (AI). AXIOM Cyber, for example, offers AI-based analysis functions alongside computer, mobile, and automobile data processing. Oxygen, on the other hand, specialises in mobile forensics but also supports computer and cloud forensics. EnCase, traditionally a computer forensics tool, now offers mobile analysis and cloud analysis modules. UFED provides drone-based digital forensics solutions. Therefore, in light of the potential for further functional expansion, computer and mobile forensic tools should be incorporated as standard, as confirmed by the survey results. Therefore, specialized forensic tools for specific equipment like drones or IoT were excluded from the list due to relatively low market demand and technical limitations. Furthermore, while existing digital forensic tools offer some AI-based forensic capabilities as modules, standalone AI-based forensic tools were excluded from the standard list, considering insufficient market demand and technological development. Nevertheless, there is a clear demand for tools incorporating new technologies based on each organization's characteristics and requirements. For example, E-Discovery requires digital forensics products for big data processing, such as automated data analysis and classification. DFIR (Digital Forensics and Incident Response) products for cyber intrusion response focus on log analysis and malware detection. Specialized tools for cloud data seizure are also required. Reflecting all these diverse requirements would cause the scale and number of scenarios to consider during implementation to increase exponentially. However, as this study focuses on identifying the fundamental tools/equipment for the initial establishment of a DFL, the introduction of future-oriented tools is limited to suggesting possibilities. The specific implementation phase is left open to be considered based on future technological advancements and market demand.

5.1.3. Environmental considerations for digital forensic tools

While the criteria for selecting or evaluating digital forensics tools presented in prior research are important, there were some discrepancies when analyzing interview results with personnel actually working in the field and case studies of lab construction and delivery. For EnCase, its use is prevalent in domestic public organizations due to certifications, court testimony, symbolic value, and expertise. However, this is heavily influenced by digital forensics personnel and budget constraints. For instance, DFLs with only one or two personnel often find it difficult to replace the software initially introduced due to budget constraints, leading some to operate solely on annual maintenance renewals. Furthermore, tool selection varies depending on organizational characteristics. When seizing and searching servers related to illegal sites, database forensic software is necessary to investigate WAS or DB within the server. Organizations conducting extensive CCTV investigations require video restoration software. Public organizations, often using proprietary internal messengers, sometimes need customized extraction and analysis tools. Meanwhile, high-cost tools like Nuix are utilized by being lent from the Supreme Prosecutors' Office to local prosecutors' offices. Additionally, the Supreme Prosecutors' Office provides evidence management and analysis services through the National Digital Forensics as a Service (NDFaaS) cloud platform. NDFaaS supports automatic analysis when data such as call logs, account statements, mobile phone information, emails, and multimedia are uploaded to its cloud-based web interface. Tool selection also varies based on user proficiency. AXIOM is popular among beginners due to its straightforward procedures and user-friendly interface for evidence processing and analysis. However, experienced users with a high level of understanding of digital evidence prefer using X-Ways. Whether the tool is subject to strategic goods regulations also influences selection. UFED, for instance, has sales restrictions for certain countries due to manufacturer policies or international export control norms. Thus, factors like organizational size and characteristics, budget constraints, skill level and preferences, and manufacturer policies must be considered when selecting tools.

5.1.4. International application strategies

This study presents implementation strategies within an international context based on the results of the ODA project for establishing a DFL. First, the procurement, ordering, and delivery processes for tools and equipment must systematically consider various price fluctuation factors. Exchange rate fluctuations, in particular, directly impact the types and quantities of tools and equipment that can be secured within the total project budget. The differing customs duties and value-added tax systems across countries also become critical variables when calculating procurement budgets. Additionally, logistics costs and delivery lead times associated with different supply methods are important considerations. For instance, air freight may be preferable to sea freight when rapid delivery is required, but sea freight is relatively more efficient for transporting large volumes. Therefore, it is advisable to determine the transportation method by comprehensively analyzing the procurement purpose, delivery deadline, and volume scale. Expenses such as accommodation, labor costs, airfare, and other miscellaneous costs incurred by the winning contractor for delivery and installation must also be considered. Furthermore, some digital forensics tools are classified as strategic goods in certain countries, leading to cases where vendors restrict exports or deliveries. If delivery of a specific tool is restricted, it is necessary to preemptively review the feasibility of securing functionally and technically equivalent or similar alternative equipment. Changes in vendor policies also directly impact equipment costs and budget planning. For example, Maltego previously offered a Classic model but now primarily sells the Professional version. AXIOM used to be available for purchase separately as Computer and Mobile, which are now combined into Advanced. Some products have also switched from Perpetual to Subscription licensing. These changes in vendor policies have a significant impact on the cost structure of tools and equipment

