Received: 25 January 2023 | Revised: 13 March 2023 | Accepted: 25 March 2023

DOI: 10.1111/1556-4029.15254

JOURNAL OF FORENSIC SCIENCES AAFS

ORIGINAL PAPER

Digital & Multimedia Sciences

Study on the standard components of digital forensics laboratory

Su-Min Shin MA | **Jae-Won Hong BA** | **Gi-Bum Kim PhD**

Digital Forensics, Department of Forensic Science, University of Sungkyunkwan, 25-2, Seonggyungwan-ro, Jongno-gu, Seoul, Korea

Correspondence
Gi-Bum Kim, PhD, Digital Forensics, Department of Forensic Science, University of Sungkyunkwan, 25-2, Seonggyungwan-ro, Jongno-gu, Seoul, Korea.
Email: freekgb02@gmail.com

Funding information
The supreme prosecutor's office, Grant/Award Number: S-2021-1601-000

Abstract

Recently, digital forensics has become increasingly important as it is used by investigation agencies, corporate, and private sector. To supplement the limitations of evidence capacity and be recognized in court, it is essential to establish an environment that ensures the integrity of the entire process ranging from collecting and analyzing to submitting digital evidence to court. In this study, common elements were extracted by comparing and analyzing ISO/IEC 17025, 27001 standards and Interpol and Council of Europe (CoE) guidelines to derive the necessary components for building a digital forensic laboratory. Subsequently, based on 21 digital forensic experts in the field, Delphi survey and verifications were conducted in three rounds. As a result, 40 components from seven areas were derived. The research results are based on the establishment, operation, management, and authentication of a digital forensics laboratory suitable for the domestic environment, with added credibility through collection of the opinions of 21 experts in the field of digital forensics in Korea. This study can be referred to in establishing digital forensic laboratories in national, public, and private digital forensic organizations as well as for employing as competency measurement criteria in courts to evaluate the reliability of the analysis results.

KEYWORDS

Delphi method, digital forensic, digital forensic governance, digital forensic laboratory, evidence handling procedure, information security management, laboratory management

Highlights

- 40 components for digital forensic laboratory established via three Delphi surveys with 21 experts.
- Components cover professional responsibility, policies, structure, skills, case and laboratory management, analysis procedures.
- Study provides reliability through input from digital forensics experts.
- Components can be used as standards for building digital forensic labs in public and private sectors.
- The findings can be used for accreditation, evaluation, and to improve overall reliability of digital forensic analysis.

Presented at the 17th Asia Pacific International Conference on Information Science and Technology (APIC-IST 2022), June 19–21, 2022, in Gangneung, South Korea.

1 | INTRODUCTION

Digital forensics is used not only by investigation agencies such as the police, prosecutors, special judicial police officers, election commission, board of audit and inspection, and the fair-trade commission, but also by corporate accounting in fraud investigations, insider threats (e.g., data exfiltration of proprietary data) and external threat investigations (e.g., phishing and malware threats) resulting in increased legal disputes over the employed procedures and methods. Investigation agencies are expanding consignment analysis as a result of the increase in demand for digital forensics and the limitations of technological capabilities; therefore, it is also necessary to measure the reliability of digital forensics companies [1,2]. Digital forensics continues to develop as there is a growing demand for international litigation, with Korean companies filing lawsuits in US courts to utilize e-discovery and punitive damage systems [3]. In the past, most debates concerned the analysis results and procedures of investigators and analysts, but recently, outsider access control, management and disposal of evidence, chain of custody, and the process of deriving analysis opinions have gone beyond the expertise and reliability of tools. The fronts are expanding throughout digital forensic laboratories. Therefore, to supplement the limitations of evidence capacity and be recognized in court, it is essential to establish an environment that ensures the integrity of the entire process from collecting and analyzing to submitting digital evidence to court. This is an important task in securing the accuracy, reliability, and verifiability of the criminal justice system and can be resolved through digital forensic laboratory standardization.

Various movements are underway overseas to standardize digital forensic laboratories. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17025 is a standard for laboratory-related calibration and testing institutions, and thus far, organizations that build and operate many digital forensic laboratories within Korea and abroad are using it to guarantee the reliability of their work. Meanwhile, the council of Europol (CoE) established the digital forensics laboratory guide in 2017 to provide support and guidance for installation, operation, and evidence processing [4], and starting from 2019, they have begun advising the Interpol. Forensic experts from law enforcement, industry, and academia were gathered to publish and distribute guidelines based on information, knowledge, and best practices [5]. The accreditation system of the Korea laboratory accreditation scheme (KOLAS) based on ISO/IEC 17025 was used in Korea. In Korea, starting with the supreme prosecutors' office (KOLAS) in 2019, national police agency (KOLAS), Korea copyright protection agency (ANAB) in 2020, and H.M company (KOLAS) in 2022 have received ISO/IEC 17025 accreditation [6]. Considering the historical origin of ISO/IEC 17025, which will be described later, it is not a standard that is specific to digital forensics. Most domestic ISO/IEC 17025 digital forensic laboratories focus on digital evidence collection, imaging, and analysis, and since ISO deals with general content, there are some limitations in fully reflecting the specifics of digital forensics [7]. In addition, there are problems such as a lack of accreditation system infrastructure, ambiguity of accreditation scope, and lack of domestic digital forensic accredited testing institutes [8]. ISO/IEC 17025 does not specifically deal with the aspect of information protection such as the safe processing and storage of acquired digital data, other than the safe management of laboratories. Considering the characteristics of digital evidence described above, information protection can be highlighted as an important issue to counteract forgery, falsification, and damage to evidence when constructing, operating, and managing a digital forensic laboratory. In this regard, there is ISO/IEC 27001, an international standard for information security management that covers the requirements for establishing, implementing, maintaining, and continuously improving an information security management system based on the needs of the organization [9]. Because the digital forensic laboratory handles sensitive information for the requestor and information that may be impacted by leakage during the investigation, security management of data is important, and for this, information security management standards are required. In Korea, the ISO/IEC 27001-based information security management system has been improved to suit the domestic environment. The K-ISMS (ISMS-P) system, which adds personal information protection requirements, has been introduced and is in operation. As such, the need for digital forensic laboratories is increasing because of the diversification and mass production of digital evidence to accommodate an increase in the amount of digital information. However, ISO/IEC 17025 alone is not specialized in the field of digital forensics and thus, can neither guarantee information security of digital evidence nor fully reflect domestic conditions or domestic and foreign requirements. The need to derive a satisfactory digital forensic laboratory component is inevitable. Accordingly, this paper grafts the concept of ISO/IEC 27001 to information security management of digital evidence based on ISO/IEC 17025 and goes beyond the general ISO concept to compare, analyze, and review the guidelines for building a digital forensic laboratory. Next, standard components are derived for digital forensic laboratories that can be applied domestically and internationally, with enhanced security verified through Delphi survey.

The remainder of this study is organized as follows. In Section 2, reviews research on digital forensic laboratories and analyzes international standards and guidelines such as ISO, NIST, SWGDE, and OSAC. In Section 3, component items are derived as a result of comparing and analyzing international standards, guidelines, and KOLAS documents as part of a systematic research effort, including a third Delphi survey conducted with 21 digital forensic experts. In Section 4, concepts such as content validity, convergence, consensus, stability, and estimate validity that were applied to the analysis of the Delphi questionnaire results and further verified using Excel 2019 and SPSS (Statistical Package for the Social Sciences) 28.0.0.0, are discussed. Section 5 contains a discussion of the findings. Section 6 presents conclusions, limitations, and directions for future research.

