Standardization of Tools and Equipment for Digital Forensics Laboratories

Abstract

Establishing a digital forensics laboratory to acquire and securely process digital evidence should be the top priority when building digital forensics capabilities within an organization. However, depending on the size and characteristics of the organization, there are many difficulties owing to the lack of standardized content, from budget securing to implementation. Therefore, this study aimed to provide a guide for planning and securing a budget by deriving a list of required tools/equipment and a budget for building a digital forensics laboratory for one to two and four to five personnel. As a research method, a focus group interview was conducted with 12 experts in the field of digital forensics, through which a list of tools and equipment was derived based on the interview findings. The content was further supplemented by visits to five digital forensic laboratories and interviews with practitioners. Accordingly, a tool/equipment questionnaire was created and administered to 124 forensic digital practitioners nationwide. The derived items provide a reference point for building a digital forensics laboratory and can be used for customization by adjusting the components to suit the size and budget of the organization.

Keywords: Digital Forensics, Digital Forensics Laboratory (DFL), Digital Forensic Tool/Equipment, Standardization, Focus Group Interview (FGI), Survey

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 [1]. DFLs serve as critical infrastructures for producing reliable results, enhancing the quality of acquired information, and demonstrating the credibility of digital evidence in court [2]. In terms of quality management, nontechnical factors, such as the management of DFLs, can also affect the outcomes of forensic analyses [3]. The establishment of a digital forensics laboratory(DFL) requires a management system that encompasses human resources, equipment, facilities, environmental conditions, reference materials, record keeping, methodologies, the verification

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

and evaluation of measurement uncertainty, process validation, functionality verification (based on tools or personnel), and competency testing of staff [4–7]. The standard most commonly applied to digital forensic laboratories is ISO/IEC 17025, which sets out the general requirements for the competence of testing and calibration laboratories. This standard specifies the environmental requirements for building DFLs, including the facilities, environmental conditions (Section 6.3), and equipment (Section 6.4) [7]. 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, digital forensic laboratories function as parts of larger organizations and are generally small in scale.

Accordingly, this study aimed to derive a list of necessary tools and equipment as well as budget estimates required to establish a DFL. The analysis was based on small-scale setups consisting of one to two and four to five personnel. Considering that budget allocations and operational roles vary across institutions, this study estimates the maximum requirements by scale while accounting for such constraints. Section 2 reviews previous studies on the identification and selection of tools and equipment for DFLs. Section 3 outlines the research methodology, including focus group interviews, analysis of requests for proposals, and surveys to derive the required tools, equipment, and budgets for laboratories consisting of one to five personnel. Chapter 4 refines and adjusts the derived items and budgets based on validation by domestic digital evidence analysis service providers. Finally, Section 5 presents the conclusions of this study and discusses directions for future research.

2. Related Work

Lawrence et al. (2018) conducted a study to evaluate the budgeting requirements of DFLs. They identified a list of the essential tools and equipment required to establish a small-scale laboratory for one to two personnel and proposed the associated initial acquisition and maintenance costs [8]. They categorized the required tools and equipment into computer and mobile forensics, and they considered both commercial and open-source products. The estimated initial setup costs ranged from $8,575 to $22,052, and the maintenance costs ranged from $2,478 to $6,419. O'Connor et al. (2005) explored criteria for selecting digital forensic tools. Through in-depth interviews with digital forensics experts, they identified the selection criteria and categorized them into technical, managerial, and legal domains [9]. Each criterion

was assigned an importance rating to indicate priorities in tool selection. Hibshi et al. (2011) conducted interviews and surveys with 115 participants to investigate usability considerations for digital forensic tools [10]. Their study addressed issues such as expertise and tool sophistication, GUI versus CLI preferences, reporting and documentation functions, user training requirements, user interface design, workflow support, and various usability and technical concerns. Nodeland et al. (2020) conducted a telephone survey with Texas law enforcement agencies to identify requirements for establishing a university-affiliated cyber research lab [11]. They reviewed the initial operational costs and provided general cost estimates for purchasing computers, hardware, and software along with a brief overview of the necessary equipment. While similar in nature to Lawrence's (2018) study, their research differs in that it distinguishes between hardware and software as well as and provides specific tool and equipment recommendations for startups. Román et al. (2016) analyzed 14 digital forensics software tools and evaluated them based on six criteria: price, supported disk images, supported file systems, file analysis capabilities, forensic analysis functions, and reporting/export features [12]. The NIST Computer Forensic Tool and Technique Catalog allows manufacturers to register technical specifications of tools and equipment from a functionality perspective, thuss enabling users to search for tools based on their capabilities [13]. Ghazinour et al. (2017) compared and analyzed tool lists and attributes in matrix form, arguing that the suitability of tools varies depending on the scenario [14]. Padmanabhan et al. (2016) compared open-source mobile digital forensic tools (e.g., Autopsy, SIFT) with commercial products (for example MOBILedit! Forensic, UFED) and suggested the potential of open-source tools as viable alternatives to commercial solutions [15]. Similar to the findings of Ghazinour et al. (2017), this study implicitly indicates the necessity of combining both open-source and commercial tools to meet diverse forensic requirements. In their study of standard design plans for DFLs, Yoonsik et al. (2017) proposed criteria to assess the need to establish, expand, relocate, or modify such laboratories. Their research derived a standard design framework using various methods including police data collection, focus group interviews, workshops, on-site inspections, and surveys. This study established environmental and facility-related standards for DFLs, classified the division and integration of facilities based on personnel size, and presented standard floor plans for each configuration [16]. Hassan (2019) identified the key components required for setting up a computer forensics lab, including physical facility requirements, environmental controls, hardware, software,