and must be considered in the budgeting process. Taken together, this study emphasizes the need for a design strategy that goes beyond the simple selection of tools and equipment when building a DFL in an international context. Such a strategy must incorporate complex factors such as currency, taxation, logistics, export controls, and vendor policy changes. In summary, when applying the proposed baseline, it is necessary to clearly distinguish between region-dependent and region-stable elements. Elements likely to vary by region include pricing (exchange-rate volatility, local distributor margins, and maintenance pricing), procurement rules (tendering procedures, customs duties, and value-added taxes), and tool availability (export controls and vendor sales policies). By contrast, the functional categories of tools and equipment, the scale-based composition logic for one- and five-person laboratories, and the alignment with ISO/IEC 17025 requirements are expected to remain largely stable across regions (International Organization for Standardization, 2017; INTERPOL, 2019).

5.1.5. Validation strategy and reliability assurance for digital forensic tools under ISO/IEC 17025

The results of digital forensic examinations can vary depending on the tools used. Using different forensic tools, such as EnCase or X-Ways, on the same storage media image can lead to discrepancies in analysis outcomes due to differences in file reading units, data parsing methods, and deleted file recovery or carving techniques. Even identical files may produce results that are partially missing or that differ from one another. This variability is a primary source of errors, making it necessary to understand and compare the functionalities of each tool. Relying on a single tool leaves one vulnerable to external challenges due to these characteristics. To address this issue and ensure reliability, a “cross-validation“ strategy is necessary. This strategy involves applying multiple standardized tools to the same sample. In this process, reference datasets and tool-testing programs, such as NIST CFReDS and the CFTT (Computer Forensic Tool Testing) program, can be used to objectively verify the functions of each tool (National Institute of Standards and Technology, 2026b,a; National Institute of Standards and Technology, Computer Forensics Tool Testing Program, 2024; Hughes and Karabiyik, 2020). To meet the mandatory validation procedures of ISO/IEC 17025 and align with forensic practices, the management approach should separate “test methods” from “test tools” (Marshall and Paige, 2018; Beckett and Slay, 2007). While forensic methods remain relatively stable, software tools are frequently updated. Therefore, a revalidation process using the same control samples should be conducted every time a tool is updated to ensure consistency with previous versions. This revalidation process is not limited to documentation. It includes actually conducting tests. If the results change after a tool update, the cause must be analyzed and recorded. These tasks require considerable time and continuous personnel involvement, and the more frequent the tool updates, the greater the validation burden becomes. In summary, the validation requirements of ISO/IEC 17025 in the field of digital forensics can only be met through repetitive and systematic revalidation procedures within the organization due to the tool-dependent nature of results and the potential variability of results caused by tool updates. To this end, comparison results between tools should be secured in advance. Revalidation should be performed with the same samples upon tool updates. Separating methods and tools in management is also necessary to maintain the reliability of examination results. Table 14 presents this validation strategy as an actionable checklist. It specifies when revalidation is required, which control samples should be used, which artifacts must be retained (logs, hashes, and version records), and the corresponding acceptance criteria, in line with ISO/IEC 17025 and current SWGDE, ASTM, and ILAC guidance (International Organization for Standardization, 2017; SWGDE, 2024; ASTM International, 2018; International Laboratory Accreditation Cooperation, 2022). As Horsman notes, this is because the practical question of whether an examiner “can use that tool” ultimately depends on such documented, repeatable validation evidence (Horsman, 2024a).

5.2. Future directions for digital forensic tools, equipment, and l aboratories

5.2.1. Evolution of automated processing

The current digital evidence processing procedure consists of identification, collection, processing, analysis, and reporting. However, each stage is physically or logically separated, leading to inefficiencies in terms of time, manpower, and cost. Future digital forensics procedures are highly likely to evolve into cloud-based automated processing models tailored to specific cases. For example, data secured during the evidence collection stage could be automatically pre-processed according to specific formats and rules. It would then be linked to a cloud environment or a pre-established DFL infrastructure for real-time or near-real-time analysis. Therefore, there is a need to move beyond the concept of separately preserving and transferring evidence data secured at the scene according to the chain of custody. Instead, improvements should enable rapid preprocessing using online resources, with results verifiable on-site. Of course, for cases where confidentiality and security are particularly emphasized depending on the incident type, automated processing may be required within a dedicated cloud environment secured via a VPN or separate information protection measures, or within a semi-closed DFL environment. In other words, the future advancement of digital forensic tools/equipment must be developed along two parallel axes: enhancing automation and real-time capabilities, while simultaneously applying differentiated levels of security and control based on the risk level of the case.