2 | LITERATURE REVIEW

2.1 | Related research

In a digital forensics laboratory standard design study, Jang et al. (2017) discussed the concept of a digital forensic laboratory and design laws, standards, and reference model application standards for the design of metropolitan and provincial police agencies. Through empirical studies such as police data collection, focus group interviews, field visits, and surveys, a design suitable for domestic environment was presented [10]. Park et al. (2015) applied the value chain model, which is an organizational competency analysis model, referring to ISO/IEC 17025, ASCLD/LAB, ISO/IEC 27001, K-ISMS, and other digital forensic implementation guidelines. As a result, the digital forensic-level evaluation index was prepared, in advance, in five fields of organizational management (7), whereby 27 indicators related to digital forensic performance procedures (7), evidence acquisition and collection (4), evidence transport and storage (4), investigation and analysis (7), report preparation and utilization (5), and five procedures were developed in fields related to human resource management, technology, and facility operation. To verify the validity and suitability of the established indicators, an evaluation was conducted targeting two law enforcement agencies and law firms [11]. Nam et al. (2021) argued for the establishment of a registration system for private digital forensic companies, a consigned data history management system, and legal and institutional measures as short-term alternatives in a study on data protection methods entrusted to private digital forensic companies. In the long term, essential elements for policy compliance among ISO/IEC 17025 evaluation items and quality assurance elements of the Interpol guidelines were extracted and linked to the consigned data history management system to achieve the protection of personal information entrusted to private digital forensic companies. To suggest possible alternatives [12], Lee et al. (2020) mapped and analyzed the requirements of ISO/IEC/IEEE 29119 and ISO/IEC 25023, based on ISO/IEC 17025, to build a procedure and software test management system. For verification, a testing agency accreditation review evaluation was conducted and consequently, the requirements reflection and audit periods were shortened [13]. Casey et al. (2020), based on their experience with digital forensic laboratories, specified considerations for digital forensic labs in terms of risk management such as loss of evidence, alleged misconduct by employees, disclosure requirements, and information security breaches, emphasizing the concept of digital forensic preparedness to detect and prevent breaches [14]. Amann (2015) and others conducted a study to define and identify key elements of robustness and resilience in terms of sustainable digital forensic capabilities. As a research method, an online questionnaire consisting of 35 closed and open questions was studied in 72 law enforcement agencies for experts in the field. Robustness and recovery of digital investigation capabilities at strategic and operational levels, including digital forensic strategies, forensic principles, standardization, continuing education and training, research and development, collaboration, and human resources, have been identified and discussed based on an analysis of EU law enforcement survey results. Key for resilience and robustness are digital investigation competencies at strategic and operational levels, including digital forensic strategy, forensic principles, standardization, continuing education and training, research and development, collaboration, and human resources. Based on the analysis of EU law enforcement survey results, elements were identified and discussed. In this study, the opinions of field workers were collected with a focus on robustness and resilience in terms of maintaining the capabilities of the digital forensic organization with regard to policy and management. However, the survey population and number of respondents were low, and the analysis was carried out using only simple statistics [15]. Guo (2018) and others started developing a standard system to solve problems such as duplication of standard items, errors in selected standard items, and insufficient quality control through the evolution and comparison of digital forensic accreditation in China. The solutions for digital forensic accreditation were education and training, methodologies, equipment, and software. China has 4 national standards, 19 public safety industry standards, and 10 forensic technical specifications in digital forensic-related standards. To further improve the process, standard unification and system establishment are in progress [16]. Tully et al. (2020) reviewed the results of approximately 61 evaluations of digital forensic device upgrades in the digital field (computer, phone, video, etc.) of the UK accreditation agency (UKAS) and were subsequently commissioned by a regulatory agency to analyze the quality problem. From 2015 to the end of August 2018, feedback from technical assessors was collected and analyzed in 61 UKAS evaluations. This was contrasted with the results of 29 surveillance assessment visits to the accredited DFUs by the UKAS between September 2018 and April 2019. That is, the collected data were analyzed for a certain period to verify that the follow-up measures for the raised issues were properly implemented. Following accreditation, considerations (specialization, tools, scope, experience, etc.) in terms of quality management were mentioned [17]. Hykš et al. (2014) introduced requirements for developing a digital forensic laboratory management system and prepared a quality management standard by comparatively analyzing ISO 9001, and ISO/IEC 17025, which is a general requirement standard for testing and calibration institutions. For continuous improvement in the future, it was proposed that methodologies such as EFQM (European Foundation for Quality Management) excellence model, six sigma, and lean management be applied [18]. However, previous research did not provide specific guidelines for the design of a digital forensic laboratory in Korea because of a lack of discussion on the components of the digital forensic laboratory.

2.2 | Guidelines and standards for digital forensics laboratory

2.2.1 | Interpol and global guidelines for digital forensics laboratory

Interpol's international guidelines for digital forensics laboratory organized a digital forensic expert group meeting to bring together

TABLE 1 Fields and scope of accreditation by KOLAS accredited organizations.

Main category	Middle category		
Forensic science testing	10.001 Regulatory materials	10.006 Firearms and bullets	10.011 Accidentology
	10.002 Poisons	10.007 Handwriting and document	10.012 On-site investigation
	10.003 Immuno-serology testing	10.008 Fingerprints	10.013 Forensic pathology
	10.004 DNA-type testing	10.009 Traces/signs	10.014 Entomology
	10.005 Trace evidence	10.010 Audio/computer analysis	10.015 Digital Forensic

digital forensic experts from law enforcement, industry, and academia to share information, knowledge, and best practices to reflect practical experiences as a guide [5]. the main components were digital forensic laboratory management, case management, evidence analysis procedures, and quality assurance.

2.2.2 | CoE: A basic guide for the management and procedures of a digital forensics laboratory

The CoE guidelines for digital forensics labs were published under a joint project between the CoE and the European Union on global action against cybercrime (GLACY). The guidelines aim to provide support and guidance to managers and practitioners in setting up, operating, and handling evidence in digital forensic laboratories [4]. Its main content is centered around management of evidence analysis and the processes and procedures of the digital forensics laboratory. The CoE guidelines are significant in that the administrative and technical aspects of digital forensic functions are reviewed. However, it is disappointing that there is a lack of classification in the content of the guidelines, and the improvement of the guidelines can be regarded as Interpol guidelines.

2.2.3 | ISO/IEC 17025:2017

ISO/IEC 17025:2017 is an international standard specification of the general requirements for competence, fairness, and consistent operation of laboratories or calibration laboratories by the ISO [19]. It is applied according to ISO/IEC 9001 and is largely composed of resource, organizational structure, process, and management system requirements. Because this standard is a general requirement, it can be applied to a digital forensic laboratory, and any particular scientific field or discipline. but it is not specialized in the digital forensic field. Therefore, it is necessary to examine domestic application cases for related requirements.

2.2.4 | SWGDE requirements and frameworks for digital forensic quality assurance

SWGDE has provided guidelines for Education/Training, Certification (Sub-Discipline Specific), Laboratory Standards, Examination Requirements as minimum requirements for a Quality Management System (QMS) [20]. The document uses the term digital evidence laboratory, and the laboratory standards presented in the study include Personnel, Facility Design, Evidence Control, Validation, Equipment Performance, Examination Procedures, Examination Review, Documentation and Reporting, Competency and Proficiency Testing, Audits, Deficiencies, Health and Safety, Customer Complaints, Document Control, and Disclosure of Information. In 2017, the SWGDE established a QMS framework for DME forensic service providers, with guidelines for employment qualifications, professional development and training, laboratory standards, and case workflow [21].

2.2.5 | KOLAS (Korea Laboratory Accreditation Scheme)

KOLAS evaluates and certifies testing, calibration, inspection, standard material production, medical testing, and proficiency testing for institutions operating according to the framework act on national standards and the international standards set by the ISO [22]. In digital forensics, accreditation is performed in the test field according to the requirements of ISO/IEC 17025.

It is noteworthy that KOLAS has recognized digital forensics as an area of the forensic science examination, as shown in Table 1 [22–24].

2.3 | Other standards and guidelines for digital forensics and more

2.3.1 | ISO/IEC standards for digital forensics

ISO/IEC 27037 is an international standard for identification, collection, acquisition, and preservation of digital evidence [25]. ISO/IEC 27037 addresses chain of custody, roles and responsibilities, competency, and more in the identification, collection, acquisition, and preservation of digital evidence. ISO/IEC 27041 addresses the conformity and assurance of methods applied to the investigation process described in ISO/IEC 27037 and ISO/IEC 27042. It consists of the steps of process design, implementation, validation, inspection, verification deployment, review, and maintenance [26]. ISO/IEC 27042 provides guidance on the analysis and interpretation of digital evidence [27]. It covers key attributes of an investigation (continuity, repeatability and reproducibility, uncertainty) and general principles of analysis, tool use and record

keeping, analytical models (static and dynamic analysis), interpretation, reporting, competence, and proficiency. ISO/IEC 27050 provides general requirements and guidance for electronically stored information (ESI) [28]. ISO/IEC 27050-1 covers an overview of e-discovery, related terminology, concepts, and processes. ISO/IEC 27050-2 provides guidance for e-discovery management and governance [29]. ISO/IEC 27050-3 describes the e-discovery process and specific requirements and guidelines for adherence to ISO/IEC 27050 [30]. ISO/IEC 27050-4 provides guidance on ICT readiness for conducting e-discovery [31].

2.3.2 | NIST IR 8354 digital investigation techniques

NIST IR 8354 provides a review of the scientific foundations of digital forensics [32]. The report is based on an evaluation of a collection of peer-reviewed literature, interlaboratory studies, proficiency testing, interviews, and workshops to gather input from community members. It mainly describes the relationship between computers and digital forensics, a review of information and data sources for digital forensics, considerations for each step of performing digital forensics, and technology/tool validation and testing. A review of digital forensic laboratory was also conducted. Digital forensic laboratory in the United States are identified in law enforcement, corporate offices, incident response, and other cybersecurity operations, and are utilized in civil litigation as a form of e-discovery. Major U.S. digital forensics laboratory identified through the capture–recapture methodology include IACP, IACIS, ANAB, SWGDE, and NW3C. It is important to note that the digital forensics community is decentralized and diverse, making it difficult to determine its true size.

2.3.3 | SWGDE's guidelines for quality management systems

The SWGDE guides Digital and Multimedia Evidence (DME) organizations to establish an organization's quality management system (QMS) in accordance with ISO/IEC 17025 and ISO/IEC 17020 [33]. ISO/IEC 17025 is a broadly applicable standard for testing laboratories, while ISO/IEC 17020 is a standard for inspection organizations and is used to establish impartiality and consistency in inspection activities. SWGDE notes that DME organizations can become accredited to ISO/IEC 17020 in addition to ISO/IEC 17025.

2.3.4 | OSAC, report of the digital evidence task group quality study

This document addresses digital forensic laboratory in terms of digital forensic quality management [34]. Data was collected and analyzed through interviews and surveys with 31 people, comprising 17 laboratory personnel and 14 legal customers. The survey covered eight topics: (1) documentation, (2) tool validation and testing, (3) management and peer reviews, (4) audits, (5) testimony monitoring, (6) personnel qualifications, (7) presence of a quality manager, and (8) accreditation. The results showed that a one-size-fits-all application of ISO/IEC 17025 accreditation is not well suited to the digital forensics field, as it focuses on demonstrating laboratory excellence, but not on improving laboratory quality. They identified that good staffing, technical review, and CoC management are important for the quality of a digital forensic laboratory (while testimony monitoring, testing/validation, internal audit, and accreditation are not). Furthermore, from the customer's perspective, they concluded that accuracy, understandability, and timeliness should be the goals for a successful quality management system.

2.3.5 | ISO/IEC 27001:2013

ISO/IEC 27001 is an international standard for information security management systems and provides requirements for the establishment, implementation, maintenance, and continuous improvement of information security management systems. In addition, by applying the risk management process, the confidentiality, integrity, and availability of information are maintained, assuring stakeholders that risks are properly managed [9]. The document describes seven areas: context of the organization, leadership, planning, support, operation, performance evaluation, and improvement. Annex A of this document describes 114 controls in 14 areas that are necessary to implement the information security risk treatment.

2.3.6 | K-ISMS (ISMS-P)

The K-ISMS was created based on ISO/IEC 27001 and has legal obligations for certification in the domestic information and communications network act and personal information protection act. Implemented in 2001, it was integrated with the personal information protection management system (PIMS) in 2018 and has been in operation as an ISMS-P certification system until now. In the case of ISMS, the certification criteria are divided into the establishment and operation of the management system (16 control items in four fields) and requirements for protection measures (64 control items in 12 fields). In the case of personal information, there are 22 control items in five areas for each processing stage and a total of 102 control items [35].

3 | METHODOLOGY

3.1 | Research process

3.1.1 | Research method

By comparing and analyzing domestic and foreign standards and guidelines, overlapping and non-overlapping items were collected to identify 47 components in eight areas. For the components identified, a Delphi survey was conducted targeting 21 experts with experience in building, operating, or auditing a domestic digital forensic laboratory

(Table 2). The experts had been active in this capacity for more than 10 years. The general characteristics of the panel are shown in Table 3. Demographically, there are 19 males (90.5%) and 2 females (9.5%), with a significantly higher proportion of males, 4 (19%) in their 30s, 12 (57.1%) in their 40s, and 5 (23.8%) in their 50s, with a predominantly 40-something age group, and 3 (14.3%) PhDs, 12 (57.1%) Masters, and 6 (28.6%) Bachelors. 16 (76.2%) had certifications and 5 (28.6%) did not. The industries represented were private (33.3%), public (57.1%), and military (9.5%), and the occupations were president (4.8%), director (14.3%), investigator (14.3%), examiner (33.3%), researcher (14.3%), professor (4.8%), team leader (9.5%), and law firm specialist (4.8%). Experience with digital forensic laboratory was considered to be present if any of the following were applicable: participating in or running a construction project, or preparing for and conducting a ISO/IEC 17025 accreditation audit. Of the 21 Delphi panelists, all but three (14.3%) of the 18 (85.7%) were found to have experience.

The first questionnaire was administered so that additional elements could be identified by presenting an explanation of the eight derived areas and open-ended questions. As a result of the first survey, the items that were added and corrected were reflected and compiled. After writing this as a closed-ended question, a second questionnaire was provided and the adequacy of each area and component was verified. In the 3rd survey, the statistical values of the expert panel's responses returned in the 2nd round and the status of each individual's responses were finally presented so that their opinions could be reconsidered. The Delphi survey results were analyzed using Excel 2019 and SPSS 28.0.0.0. Excel was used to analyze the mean, standard deviation, content validity ratio (CVR), stability, convergence, and agreement, and the reliability was analyzed using SPSS. Reliability measures the internal consistency of the Delphi questionnaire, to confirm whether the questionnaire was conducted consistently (Figures S1).

To enhance the credibility of the research, the subjects were selected from among domestic digital forensics-related workers with considerable practical and research experience as well as technical expertise. Regarding the number of Delphi expert panels, there are opinions that approximately 10 people are sufficient for a homogeneous group; others think 10–15 people are sufficient [36]; and still insist on using 5–20 experts [37].

3.1.2 | Delphi survey methodology and reasons for selection

The Delphi survey is a method for handling complex problems by structuring the communication process of an expert group and is characterized by anonymity, repeatability, controlled feedback, and statistical aggregation of respondents [38]. Anonymity implies not disclosing information between the survey subjects in questionnaires. Repeatability tests the questionnaire at multiple levels. Controlled feedback presents the opinions of the members in a non-face-to-face manner by providing statistical characteristics to respondents after synthesizing the questionnaire results. At the end of the survey, opinions are collected using the statistical average estimated by the Delphi panel in the final round [37]. In the case of digital forensic laboratories, the majority is small, and there are restrictions on securing related data because the laboratory is built and operated mainly by investigative agencies and are closed to information disclosure. In addition, there are some limitations to research conducted through empirical analysis because the components for building and operating a digital forensic laboratory are intertwined with not only technical but also administrative factors in a complex manner. Considering these points, the Delphi method, which can collect the opinions of experts in the field of digital forensics, can be an appropriate method to solve the problem proposed in this study and assess the ramifications.

3.2 | Component derivation

The method for deriving the components is as Figures S2. Based on the comparatively analyzed items, the items necessary for building a digital forensic laboratory were cross analyzed to identify common elements.

3.3 | Delphi survey

3.3.1 | Delphi survey (1st)

The first Delphi survey was conducted for approximately 2 weeks from September 7 to 17, 2021. Eight areas were presented, along with the expert panel's opinions on the appropriateness of the area and the elements to be included as subcomponents for each area. The first question of the Delphi questionnaire was designed as an open-ended question to derive items, as an addition to the 47 components in eight areas presented in the comparative analysis of previous standards and guidelines. If an overly structured and detailed survey was conducted, the range of responses of respondents may have been reduced, and the scope of problem-solving may have been limited. Therefore, the opinions of the panels were

TABLE 2 Delphi 1st, 2nd, and 3rd survey.

Degree	Period	Subcomponent			Res rate	Survey method	Survey contents
		Req	Res	Select			
1	2021.9.7 ~ 9.17	21	14	18	66%	E-mail	Open
2	2021.10.6 ~ 10.26	21	21	18	100%	E-mail	Closed
3	2021.10.27 ~ 11.10	21	19	18	90%	E-mail	Final verification

collected by presenting them in an open format to freely accept the opinions of the experts [39]. For the composition, only eight areas were presented, and the questions were prepared to accommodate the opinions of the expert panel as much as possible. The synthesized content was organized in the form of corrections, additions, deletions, divisions, and integration, considering redundancy and differentiation of the 47 components derived from standards and guidelines. The results of the first Delphi survey were organized into eight areas and 50 components.