5.2.2. LLM-based data processing for evidence

LLM-based digital forensic techniques enable the identification of evidence in a way that goes beyond the knowledge and experience of the examiner (Dunsin et al., 2024). The development of tools and equipment capable of executing small-scale LLM models is necessary for this data processing method, as is training for evidence data processing. In line with this technological evolution, the construction of future DFLs will enhance infrastructure and transform analytical approaches. For example, evidence secured in the DFL is linked, and the AI model learns from it immediately. Based on the learned results, the location, type, and relevance of digital evidence to the case could be verified through AI, with analysts conducting secondary and tertiary verification. This represents a potential shift in workflow processes. It signifies a transformation in digital evidence processing brought about by AI technology. To achieve this, the development of AI-based digital forensics tools/equipment capable of eliminating current AI model issues such as hallucinations and bias is necessary.

5.2.3. AI-based digital evidence processing

Current AI operates by processing user input and returning results based on trained models. However, future AI will evolve to autonomously learn, update its models, and self-improve by collecting feedback. Digital forensics tools/equipment will also advance with this AI trend, enabling them to independently learn from evidence input by analysts. By cross-referencing and inferring from data in existing cases, they will prioritize and present evidence most relevant to the analyst’s needs. Beyond this, based on learned data, they will advance to provide investigative insights—assessing the appropriateness of criminal allegations, identifying what additional evidence must be secured to substantiate them, and determining which devices require seizure and search.

5.3. Contributions

As a result of this study, in addition to securing digital forensic tools and equipment, additional budgets were reviewed considering other secondary factors. Interior elements such as interior construction, for example, are factors that many organizations can miss. However, considering promotional factors such as the degree of media exposure of digital forensics and the spread of performance, the opinion of incumbent workers is that aesthetic factors should also be included when

Table 14
Tool validation checklist for ISO/IEC 17025 compliance in digital forensics laboratories.

Validation Activity/Trigger	Control Samples	Artifacts to Retain	Acceptance Criteria
Initial validation — before first operational use of a tool or a tool function	Reference datasets (e.g., NIST CFReDS, CFTT test images) and known-content in-house samples	Validation plan and report (tester, date); tool name, version, and configuration; hash values of reference data and outputs; execution logs	Results match the expected reference results for every tested function; any deviation is documented and risk-assessed
Revalidation — tool update, patch, OS change, or configuration change that can affect results	The *same* control samples used in the initial validation (fixed reference set)	Version-change record; before/after comparison results; execution logs; updated validation report	Results are consistent with the previously validated version; any difference is analyzed, documented, and approved before redeployment
Periodic verification — recurring routine check at a risk-based interval defined in the QMS (e.g., annually), between full validations	A small, fixed selection from the initial-validation reference set that exercises the critical functions (imaging, hashing, deleted-data recovery); a full revalidation is not required	Verification records; equipment maintenance logs; hash verification records	Each critical function reproduces the same reference results as in the last validation (within documented tolerances); any deviation triggers revalidation
Deviation handling — unexpected result, cross-tool discrepancy, or casework anomaly	Replication on the same samples with a second validated tool (cross-validation)	Nonconformity record; root-cause analysis; corrective-action (CAPA) documentation	Cause is identified and recorded; affected casework is assessed; corrective action is verified before the tool returns to service

Sources: (International Organization for Standardization, 2017; SWGDE, 2024; ASTM International, 2018; International Laboratory Accreditation Cooperation, 2022; National Institute of Standards and Technology, 2026a,b). ISO/IEC 17025 clauses chiefly applied: 6.4 (equipment), 7.2 (methods and validation), 7.10 (nonconforming work).