3.3.2 | Delphi survey (2nd and 3rd)

The second Delphi survey was conducted for approximately 3 weeks from October 6 to 26, 2021. An appropriateness evaluation was performed for each area and component derived during the first round. For the second question, the results obtained by adjusting the responses collected in the first phase were summarized into 50 subcomponents in eight domains on a Likert 5-point scale (1: strongly disagree, 2: disagree, 3: neutral, 4: agree, 5: strongly agree), so that appropriateness evaluation for each area and component could be performed. The 3rd survey was conducted for approximately 2 weeks from October 27 to November 10, 2021, and was conducted in the form of reconsidering the panel's individual responses to the second result. The 3rd questionnaire was designed to reflect the interquartile range (Q1, Q3) and median (Md) of the 2nd questionnaire, and the statistical details of the respondents' responses to the 2nd questionnaire in reconsidering the final opinion.

4 | DERIVATION AND VERIFICATION OF FINAL COMPONENTS

4.1 | Delphi survey analysis indicators and analysis results

Indices required to analyze the Delphi questionnaire include the CVR, convergence, agreement, stability, and validity estimation. The CVR refers to items rated as agree (4 points) or strongly agree (5 points) by more than half of the respondents [40].

$$\mathrm{CVR} = \frac{n_e - \frac{N}{2}}{\frac{N}{2}} \tag{1}$$

(n_e: Number of panelists who answered strongly agree (5 points) and agree (4 points); N: Total Delphi panels.)

There was a difference in the validity of the CVR values depending on the number of panel responses. According to Lawshe [40], the validity figures according to the response panel are shown in the table below. For example, if the number of Delphi panels was 20, a CVR value of 0.42 or higher was considered as the validity of the response panel.

Convergence refers to the degree to which the opinions of the Delphi panel converged; the closer it was to 0, the more appropriate it was. The agreement had a value close to 1 when the first quartile coefficient (Q1) and third quartile coefficient (Q3) were agreed upon [41].

$$\text{Degree of convergence} = \frac{Q_3 - Q_2}{2},\ \text{Degree of agreement} = \frac{Q_3 - Q_2}{\mathrm{Md}} \tag{2}$$

Stability was calculated as the coefficient of variation obtained by dividing the standard deviation (SD) by the arithmetic mean ($\bar{X}$). If the value was <0.5, no additional questionnaires were required; if it was between 0.5 and 0.8, it was stable; and if it was more than 0.8, an additional questionnaire was required (Table 4) [42].

$$\text{Stability (coefficient of variation)} = \frac{\mathrm{SD}}{\bar{X}} \tag{3}$$

In this study, CVR of 0.49 or more, convergence of 0.5 or less, agreement of 0.75 or more, stability of 0.8 or less, and mean of 3.5 or more, were set as the Delphi questionnaire criteria for digital forensic laboratory component selection. As a result of the 2nd and 3rd Delphi survey, the mean value was 3.5 or higher and the stability was 0.8 or lower, confirming that the criteria set in this study were satisfied. Regarding the internal reliability of the components, all reliability (Cronbach's α) values were above 0.5, indicating acceptable results. Affiliation, organizational culture, and R&D were excluded from the components, as it was confirmed that the CVR value was <0.49 for both the secondary and tertiary stages. Organizational goals and vision, appointment and qualification, safety and health, and investigation did not meet the level of convergence, agreement, and CVR in the second round. However, during the 3rd Delphi survey, the results of the expert panel were reconsidered and reflected upon. The executive's interest, separation of duties, and contact with relevant organizations/expert groups were excluded from the components, as they did not meet the level of convergence, agreement, and CVR in both the 2nd and 3rd rounds. Digital evidence privacy protection was returned as inappropriate in both the secondary and tertiary domains; therefore, all elements, including the components, were excluded from the result (Table 5).

The opinions of the expert panel were additionally confirmed regarding convergence, agreement, and content validity values that did not meet the standards. In the case of organizational culture, it was suggested that this was inappropriate because there was room for bias in external viewpoints. It was also suggested that management concerns be excluded, as they are an aspect of support and not intervention or fine-grained control. Since the separation of duties is based on the operation of each institution, some experts gave opinions on maintaining the appropriate minimum conditions. Although it is necessary to communicate with the relevant institutions/expert groups, this is not appropriate in

TABLE 3 Delphi panel.

No	G	A	C	J	E	Q	DF.Lab EXP			No	G	A	C	J	E	Q	DF.Lab EXP		
							B/O	PFA	CA								B/O	PFA	CA
1	M	40	17	⑧	m	(1), (2)	○	–	–	12	M	40	15	⑪	m	(2), (7)	○	–	–
2	M	40	8	⑮	m	(2)	○	–	–	13	F	30	6	⑨	d	(2), (7), (9), (11)	○	○	–
3	M	40	9	⑧	m	(2)	–	○	–	14	F	40	15	⑭	m	–	○	○	–
4	M	40	10	⑤	m	–	○	○	○	15	M	30	3	⑥	b	–	○	–	–
5	M	50	25	⑬	b	–	○	–	–	16	M	50	23	①	m	(2), (7), (11)	○	–	–
6	M	40	19	⑫	b	(2), (3), (4)	○	○	–	17	M	40	18	②	d	(2), (7)	○	–	–
7	M	40	16	⑨	m	(1)	○	–	–	18	M	50	10	⑨	b	(2)	○	–	–
8	M	40	19	⑦	d	(5)	–	–	○	19	M	40	14	④	b	(2), (7), (10), (11)	–	–	–
9	M	40	7	⑩	m	(2), (6), (7), (8)	○	○	–	20	M	40	14	⑦	b	(4)	○	–	–
10	M	30	9	⑤	m	(2), (7)	○	–	–	21	M	50	22	⑦	m	(2), (6)	–	–	–
11	M	50	10	③	m	(2)	○	–	–										

Note: Gender: M (male), F (female). Age: 30 (30 ~ 39 years old), 40 (40 ~ 49 years old), 50 (50 ~ 59 years old). Career: year or experience. Job: ① digital forensic private company representative, ② national forensic service researcher, ③ prosecutor's office digital forensic investigator, ④ defense counterintelligence command digital forensic examiner, ⑤ national investigation headquarters researcher, ⑥ special judicial police digital forensic investigator, ⑦ digital forensic private company director, ⑧ digital forensic police investigator, ⑨ digital forensic police examiner, ⑩ public institution digital forensic team leader, ⑪ financial supervisory service special judicial police examiner, ⑫ digital forensic private company team leader, ⑬ professor, ⑭ ministry of defense digital forensic examiner, ⑮ digital forensics specialist at a Law Firm. Education: b (bachelor), m (masters), d (doctor). *Qualification*: (1) Professional investigator (Korea), (2) EnCE, (3) CISSP, (4) Information processing engineer (Korea), (5) ISO17025 auditor, (6) Digital forensics level 2 (Korea), (7) ACE, (8) MCFE, (9) Information security engineer (Korea), (10) Security+, (11) ETC. ○ indicates experience in building/operating a digital forensics lab or preparing for/conducting an accreditation process.

Abbreviations: A, age; B/O, digital forensics laboratory build and operation experience; C, career; CA, conduct accreditation experience; E, education; G, gender; J, Job; PFA, preparation for accreditation experience; Q, qualification.

TABLE 4 CVR minimum according to the number of Delphi panels.

Num. of panels	CVR min	Num. of panels	CVR min	Num. of panels	CVR min	Num. of panels	CVR min
5	0.99	9	0.78	13	0.54	25	0.37
6	0.99	10	0.62	14	0.51	30	0.33
7	0.99	11	0.59	15	0.49	35	0.31
8	0.75	12	0.56	20	0.42	40	0.29

terms of standardization evaluation. It was suggested that R&D be carried out by specialized research institutes having necessary competence within a system of cooperation. In the case of personal information protection, although its necessity was acknowledged, it was suggested that its effectiveness would be low as it would be a matter of personal information and its handler in the analysis process. There was an opinion that it is not appropriate to guarantee the right to participate after obtaining consent for the seized personal information, as personal information of an "individual" is identified through information rather than the information of the "confiscated person." Additionally, it was suggested that it would be beneficial to include the collection and disposal of personal information in case of evidence management, although this is difficult in practice due to the problem of calculating the scope of personal information.