building functions, and this study actively reflected these. Consideration has also been given to space compartments. It was intended to derive tools and equipment by dividing them into space sections according to the digital forensics process, such as on-site dispatch, reception/preprocessing, storage, participation/observation, and analysis, without simply stopping at the premise that a certain area of space was given. We also considered office environment elements that support digital forensics functions. This study is meaningful in that it presents practical criteria for implementing digital forensics functions by deriving the maximum elements that can be constructed under the assumption that manpower and space are assumed. In addition, based on the case of Korea, the voices of former and current personnel in charge of digital forensics were heard and reflected. Through focus group interviews, we were able to get opinions on what tools are used from the actual user's point of view and what other tools are needed. We visited investigative agencies and appraisal agencies with digital forensics as their main business and supplemented the deficiencies through on-site inspections and interviews. Furthermore, it was intended to minimize the gap by presenting the list derived from this study and the calculated budget to the officials who participated in the establishment of the actual digital evidence analysis room. In addition, we reviewed the current status of the lab's tools and equipment built through the digital forensics ODA project. In particular, a detailed list of tools and equipment obtained in the course of the project was collected, and the budget status executed for each piece of equipment was compared and analyzed. Through this process, we were able to bridge the gap with data from 2021. Finally, the accuracy and reliability of the research results were verified by utilizing the comparison and analysis results of the equipment and budget.

6. Limitations and conclusion

This study used a mixed methodology to derive a comprehensive list of digital forensic tools and equipment. This methodology included surveys, on-site visits, and reviews of requests for proposals (RFPs) and official development assistance (ODA) delivery records. However, this research has several limitations. First, the survey samples mainly focused on South Korea, so recall or social desirability bias may have influenced the responses. Second, the policies and budgetary conditions of respondents' organizations may have affected their answers, creating a potential discrepancy between self-reported preferences and the tools actually in use. Third, the survey and interview results reflect perceptions from 2021 and may not capture subsequent technological and legal developments or tool updates. To address these limitations, the study reviewed the delivery details of the "Digital Forensics Lab Building" ODA project conducted in five countries from 2022 to 2025. Nevertheless, these findings are specific to the context of the ODA target countries. Thus, limitations remain in generalizing tool preferences and budget structures to specific regions or countries. In particular, prices, procurement rules, and tool availability are region-dependent, whereas the functional categories and the scale-based composition logic of the proposed baseline are considered likely to remain stable across jurisdictions. In addition, the unit prices and market estimates were validated by two domestic industry experts. Although these figures are anchored in actual procurement records, they may reflect domestic market conditions and a limited range of expert judgment. In future research, it is essential to empirically verify whether key criteria for introducing tools, such as reliability, integrity, and accuracy, identified in this study, lead to actual purchases. This will require repeated tests to measure the tools, make mutual comparisons, and analyze error types using actual event data. Furthermore, a thorough analysis is necessary to understand the impact of subscription-based billing models for major tools, such as FTK and AXIOM, on budgeting and selection preferences, as well as the discrepancies between preferred and actual tools used regarding evidence processing capacity. Finally, discussions are needed regarding the composition of tools optimized for the missions and roles of various organizations. The required equipment list varies depending on each agency's investigative characteristics and personnel management methods, such as rotational assignments versus specialized personnel, including those of local police departments, security investigations, and special judicial police. In the future, statistical data derived from digital evidence analysis reports should be used to track changes in preferences over time, compare past and present data, and facilitate research responding to technological paradigm shifts, such as cloud computing and AI forensics.

CRediT authorship contribution statement

Sumin Shin: Writing – original draft, Visualization, Project administration, Methodology, Formal analysis, Data curation, Conceptualization. **Byounghun Moon:** Validation, Software, Resources, Formal analysis, Data curation. **Jihye Jang:** Visualization, Investigation, Formal analysis, Data curation. **Gibum Kim:** Writing – review & editing, Resources, Project administration, Methodology, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported by the Supreme Prosecutors' Office under S-2021-1601-000 ("Study of Digital Forensic Laboratory Construction Standard Model").

Data availability

The authors do not have permission to share data.

References

Almuqren, A., Alsuwaelim, H., Rahman, M.M.H., Ibrahim, A.A., 2024. A systematic literature review on digital forensic investigation on Android devices. Procedia Comput. Sci. 235, 1332–1352. https://doi.org/10.1016/j.procs.2024.04.126

Sunardi, Herman, Ardiningtias, S.R., 2022. A comparative analysis of digital forensic investigation tools on facebook messenger applications. J. Cyber Secur. Mobil. 11, 655–672. https://doi.org/10.13052/jcsm2245-1439.1151

ASTM International, 2018. ASTM E3016-18: Standard Guide for Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis. Technical Report, ASTM International, West Conshohocken, PA, https://doi.org/10.1520/E3016-18

Ayers, R., Brothers, S., Jansen, W., 2014. Guidelines on Mobile Device Forensics. Technical Report SP 800-101 Revision 1, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.SP.800-101r1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf.