4.2 | Derivation of final components and elements

For the digital forensic laboratory components, seven areas and 40 components were finally derived through three rounds of Delphi survey (Table 6).

5 | DISCUSSION

The ISO/IEC 27037, ISO/IEC 27039, ISO/IEC 27041, and ISO/IEC 27050 standards focus on the procedural and methodological aspects of digital forensics. Therefore, it is meaningful to study the components of a standard that includes procedures and methods and addresses the digital forensics laboratory from an organizational perspective, such as this study. NIST mentioned the existence and number of digital forensic laboratories in various fields, and SWGDE considered that digital forensic laboratory can also be applied to accredited testing laboratories or accredited inspection laboratories. These studies provided directions for future research on the prioritization of the identified components, applicability to smaller laboratories, and compatibility with testing and inspection laboratories, which were not addressed in this study. On the other hand, OSAC's study suggests that ISO/IEC 17025 is used to demonstrate excellence in digital forensic laboratory and is not suitable for practical quality improvement activities, which raises the need for a suitable component or accreditation standard for digital forensic laboratory, and this study can be seen as a challenging attempt to address this question. In the case of K-ISMS, the information security management system of ISO/IEC 27001 was customized to the Korean environment, and the area of personal information protection was additionally reflected. In this study, this study aims to verify whether the increasing area of personal information protection in the future can be affected in digital forensic laboratory. The area of privacy in digital forensic laboratories is still largely covered by digital forensics in investigations and examination agencies/organizations. In addition, since the private sector also carries out work through user requests, it is significant that issues such as access to personal information and storage of evidence that occur in the process of analyzing data were excluded from the study.

6 | CONCLUSION AND FUTURE WORK

In this study, a total of 40 components in seven areas were derived as components for the establishment and operation of a digital forensic laboratory through three Delphi surveys administered to 21 digital forensic experts (Professional responsibility and fairness, Principles, Policies and Procedures, Organizational structure, Human, skills and competencies, Digital forensic laboratory management, Digital forensic case management, Digital evidence analysis procedure). This study accomplished research achievements in that it derived the elements of establishment, operation, and management of a digital forensic laboratory. Reliability was added to the study by collecting the opinions of 21 experts in the field of digital forensics. The derived components can be used as standards for building digital forensic laboratories in national and public institutions (investigation agencies, investigation agencies, appraisal agencies, and standard agencies) and private digital forensic companies. Digital forensics were approached as an organizational function from a company-wide perspective, such as expert responsibility, policy, manpower, information security, case management, analysis procedures, and enhancement of reliability as well as image through accreditation. Therefore, administratively missing items can be minimized and utilized according to the organization's environment. Second, the findings of this study can be used as an accreditation standard for digital forensic laboratories. Since the result were derived based on ISO/IEC 17025, ISO/IEC 27001, CoE and Interpol guidelines, and K-ISMS (ISMS-P), preparation of testing and calibration in institutions and information security management can be carried out more easily. Additionally, it is possible to overcome the problem of the comprehensive standard presented in ISO/IEC 17025 by

TABLE 5 Delphi survey analysis results (2nd/3rd).

Digital forensics (DF) laboratory components and subcomponents	2 round								3 round							
	M	SD	C	A	CVR	S	R		M	SD	C	A	CVR	S	R	
I. Professional responsibility and fairness	4.22	0.73	0.50	0.75	0.67	0.17			4.31	0.62	0.50	0.75	0.78	0.14		
1) Affiliation; organizational culture	3.61	1.04	0.50	0.75	0.11	0.29	0.57	0.675	3.61	0.85	0.50	0.75	0.22	0.23	0.66	0.755
2) Organizational goals and vision	4.00	0.84	1.00	0.50	0.33	0.21	0.68		4.11	0.76	0.50	0.75	0.56	0.18	0.69	
3) Executive's interest	3.94	1.11	1.00	0.50	0.22	0.28	0.63		4.11	0.96	0.88	0.56	0.44	0.23	0.75	
4) Professional responsibility (code of ethics and conduct)	4.56	0.70	0.50	0.80	0.78	0.15	0.55		4.78	0.55	0.00	1.00	0.89	0.11	0.72	
5) Fairness Management	4.50	0.62	0.50	0.80	0.89	0.14	0.67		4.61	0.50	0.50	0.80	1.00	0.11	0.73	
II. Principles, policies, and procedures	4.67	0.49	0.50	0.80	1.00	0.10			4.67	0.49	0.50	0.80	1.00	0.10		
6) Declaration of evidence analysis principles	4.56	0.62	0.50	0.80	0.89	0.14	0.77	0.746	4.72	0.46	0.38	0.85	1.00	0.09	0.83	0.851
7) Establishment and publication of policies/guidelines	4.33	0.84	0.50	0.78	0.78	0.19	0.64		4.56	0.51	0.50	0.80	1.00	0.11	0.83	
8) Regular review and revision	4.50	0.62	0.50	0.80	0.89	0.14	0.75		4.50	0.51	0.50	0.78	1.00	0.11	0.84	
9) Risk management	4.33	0.77	0.50	0.78	0.67	0.18	0.64		4.50	0.62	0.50	0.80	0.89	0.13	0.76	
10) Establish an annual plan	4.44	0.86	0.50	0.80	0.78	0.19	0.68		4.44	0.86	0.50	0.80	0.78	0.19	0.84	
III. Organizational structure	4.00	0.84	0.38	0.81	0.56	0.21			4.11	0.83	0.50	0.75	0.67	0.20		
11) Defining the scope of duties and division of duties	4.22	0.81	0.50	0.75	0.56	0.19	0.76	0.828	4.28	0.75	0.50	0.75	0.67	0.17	0.73	0.82
12) Roles and responsibilities	4.44	0.86	0.50	0.80	0.78	0.19	0.77		4.61	0.70	0.38	0.85	0.78	0.15	0.78	
13) Separation of duties	3.83	0.92	0.88	0.56	0.22	0.24	0.76		3.89	0.90	0.88	0.56	0.33	0.22	0.72	
14) Appointment and qualification	3.94	0.87	0.75	0.63	0.44	0.22	0.82		4.11	0.68	0.38	0.81	0.67	0.16	0.76	
15) Securing employees and external personnel	4.22	0.73	0.50	0.75	0.67	0.17	0.85		4.33	0.69	0.50	0.75	0.78	0.15	0.89	
IV. Human, skills and competencies	4.61	0.70	0.38	0.85	0.78	0.15			4.94	0.24	0.00	1.00	1.00	0.05		

TABLE 5 (Continued)

Digital forensics (DF) laboratory components and subcomponents	2 round								3 round							
	M	SD	C	A	CVR	S	R		M	SD	C	A	CVR	S	R	
16) Human resource management	4.33	0.84	0.50	0.80	0.56	0.19	0.81	0.844	4.61	0.61	0.50	0.80	0.89	0.13	0.78	0.933
17) Job training	4.67	0.69	0.00	1.00	0.78	0.15	0.81		4.94	0.24	0.00	1.00	1.00	0.05	0.81	
18) Qualification management	4.33	0.84	0.50	0.80	0.56	0.19	0.86		4.56	0.70	0.50	0.80	0.78	0.15	0.81	
19) Proficiency assessment	4.28	0.96	0.50	0.80	0.56	0.22	0.79		4.56	0.70	0.50	0.80	0.78	0.15	0.77	
20) Contact with relevant organizations/ specialties and groups	3.83	0.92	0.88	0.56	0.22	0.24	0.83		4.00	0.84	1.00	0.50	0.33	0.20	0.81	
21) Digital forensic R&D	3.72	0.89	0.50	0.75	0.11	0.24	0.81		3.83	0.86	0.50	0.75	0.33	0.22	0.79	
V. DF laboratory management	4.61	0.50	0.50	0.80	1.00	0.11			4.61	0.50	0.50	0.80	1.00	0.11		
22) Physical environment configuration	4.28	0.67	0.50	0.75	0.78	0.16	0.89	0.907	4.39	0.61	0.50	0.75	0.89	0.13	0.92	0.933
23) Laboratory operation	4.33	0.84	0.50	0.78	0.78	0.19	0.90		4.39	0.70	0.50	0.78	0.78	0.15	0.93	
24) Asset management	4.17	0.71	0.50	0.75	0.67	0.17	0.90		4.17	0.71	0.50	0.75	0.67	0.16	0.92	
25) Evidence management	4.72	0.57	0.00	1.00	0.89	0.12	0.91		4.89	0.32	0.00	1.00	1.00	0.06	0.93	
26) Human security	4.50	0.62	0.50	0.80	0.89	0.14	0.90		4.61	0.50	0.50	0.80	1.00	0.11	0.93	
27) Physical security	4.50	0.62	0.50	0.80	0.89	0.14	0.90		4.56	0.62	0.50	0.80	0.89	0.13	0.92	
28) Information security	4.39	0.78	0.50	0.78	0.89	0.18	0.90		4.56	0.51	0.50	0.80	1.00	0.11	0.92	
29) Supplier relationship	3.89	0.90	0.00	1.00	0.56	0.23	0.89		3.89	0.83	0.00	1.00	0.67	0.21	0.93	
30) Deployment, development, and maintenance	4.33	0.77	0.50	0.78	0.67	0.18	0.90		4.39	0.70	0.50	0.78	0.78	0.15	0.93	
31) Compliance	4.33	0.77	0.50	0.78	0.67	0.18	0.91		4.44	0.62	0.50	0.78	0.89	0.13	0.94	
32) Quality assurance and accreditation	4.28	0.83	0.50	0.78	0.56	0.19	0.89		4.39	0.70	0.50	0.78	0.78	0.15	0.92	
33) Business continuity management	4.28	0.83	0.50	0.78	0.56	0.19	0.90		4.39	0.70	0.50	0.78	0.78	0.15	0.92	
34) Safety and health	4.11	0.90	1.00	0.50	0.33	0.22	0.91		4.28	0.83	0.50	0.78	0.56	0.19	0.94	
VI. DF case management	4.61	0.61	0.50	0.80	0.89	0.13			4.72	0.46	0.38	0.85	1.00	0.09		

(Continues)

TABLE 5 (Continued)

Digital forensics (DF) laboratory components and subcomponents	2 round								3 round							
	M	SD	C	A	CVR	S	R		M	SD	C	A	CVR	S	R	
25) Receiving a request	4.44	0.78	0.50	0.80	0.67	0.18	0.80	0.836	4.50	0.62	0.50	0.80	0.89	0.13	0.84	0.838
36) Registering a case	4.44	0.78	0.50	0.80	0.67	0.18	0.83		4.67	0.49	0.50	0.80	1.00	0.10	0.80	
37) Registering an exhibit	4.67	0.59	0.38	0.85	0.89	0.13	0.82		4.89	0.32	0.00	1.00	1.00	0.06	0.82	
38) Photographing an exhibit	4.39	0.78	0.50	0.80	0.67	0.18	0.80		4.50	0.62	0.50	0.80	0.89	0.13	0.83	
39) Conducting analysis	4.78	0.55	0.00	1.00	0.89	0.11	0.83		4.83	0.38	0.00	1.00	1.00	0.08	0.81	
40) Returning the exhibit	4.56	0.70	0.50	0.80	0.78	0.15	0.81		4.67	0.49	0.50	0.80	1.00	0.10	0.80	
41) Closing the case	4.56	0.70	0.50	0.80	0.78	0.15	0.81		4.67	0.49	0.50	0.80	1.00	0.10	0.81	
VII. DF analysis procedure	4.28	0.96	0.50	0.80	0.56	0.22			4.72	0.57	0.00	1.00	0.89	0.12		
42) Acquisition	4.28	0.75	0.50	0.75	0.67	0.18	0.83	0.891	4.56	0.51	0.50	0.80	1.00	0.11	0.79	0.849
43) Investigation	4.00	0.97	1.00	0.50	0.33	0.24	0.87		4.33	0.84	0.50	0.78	0.78	0.19	0.69	
44) Analysis	4.17	0.92	0.50	0.75	0.56	0.22	0.84		4.61	0.78	0.38	0.85	0.89	0.16	0.80	
45) Presentation	4.33	0.84	0.50	0.80	0.56	0.19	0.65		4.67	0.59	0.38	0.85	0.89	0.12	0.90	
VII. Digital evidence privacy	4.22	1.06	1.00	0.60	0.33	0.25			4.11	1.02	1.00	0.56	0.33	0.24		
46) Protective measures when collecting digital evidence with personal information	4.06	1.21	0.88	0.61	0.44	0.30	0.97	0.977	4.39	1.04	0.50	0.80	0.78	0.23	0.97	0.970
47) Protective measures for possession and use of digital evidence with personal information	4.06	1.06	0.88	0.56	0.44	0.26	0.98		4.33	0.84	0.50	0.78	0.78	0.19	0.96	
48) Protection measures when providing digital evidence with personal information	4.00	1.24	1.00	0.56	0.33	0.31	0.97		4.17	1.15	0.88	0.65	0.44	0.27	0.97	
49) Protective measures when personal information of digital evidence is destroyed	4.22	1.11	0.88	0.65	0.44	0.26	0.98		4.39	0.92	0.50	0.80	0.67	0.20	0.96	
50) Protection of rights of data subjects for digital evidence	4.17	1.10	0.88	0.65	0.44	0.26	0.98		4.44	0.86	0.50	0.80	0.78	0.19	0.96	

Note: The grayed out areas are those that did not meet the criteria.

Abbreviations: A, agreement; C, convergence; M, mean; R, reliability; S, stability; SD, standard deviation.

TABLE 6 Results of the components of the digital forensics laboratory.

Area	Component	Description
I. Professional responsibility and fairness	1) Organizational goals and vision	• Digital forensic laboratory activities must be aligned with the organization's goals and vision, and maintain direction
	2) Professional responsibility (code of ethics and conduct)	• Sharing professional responsibilities through ethics charters and guidelines
	3) Fairness management	• Maintaining and guaranteeing fairness during evidence analysis work and maintaining confidentiality of identified contents between tasks
II. Principles, policies, and procedures	4) Declaration of evidence analysis principles	• Establishing principles for operation and management of digital forensics labs
	5) Establishment and publication of policies/guidelines	• Define detailed policies and guidelines in consideration of relevance to the organization's policies
	6) Regular review and revision	• Policies should be reviewed and revised periodically, and documented and maintained
	7) Risk management	• Act on risks identified through periodic risk assessment
	8) Establish an annual plan	• The establishment of the digital forensics laboratory, manpower, operation, budget, etc. are reflected through the annual implementation plan, and the top management of the organization approves and supports it to ensure that it is carried out
III. Organizational structure	9) Defining the scope of duties and division of duties	• Define job scope and segregate duties for a digital forensics laboratory
	10) Roles and responsibilities	• Assign roles and responsibilities to each person according to work
	11) Appointment and qualification	• Notarize that you have the expertise, skills required for digital forensics activities, and certain experience through qualification
	12) Securing employees and external personnel	• Secure adequately qualified staff for evidence analysis and publicize in the form of organization rules and division of duties
IV. Human, skills, and competencies	13) Human resource management	• Securing and managing manpower capable of performing digital forensic tasks
	14) Job training	• Efforts to continuously maintain professionalism through education and training
	15) Qualification management	• Maintaining activities such as program development and operation, seminar attendance, and technology exchange to maintain and manage digital forensics laboratory expert qualifications
	16) Proficiency assessment	• Periodic verification of competence of personnel expertise through employee proficiency evaluation
V. Digital forensics laboratory management	17) Physical environment configuration	• Design a secure physical space for performing digital evidence analysis work and divide the work area accordingly so that integrity is not compromised
	18) Laboratory operation	• Manage change history of digital forensic laboratory assets; secure space for evidence storage; define system performance and capacity requirements for evidence data management; manage failure preparedness and backup in digital forensics laboratory; and manage records of analyst work history; perform regular inspection, tool/equipment maintenance; establish and implement disposal procedures
	19) Asset management	• Identify and catalog assets related to digital forensics laboratory operations • Manage by establishing asset management policies and conducting risk assessments to assign grades according to importance
	20) Evidence management	• Establish labeling standards so that evidence can be systematically managed and searched, and a detailed description of evidence is recorded and maintained so that there is no omission when moving evidence
	21) Human security	• Check whether there are any security problems through background check of digital forensic laboratory personnel and reputation inquiry in previous workplaces • Before hiring, write a security pledge to comply with the prohibition of divulging confidential information learned in the course of work and conduct periodic security awareness training while working • In case of violation, disciplinary action is taken, and in case of job change or retirement, a confidentiality agreement is written, and related accounts and privileges are deleted

(Continues)

TABLE 6 (Continued)