Beckett, J., Slay, J., 2007. Digital forensics: validation and verification in a dynamic work environment. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07). IEEE, https://doi.org/10.1109/HICSS.2007.175. p. 266a.

Bhat, W.A., AlZahrani, A., Wani, M.A., 2021. Can computer forensic tools be trusted in digital investigations? Sci. Justice 61, 198–203. https://doi.org/10.1016/j.scijus.2020.10.002

Buchanan-Wollaston, J., Storer, T., Glisson, W., 2013. Comparison of the data recovery function of forensic tools. In: Peterson, G., Shenoi, S. (Eds.), Advances in Digital Forensics IX. Springer, Berlin, Heidelberg, pp. 331–347. https://doi.org/10.1007/978-3-642-41148-9_22. volume 410 of IFIP Advances in Information and Communication Technology.

Carrier, B., 2002. Open Source Digital Forensics Tools: The Legal Argument. research report. Revised version (2003) available at the URL, @stake, Inc. https://www.digital-evidence.org/papers/opensrc_legal.pdf.

Council of Europe, 2017. Digital Forensics: A Basic Guide for the Management and Procedures of a Digital Forensics Laboratory. Technical Report. GLACY DFL Guide, Version 1.1, June 2017, Council of Europe, Strasbourg. https://rm.coe.int/glacy-dfl-guide-version-aug-2017-v8/16809ebf68.

Dubettier, A., Gernot, T., Giguet, E., Rosenberger, C., 2023. File type identification tools for digital investigations. Forensic Sci. Int. Digit. Investig. 46, 301574. https://doi.org/10.1016/j.fsidi.2023.301574

Dubey, H., Bhatt, S., Negi, L., 2023. Digital forensics techniques and trends: a review. Int. Arab J. Inf. Technol. 20, 644–654. https://doi.org/10.34028/iajit/20/4/11

Dunsin, D., Ghanem, M.C., Ouazzane, K., Vassilev, V., 2024. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Sci. Int. Digit. Investig. 48, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

ENFSI, 2015. Best Practice Manual for the Forensic Examination of Digital Technology. Technical Report ENFSI-BPM-FIT-01. Version 01, November 2015, European Network of Forensic Science Institutes. https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf.

Friedl, S., Englbrecht, L., Böhm, F., Pernul, G., 2023. Support tool selection in digital forensics training. In: Ubiquitous Security: Second International Conference, UbiSec 2022, Zhangjiajie, China, December 28–31, 2022, Revised Selected Papers. Springer Nature Singapore, pp. 3–21, https://doi.org/10.1007/978-981-99-0272-9_1

Ghazinour, K., Vakharia, D.M., Kannaji, K.C., Satyakumar, R., 2017. A study on digital forensic tools. In: 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). IEEE, pp. 3136–3142, https://doi.org/10.1109/ICPCSI.2017.8392304

Glisson, W.B., Storer, T., Buchanan-Wollaston, J., 2013. An empirical comparison of data recovered from mobile forensic toolkits. Digit. Investig. 10, 44–55. https://doi.org/10.1016/j.diin.2013.03.004

Grance, T., Hash, J., Stevens, M., O'neal, K., Bartol, N., 2003. Guide to Information Technology Security Services. Technical Report NIST SP 800-35, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.SP.800-35. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-35.pdf.

Guo, Y., Slay, J., Beckett, J., 2009. Validation and verification of computer forensic software tools—searching function. Digit. Investig. 6, S12–S22. https://doi.org/10.1016/j.diin.2009.06.015. Proceedings of the Ninth Annual DFRWS Conference.

Gupta, K., Neyaz, A., Shashidhar, N., Varol, C., 2022. Digital forensics lab design: a framework. In: 2022 10th International Symposium on Digital Forensics and Security (ISDFS). IEEE, pp. 1–6, https://doi.org/10.1109/ISDFS55398.2022.9800799

Hargreaves, C., Breitinger, F., Dowthwaite, L., Webb, H., Scanlon, M., 2024a. DFPulse: the 2024 digital forensic practitioner survey. Forensic Sci. Int. Digit. Investig. 51, 301844. https://doi.org/10.1016/j.fsidi.2024.301844

Hargreaves, C., Nelson, A.J., Casey, E., 2024b. An abstract model for digital forensic analysis tools – a foundation for systematic error mitigation analysis. Forensic Sci. Int. Digit. Investig. 48, 301679. https://doi.org/10.1016/j.fsidi.2023.301679

Hassan, N.A., 2019. Computer forensics lab requirements. In: Digital Forensics Basics: A Practical Guide Using Windows OS. Apress, pp. 69–91. https://doi.org/10.1007/978-1-4842-3838-7_3

Hibshi, H., Vidas, T., Cranor, L., 2011. Usability of forensics tools: a user study. In: 2011 Sixth International Conference on IT Security Incident Management and IT Forensics (IMF). IEEE, pp. 81–91, https://doi.org/10.1109/IMF.2011.19

Hildebrandt, M., Kiltz, S., Dittmann, J., 2011. A common scheme for evaluation of forensic software. In: 2011 Sixth International Conference on IT Security Incident Management and IT Forensics (IMF). IEEE, pp. 92–106, https://doi.org/10.1109/IMF.2011.11

Horsman, G., 2019. Tool testing and reliability issues in the field of digital forensics. Digit. Investig. 28, 163–175. https://doi.org/10.1016/j.diin.2019.01.009

Horsman, G., 2024a. Commentary:- can I use that tool? Forensic Sci. Int. Digit. Investig. 51, 301843. https://doi.org/10.1016/j.fsidi.2024.301843

Horsman, G., 2024b. Sources of error in digital forensics. Forensic Sci. Int. Digit. Investig. 48, 301693. https://doi.org/10.1016/j.fsidi.2024.301693

Hughes, N., Karabiyik, U., 2020. Towards reliable digital forensics investigations through measurement science. WIREs Forensic Sci. 2, e1367. https://doi.org/10.1002/wfs2.1367

Hughes, N., Ziemak, E., Martinez, C., Stout, P., 2022. Toward a cost–benefit analysis of quality programs in digital forensic laboratories in the United States. WIREs Forensic Sci. 4, e1422. https://doi.org/10.1002/wfs2.1422

International Laboratory Accreditation Cooperation, 2022. ILAC-G19:06/2022: Modules in a Forensic Science Process. Technical Report. ILAC, Silverwater, Australia. https://ilac.org/?ddownload=124605, Available via https://ilac.org/publications-and-resources/ilac-guidance-series/.

International Organization for Standardization, 2017. ISO/IEC 17025:2017 — General Requirements for the Competence of Testing and Calibration Laboratories. Technical Report, ISO, Geneva. https://www.iso.org/standard/66912.html.

International Organization for Standardization, International Electrotechnical Commission, 2012. ISO/IEC 27037:2012 — Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Technical Report ISO/IEC 27037:2012. October 2012, ISO/IEC, Geneva, Switzerland. https://www.iso.org/standard/44381.html. First.

INTERPOL, 2019. Global Guidelines for Digital Forensics Laboratories. Technical Report, INTERPOL Global Complex for Innovation, Singapore. https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensics.

Ismail, I., Ariffin, K.A.Z., 2025. The admissibility of digital evidence from open-source forensic tools: development of a framework for legal acceptance. PLoS One 20, e0331683. https://doi.org/10.1371/journal.pone.0331683

Jang, Y.S., 2017. A Study on the Standard Design of Digital Evidence Analysis Laboratories. Technical Report. In Korean, National Police Agency, Seoul, Republic of Korea. https://policy.nl.go.kr/search/searchDetail.do?rec_key=UH1_00000129092658.

Karabiyik, U., Karabiyik, T., 2020. A game theoretic approach for digital forensic tool selection. Mathematics 8, 774. https://doi.org/10.3390/math8050774

Lawrence, T., Karabiyik, U., Shashidhar, N., 2018. Equipping a digital forensic lab on a budget. In: 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, pp. 1–7, https://doi.org/10.1109/ISDFS.2018.8355345

Lyle, J.R., Guttman, B., Butler, J.M., Sauerwein, K., Reed, C., Lloyd, C.E., 2022. Digital Investigation Techniques: A NIST Scientific Foundation Review. Technical Report NIST IR 8354, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8354

Mahmood, H., Arshad, M., Ahmed, I., Fatima, S., Ur Rehman, H., 2024. Comparative study of IoT forensic frameworks. Forensic Sci. Int. Digit. Investig. 49, 301748. https://doi.org/10.1016/j.fsidi.2024.301748

Malik, A.W., Bhatti, D.S., Park, T.J., Ishtiaq, H.U., Ryou, J.C., Kim, K.I., 2024. Cloud digital forensics: beyond tools, techniques, and challenges. Sensors 24, 433. https://doi.org/10.3390/s24020433

Manson, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M., Treichelt, J., 2007. Is the open way a better way? Digital forensics using open source tools. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07). IEEE, https://doi.org/10.1109/HICSS.2007.301. p. 266b.