Area	Component	Description
	22) Physical security	• The digital forensic laboratory is defined as a protected area to control access by unrelated personnel outside of work and access control • Install CCTV to keep records of the number of people entering and exiting; physically separate the space in consideration of the movement route; and grant access rights differentially
	23) Information security	• Establish management responsibilities and procedures to prevent accidents such as leakage, alteration, and damage of digital evidence in the digital forensic laboratory, and establish a communication system that can promptly report any situation • Control access to evidence analysis systems other than authorized persons and ensure confidentiality through data encryption when accessing evidence management or criminal justice information systems • To secure the stability of evidence processing, configure an internal or independent network environment and record evidence data processing step-by-step logs
	24) Supplier relationship	• Define relationships with suppliers of tools, equipment, and services within the digital forensics lab • Maintain documented security requirements to reduce supplier risk and define supplier service requirements level
	25) Deployment, development and maintenance	• Check whether the related requirements are met when introducing or developing digital forensic tools/equipment • Review the budget considering the annual maintenance cost when introducing tools/equipment • Establish development policies/guidelines during development, manage changes and history, and perform security management for the development environment • When developing outsourced development, check and supervise whether it is implemented to meet the contract conditions, and verify conformity through acceptance tests
	26) Compliance	• Identify and manage factors that meet laws, regulations, and requirements related to digital forensic laboratories, digital forensic organizations, and evidence acquisition, processing, analysis, and records management • Products installed and operated in the digital forensic laboratory must use genuine products • Review relationship with laws such as the Personal Information Protection Act, the Information and Communications Network Act, the Electronic Financial Transactions Act, and the Communication Secret Protection Act
	27) Quality assurance and accreditation	• Perform annual internal audit to maintain the work quality of the digital forensics laboratory • Regularly inspect the physical environment and conduct management and maintenance of digital forensic tools/equipment • Maintain the reliability of digital forensic technology through standard operating procedures (SoP) • Continuously maintaining and improving the quality of digital forensics laboratory activities through KOLAS or ISO 17025 accreditation
	28) Business continuity management	• Establish a digital forensic laboratory business continuity plan and procedure to analyze failure types, damage scale, and impact by scenario; establish strategies and countermeasures for normal business recovery • Evaluate the adequacy of the plan through periodic training; correct and supplement shortcomings
	29) Safety and health	• Identification of factors that could be hazardous to safety or potentially damaging to humans in and out of digital forensics labs • Periodic safety risk assessment should be conducted to prevent exposure of personnel to hazardous substances. Personnel should be familiar with and comply with safety and health-related legal requirements
VI. Digital forensics case management	30) Receiving a request	• Review received requests considering whether they are within the scope of digital forensics, available methods and tools, considering who can perform them, and whether legal requirements have been met, and the results are formally returned
	31) Registering a case	• Generate a unique case number upon filing and fill out the registration form • Confirm normal case registration by filling in specific details of the request and have it signed by the requester and digital forensics laboratory staff member
	32) Registering an exhibit	• Seal the evidence upon receiving, register and designate a unique evidence label • All defects in the evidence are recorded on the evidence registration form • The evidence reception staff fills out the form, and when not in use, stores it in the evidence storage room

TABLE 6 (Continued)

Area	Component	Description
	33) Photographing an exhibit	• Document the condition of the evidence and take pictures for effective identification in the future • The photographed photos are uploaded to the case folder and additional evidence is taken before being returned to the requestor
	34) Conducting analysis	• Carry out work according to the steps of obtaining, investigating, analyzing, and submitting evidence
	35) Returning the exhibit	• Upon completion of the analysis, the evidence is returned to the requester along with a digital forensic report • Seal by recording the name of the person who sealed the evidence, label of the evidence, and date and time of sealing before returning the evidence
	36) Closing the case	• Closing the case by signing the report to be delivered upon completion of the work
VII. Digital evidence analysis procedure	37) Acquire	• Create a copy of the electronic evidence (evidence) in the form of an image file or file • Create a copy of the same data, record both the evidence and the hash value of the image file, and store the copy in a storage medium other than the original evidence
	38) Investigation	• Use triage when large amounts or short-term data analyses are required • Perform cross-validation of evidence using various digital forensics tools • Use of features such as automated processing, data recovery, and filtering between investigations
	39) Analysis	• Analyze email, office documents, photographs and videos, Internet browsers, software, user activity, log files, encrypted files, unallocated space, cloud/remote storage, memory, chat log, SNS (Social Networking Service) account, calendar, memo, and access history by identifying and prioritizing artifact types, such as maps.
	40) Presentation	• Prepare and submit results reports in a way that stakeholders can understand • Record only verifiable facts and use visual aids to aid understanding • To be recognized as evidence in court, consider authenticity, completeness, credibility, persuasiveness, and proportionality; and review expert statements upon request by the court

using it as a standard to measure the capabilities of national and public institutions and private companies that operate domestic and foreign digital forensic laboratories. Because forensic laboratories are established based on ISO standard, with detailed evaluation indicators and quantification standards for each component, comparison, and analysis is possible by quantifying them. Finally, the established criteria can be used to evaluate the reliability of the analysis results of the digital forensic laboratory in court. If standards such as the analysis process and procedure according to the relevant components and management of evidence data in the digital forensic laboratory are complied with, the reliability of the evidence can be causally proven.

A digital forensic laboratory should be organically structured and operated as an element for the achievement of investigation and other organizational goals, breaking away from the concept of a space for simply analyzing the requested evidence. To this end, ISO/IEC 27001, which traditionally reflect the concept of Information security management, and ISO/IEC 17025, which is for the competence of testing and calibration laboratories, were applied along with international guidelines for digital forensic laboratories of the Interpol and CoE, and ISMS-P, an information security management system suitable for domestic environments. In other words, digital evidence data are processed in a state that meets the requirements of testing institutions and information protection. Thus, the processed data can be strictly protected through information security management. However, in this study, seven areas and 40 components were derived for standardization, making actual verification necessary for organizations that build, operate, and manage digital forensics laboratory in addition to expert verification. Therefore, it is necessary to conduct research on detailed evaluation indices of each component. Research on these detailed evaluation indicators is required to determine the suitability of the derived components for small digital forensic organizations, the effectiveness of compliance with these components compared to international standards and guidelines, etc. In addition, like the case of K-ISMS in Korea, which established an information protection management system certification system suitable for Korea based on ISO/IEC 27001, digital forensic laboratories also need future research on the establishment of a certification system suitable for each jurisdiction's environment in relation to ISO/IEC 17025.

FUNDING INFORMATION

This work was supported by the supreme prosecutor's office under S-2021-1601-000 ("Study of Digital Forensic Laboratory Construction Standard Model").

CONFLICT OF INTEREST STATEMENT

The authors have no conflicts of interest to declare.