Marshall, A.M., Paige, R., 2018. Requirements in digital forensics method definition: observations from a UK study. Digit. Investig. 27, 23–29. https://doi.org/10.1016/j.diin.2018.09.004

Morgan, D.L., 1997. Focus Groups as Qualitative Research, volume 16 of Qualitative Research Methods Series, second ed. SAGE Publications, Thousand Oaks, CA, https://doi.org/10.4135/9781412984287

Morgan, D.L., 1998. The Focus Group Guidebook, volume 1 of The Focus Group Kit, SAGE Publications, Thousand Oaks, CA, https://doi.org/10.4135/9781483328164

National Institute of Standards and Technology, 2026a. Computer forensic reference data sets (CFReDS) portal. https://cfreds.nist.gov/ (Accessed: 14 August 2026).

National Institute of Standards and Technology, 2026b. Computer forensics tool testing program (CFTT). https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt (Accessed: 14 August 2026).

National Institute of Standards and Technology, 2026c. NIST computer forensics tools & techniques catalog. https://toolcatalog.nist.gov/ (Accessed: 14 August 2026).

National Institute of Standards and Technology, Computer Forensics Tool Testing Program, 2024. Test Results for Mobile Device Acquisition Tool: Cellebrite UFED 4PC V7.69.0.1397 / Physical Analyzer V7.68.0.25. Technical Report, U.S. Department of Homeland Security, Science and Technology Directorate, Washington, DC. https://www.dhs.gov/sites/default/files/2025-04/25_0424_st_test_results_for_mobile_device_acquisition_tool-cellebrite_ufed4pc_v7.69.0.1397-pa_v7.68.0.25.pdf.

Nodeland, B., Belshaw, S., 2020. Establishing a criminal justice cyber lab to develop and enhance professional and educational opportunities. Secur. Priv. 3, e123. https://doi.org/10.1002/spy2.123

Nordvik, R., Stoykova, R., Franke, K., Axelsson, S., Toolan, F., 2021. Reliability validation for file system interpretation. Forensic Sci. Int. Digit. Investig. 37, 301174. https://doi.org/10.1016/j.fsidi.2021.301174

O'connor, R.V., 2005. Software selection: towards an understanding of forensic software tool selection in industrial practice. Int. J. Technol. Policy Manag. 5, 311–329. https://doi.org/10.1504/IJTPM.2005.008633

Padmanabhan, R., Lobo, K., Ghelani, M., Sujan, D., Shirole, M., 2016. Comparative analysis of commercial and open source mobile device forensic tools. In: 2016 Ninth International Conference on Contemporary Computing (IC3). IEEE, pp. 1–6, https://doi.org/10.1109/IC3.2016.7880238

Patel, B., Mann, P.S., 2025. A survey on mobile digital forensic: taxonomy, tools, and challenges. Secur. Priv. 8, e470. https://doi.org/10.1002/spy2.470

Riadi, I., Yudhana, A., Fanani, G.P.I., 2023. Mobile forensic tools for digital crime investigation: comparison and evaluation. Int. J. Saf. Secur. Eng. 13, 11–19. https://doi.org/10.18280/ijsse.130102

Rzepka, L., Ottmann, J., Stoykova, R., Freiling, F., Baier, H., 2025. A scenario-based quality assessment of memory acquisition tools and its investigative implications. Forensic Sci. Int. Digit. Investig. 52, 301868. https://doi.org/10.1016/j.fsidi.2025.301868

Shin, S.M., Park, H.M., Kim, G.B., 2022. A study on the methods of building tools and equipment for digital forensics laboratory. Converg. Secur. J. 22, 21–35. https://doi.org/10.33778/kcsa.2022.22.5.021

Shin, S.M., Hong, J.W., Kim, G.B., 2023. Study on the standard components of digital forensics laboratory. J. Forensic Sci. 68, 839–855. https://doi.org/10.1111/1556-4029.15254

Sinaga, S.J., Asykar, M.A., Manurung, H., Wibowo, W.C., Yazid, S., Edwardo, T.O., 2026. Comparative evaluation of artifact extraction performance and usability in digital forensic tools: a study of cellebrite UFED, MSAB XRY, and magnet AXIOM. J. Forensic Sci. 71, 1652–1661. https://doi.org/10.1111/1556-4029.70320

Stoykova, R., Andersen, S., Franke, K., Axelsson, S., 2022. Reliability assessment of digital forensic investigations in the Norwegian police. Forensic Sci. Int. Digit. Investig. 40, 301351. https://doi.org/10.1016/j.fsidi.2022.301351

Supreme Prosecutors' Office, 2021. Research on the Standard Model for Building a Digital Forensic Laboratory. Technical Report. Technical report, in Korean; unpublished internal report of the funding agency, available from the corresponding author upon reasonable request, Supreme Prosecutors' Office, Seoul, Republic of Korea.

SWGDE, 2010. SWGDE Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence. Technical Report 10-Q-001. Version 1.0, May 15, 2010, Scientific Working Group on Digital Evidence. https://www.swgde.org/documents/published-complete-listing/10-q-001-swgde-minimum-requirements-for-quality-assurance-in-the-processing-of-digital-and-multimedia-evidence/.

SWGDE, 2017. SWGDE Framework of a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Providers. Technical Report 17-Q-001. Version 1.0, September 25, 2017, Scientific Working Group on Digital Evidence. https://www.swgde.org/documents/published-complete-listing/17-q-001-swgde-framework-of-a-quality-management-system-for-digital-and-multimedia-evidence-forensic-science-service-providers/.

SWGDE, 2024. Minimum Requirements for Testing Tools Used in Digital and Multimedia Forensics. Technical Report 18-Q-001-2.1. Version 2.1, March 7, 2024, Scientific Working Group on Digital Evidence. https://www.swgde.org/documents/published-complete-listing/18-q-001-minimum-requirements-for-testing-tools-used-in-digital-and-multimedia-forensics/.

Voigt, L.L., Freiling, F., Hargreaves, C., 2025. A metrics-based look at disk images: insights and applications. Forensic Sci. Int. Digit. Investig. 52, 301874. https://doi.org/10.1016/j.fsidi.2025.301874

Watson, D.L., Jones, A., 2024. A Blueprint for Implementing Best Practice Procedures in a Digital Forensic Laboratory: Meeting the Requirements of ISO Standards and Other Best Practices, second ed. Academic Press, https://doi.org/10.1016/C2018-0-03208-9

Wu, T., Breitinger, F., O'shaughnessy, S., 2020. Digital forensic tools: recent advances and enhancing the status quo. Forensic Sci. Int. Digit. Investig. 34, 300999. https://doi.org/10.1016/j.fsidi.2020.300999

Author biography

Sumin Shin received a Ph.D. from the Department of Forensic Science, at Sungkyunkwan University, in 2025. Since 2017, Shin has been in charge of cybersecurity and converged security in the Information Infrastructure and Security Team at the Korea Institute for Defense Analyses (KIDA). Shin's research interests include information security, AI forensics, digital forensic tools and equipment, digital forensic proficiency testing, international development cooperation, and ISO/IEC 17025, 17043, and 27001.

Byounghun Moon has been a Ph.D. candidate in Digital Forensics in the Department of Forensic Science, at Sungkyunkwan University, since March 2024, and has served as a faculty member in the Department of Cyber Investigation at the Korean Police Investigation Academy since February 2022. Moon's research interests include digital forensics, cybercrime, criminal investigation, environmental criminology, and social network analysis.

Jihye Jang is pursuing her master's degree in Digital Forensics in the Department of Forensic Science at Sungkyunkwan University, South Korea. She holds a B.Sc. in Software Convergence from Sookmyung Women's University. Her research interests include cybersecurity and digital forensics.

Gibum Kim received an M.S. in 2009 and a Ph.D. in 2017 from the Graduate School of Information Security, Korea University. From 2014 to 2020, Kim served as a faculty member in the Department of Police Science at the Korean National Police University, and has been an Associate Professor in the Department of Forensic Science, Sungkyunkwan University, since March 2020. Kim's research interests include digital forensics, information security, cybercrime investigation, and international development cooperation.