ORCID

Su-Min Shin https://orcid.org/0000-0002-3184-7007

Gi-Bum Kim https://orcid.org/0000-0001-7298-4254

REFERENCES

1. Tak H-S, Lee W-S. A study on a model frame for the integration of digital forensic processes. Korean Institute of Criminology and Justice; 2016 [cited 2023 Mar 25]. Available from: https://kicj.re.kr/boardDownload.es?bid=0001&list_no=10330&seq=1
2. Kim H-K, Kim D-W, Lee K-L, Kim G-B, Kim M, Jo E, et al. Comprehensive policy for developing scientific criminal investigation and forensic science (III): review of relevant laws and policies on the effectiveness of criminal investigation. Korean Institute of Criminology and Justice; 2020 [cited 25 Mar 2023]. http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10548419
3. Han A. Civil and criminal e-discovery in the United States federal procedure and its ramifications to South Korea. Sungkyunkwan Law. 2020;32(2):179–224. https://doi.org/10.17008/skklr.2020.32.2.006
4. Nigel Jones VV, Bradley A, Stamenkovic B. A basic guide for the management and procedures of a digital forensic laboratory. Council of Europe; 2017 [cited 2023 Mar 25]. https://rm.coe.int/glacy-dfl-guide-version-aug-2017-v8/16809ebf68
5. Interpol. INTERPOL global guidelines for digital forensics laboratories. 2019 [cited 2023 Mar 25]. Available from: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf
6. KOLAS. Search for authorized organizations – search for testing organizations – 10 Forensic science – 015 Digital forensics. [cited 2023 Mar 25]. Available from: https://www.knab.go.kr/usr/inf/srh/InfoTestInsttSearchList.do?accreditClss=02&searchBigId=10&searchMiddleId=015&codeChangeValue=searchMiddleId&middleOrderBy=ID
7. Simon M, Slay J. Forensic computing training, certification and accreditation: an Australian overview. In: Futcher L, Dodge R, editors. Proceedings of the Fifth World Conference on Information Security Education (WISE 2007). 2007 June 19–21; West Point, NY. New York, NY: Springer; 2007. p. 105–12.
8. Kim H-Y. A study on the activation plan for accreditation of digital forensic laboratories in South Korea [Master's dissertation thesis]. Seoul, Korea: Sungkyunkwan University; 2021 [cited 2023 Mar 25]. http://www.riss.kr/link?id=T15770672
9. ISO. ISO/IEC 27001: 2013 information technology–security techniques–information security management systems–requirements. Geneva, Switzerland: International Organization for Standardization; 2022. [cited 2023 Mar 25]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
10. Jang Y-S, Kim J-H, Kim Y-K. Digital forensics laboratory standard design study. National Police Agency; 2017. [cited 2023 Mar 25]. Available from: https://policy.nl.go.kr/search/searchDetail.do?rec_key=UH1_00000129092658
11. Park H-I, Yoon J-S, Lee S-J. A study on development of digital forensic capability evaluation indices. J Korea Inst Inf Secur Cryptol. 2015;25(5):1153–66. https://doi.org/10.13089/JKIISC.2015.25.5.1153
12. Nam K-U, Lee S-J. A study on the protection of personal data committed to digital forensics private companies (a requirements for digital forensics labs). J Digit Forensics. 2021;15(1):12–25. https://doi.org/10.22798/KDFS.2021.15.1.12
13. Lee C-H, Kim Y-S, Noh A-R, Yang J-S, Kim M-S, Song S-H. A study on the application of ISO/IEC 17025 software accredited testing institute using ISO/IEC/IEEE 29119 and ISO/IEC 25023. J Korea Acad Ind Coop Soc. 2020;21(12):97–106. https://doi.org/10.5762/KAIS.2020.21.12.97
14. Casey E, Souvignet TR. Digital transformation risk management in forensic science laboratories. Forensic Sci Int. 2020;316:110486. https://doi.org/10.1016/j.forsciint.2020.110486
15. Amann P, James JI. Designing robustness and resilience in digital investigation laboratories. Digit Investig. 2015;12:S111–S120. https://doi.org/10.1016/j.diin.2015.01.015
16. Guo H, Hou J. Review of the accreditation of digital forensics in China. Forensic Sci Res. 2018;3(3):194–201. https://doi.org/10.1080/20961790.2018.1503526
17. Tully G, Cohen N, Compton D, Davies G, Isbell R, Watson T. Quality standards for digital forensics: learning from experience in England & Wales. Forensic Sci Int Digit Investig. 2020;32:200905. https://doi.org/10.1016/j.fsidi.2020.200905
18. Hykš O, Koliš K. Development of the digital forensic laboratory management system using ISO 9001 and ISO/IEC 17025. In: Doucek P, Chroust G, Oškrdal V, editors. Proceedings of the 22nd Interdisciplinary Information Management Talks (IDIMT 2104); 2014 Sept 10–12; Podebrady, Czech Republic. Linz, Austria: Trauner Verlag Universität; 2014. p. 87–94.
19. ISO. ISO/IEC 17025: 2017 General requirements for the competence of testing and calibration laboratories 2017. [cited 2023 Mar 25]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:17025:ed-3:v1:en
20. SWGDE. SWGDE minimum requirements for quality assurance in the processing of digital and multimedia evidence. 2010 [cited 2023 Mar 25]. Available from: https://drive.google.com/file/d/1K7v6rZXYYT_1Z8AcaEj2-Jt7OWGOhDc7/view?pli=1
21. SWGDE. SWGDE framework of a quality management system for digital and multimedia evidence forensic science service providers. 2017 [cited 2023 Mar 25]. Available from: https://drive.google.com/file/d/1yYg3gIHMi2PptZpBh2gDC9p6Woj3ASIs/view
22. Agency NTS. KOLAS accredited testing and inspection agency accreditation system operating guidelines. Revised notice, No. 2020–0103 [Announcement date 2020-06-04]. National Technical Standards Agency; 2020 [cited 2023 Mar 25]. Available from: https://www.kats.go.kr/content.do?cmsid=239&_dc=1467072000000&mode=view&page=3&cid=21541
23. Agency NTS. KOLAS accredited institution accreditation system operation guidelines [Enforcement 2021. 4. 8]", No. 2021–92 [2021. 4. 8., enacted]. 2021 [cited 2023 Mar 25]. Available from: https://www.kats.go.kr/content.do?cmsid=239&mode=view&page=41&cid=22260
24. Agency NTS. Announcement of revision of additional technical requirements for forensic science testing institute accreditation – No. 2020–0300 [Announcement date 2020-10-14]. National Technical Standards Agency; 2020 [cited 2023 Mar 25]. https://www.kats.go.kr/content.do?cmsid=239&_dc=1524689815145&mode=view&page=42&cid=21841
25. ISO. ISO/IEC 27037: 2012 Information technology — security techniques — guidelines for identification, collection, acquisition and preservation of digital evidence 2012. [cited 2023 Mar 25]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en
26. ISO. ISO/IEC 27041: 2015 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method 2015. [cited 2023 Mar 25]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27041:ed-1:v1:en
27. ISO. ISO/IEC 27042: 2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence 2015. [cited 2023 Mar 25]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en
28. ISO. ISO/IEC 27050–1: 2019 information technology — electronic discovery — Part 1: overview and concepts. 2019 [cited 2023 Mar 25]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27050:-1:ed-2:v1:en

29. ISO. ISO/IEC 27050–2: 2018 information technology — electronic discovery — Part 2: guidance for governance and management of electronic discovery. 2018 [cited 2023 Mar 25]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27050:-2:ed-1:v1:en
30. ISO. ISO/IEC 27050–3: 2020 information technology — electronic discovery — Part 3: code of practice for electronic discovery. 2020 [cited 2023 Mar 25]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27050:-3:ed-2:v1:en
31. ISO. ISO/IEC 27050–4: 2021-information technology — electronic discovery — Part 4: technical readiness. 2021 [cited 2023 Mar 25]. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27050:-4:ed-1:v1:en
32. Lyle JR, Guttman B, Butler J, Sauerwein K, Reed C, Lloyd C. Digital investigation techniques: a NIST scientific foundation review. NIST IR 8354. Gaithersburg, MD: National Institute of Standards and Technology; 2022. p. 1–53.
33. SWGDE. SWGDE establishing a quality management system for a digital and multimedia organization under ISO-IEC 17025 or 17020. 2021 [cited 2023 Mar 25]. Available from: https://drive.google.com/file/d/14LZ2-uuoQqYzKokrgNj_ntW5aeFjKd3z/view
34. Guttman B, Sauerwein K, Lyle JR. OSAC task group on quality practices in digital forensics laboratories. Report of the digital evidence task group quality study. Gaithersburg, MD: Organization of Scientific Area Committees for Forensic Science/NIST; 2022.
35. Korea Internet & Security Agency. ISMS-P certification system guide. 2022 [cited 2023 Mar 25]. Available from: https://isms.kisa.or.kr/board/file/bbs_0000000000000014/16/FILE_000000000000813/20220422162425837-610988933
36. Dalkey N. An experimental study of group opinion: the Delphi method. Futures. 1969;1(5):408–6. https://doi.org/10.1016/S0016-3287(69)80025-X
37. Rowe G, Wright G. Expert opinions in forecasting: the role of the Delphi technique. In: Armstrong JS, editor. Principles of forecasting: a handbook for researchers and practitioners. Boston, MA: Springer; 2001. p. 125–44.
38. Turoff M, Linstone HA. The Delphi method-techniques and applications. 2002 [cited 2023 Mar 25]. Available from: http://www.foresight.pl/assets/downloads/publications/Turoff_Linstone.pdf
39. Song Y-S. A study on design of organization for stability operation in North Korea [Doctoral dissertation thesis]. Seoul, Korea: Korea University; 2017 [cited 25 Mar 2023]. http://www.riss.kr/link?id=T14435151
40. Lawshe CH. A quantitative approach to content validity. Pers Psychol. 1975;28(4):563–75. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x
41. Lee J-H. Delphi method. Seoul, Korea: KYOYOOKBOOK; 2001. p. 33–136.
42. Noh S-Y. Delphi technique. Plan Policy. 2006;299:53–62.

SUPPORTING INFORMATION

Additional supporting information can be found online in the Supporting Information section at the end of this article.

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