furnishings and consumables, workstations, evidence containers, software/hardware validation and verification, lab managers, lab data backups, training requirements, lab policies and procedures, documentation, and accreditation requirements [17]. Although the study provided a comprehensive overview of the elements needed to implement forensic lab functions, it primarily focused on lists and specifications without addressing budgetary considerations. In the Korean context, 16 digital forensic request for -proposal (RFP) documents published by the Public Procurement Service's "Nara Marketplace" between 2016 and August 2021 were analyzed to extract lists of tools and equipment. Duplicate or redundant items were removed, and missing elements were added or refined to enable a comparative analysis of tools and equipment suitable for labs staffed with one to two and four to five personnel. The estimated setup cost was approximately 145,777 USD for a one-person lab and 358,790 USD for a five-person lab, based on an exchange rate of 1 USD = 1,500 KRW.

3. Research Methodology and Procedure

3.1. Research Framework

This study begins by identifying the key factors necessary for selecting digital forensic tools and equipment based on a review of previous research. Group interviews were conducted to collect additional information. Subsequently, onsite inspections were conducted at five institutions in which DFLs had already been established. Following the site visits, a questionnaire was distributed to 200 current and former digital forensic professionals, and 124 valid responses were collected. Based on the findings of focus group interviews, site visits, and survey results, a draft standard list of tools and equipment as well as the corresponding budget estimates were developed. This draft was reviewed and refined through expert consultation with two industry professionals with direct experience in establishing DFLs (Figure 1).

3.2. Research Methods and Procedures

3.2.1 Focus Group Interview

A focus group interview is a qualitative research methodology in which a small group of participants engages in discussions on a specific topic to elicit a range of perspectives. The resulting data are often used to develop survey instruments and inform research design [18]. For this study, participant homogeneity was ensured by selecting individuals who were

actively engaged in the field of digital forensics at the time of the research and had experience in using tools or conducting forensic analysis. To minimize bias, participants were selected so that they had no prior personal connections with one another. Recruitment was based on a list compiled by the research team, and candidates who met the criteria were identified. Participation was confirmed via 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 the study [19]. The interviews were conducted over four sessions: the first on August 10, 2021, second on August 12, 2021, third on August 26, 2021, and fourth on August 27, 2021. Each session involved the same group of 12 experts (Table 1).

The interviews were conducted remotely via video conferencing (WebEx). Informational materials were shared in advance to ensure that participants were familiar with the content. The interview sessions followed a structured sequence: explanation of the purpose and background of the study, participant introductions, an overview of relevant prior research, guidance on the interview process, and the interview itself. Each session lasted for 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 concluded [20].

3.2.2 Derivation of the Tool/Equipment Pool

A comprehensive pool of tools and equipment required to establish a DFL was derived through focus group interviews. The items were categorized based on whether they should be possessed individually or at the team level and were further classified into computer and mobile forensic categories. Items that needed to be managed at the organizational level were identified separately. In addition, items that individual organizations might wish to acquire, but are often limited by budgetary and operational constraints, were included. These items typically require support from higher-level institutions. Shared items refer to the tools and equipment used by forensic analysts in laboratories. Although some smaller organizations reportedly assign field kits and imaging devices to individuals, the majority opinion during the interviews favored treating these items as shared resources, which was reflected accordingly. Other considerations include the storage of evidence, network equipment, safety and security-

related devices, office supplies, facilities, and miscellaneous items [21].

3.2.3. On-site Visits and Practitioner Interviews in DFLs

To understand the current state of tools and equipment in practice, on-site visits and practitioner interviews were conducted at five digital forensics organizations, each comprising approximately one to five personnel (< Table 2 >). 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, whereas the use of J-Tag and Chip-Off stations was infrequent and checked annually. With the support of file-level encryption in smartphones, J-Tag and Chip-Off have become less significant. Most agreed that using the J-Tag and Chip-Off in organizations with one to two personnel could be considered a waste of budget. The use of write blockers varied, depending on whether the organization used portable or built-in devices, with some using both types of devices, 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 24–32 in, with 2–4 units in use. Recently introduced workstations typically use Xeon Silver to Gold series processors, with higher-end models preferred. The memory was typically 128 GB, and hard drives ranged from 512 GB to 1 TB, with an additional 10 TB used separately. The costs of these systems range from $46,666.70 to $86,666.70. Some laboratories use USIM readers to verify phone model information during mobile analyses or maintain information in the form of evidence reports. Most laboratories conduct mobile analyses, making mobile multichargers a required possession. 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 for being static-free and low-wear. Tools with specialized features, such as Nuix, Chain Analysis, I2, and Sentinel, are not commonly used. Some institutions offer digital forensic tool/equipment rental services. Field response kits are equipped with tools and devices based on support requests and incident summaries or are pre-packaged and prepared according to various operational methods. Evidence photography has been conducted using camcorders or GPS watches, and some institutions have operated self-made evidence authentication systems or personal mobile phones for this purpose. Safety bags (shield packs) and anti-static bags were commonly used by most institutions, whereas Faraday bags were not available in some institutions. Seals and labels were used to secure evidence in storage boxes, and specific

areas were designated as evidence storage zones for management. Network-attached storage (NAS) is universally used, with institutions adapting it to the requirements of storing image files or analysis results. Some institutions use self-developed digital forensic tools, whereas most specialized investigative agencies use CFT and DFT (64-bit). The interview results suggested that when supporting digital forensic work at the Supreme Prosecutor's Office, there is a need for a contact point to provide guidance on the analytical methods, CFT/DFT distribution, sharing of self-developed tools, NDFaaS, and other related matters concerning DFLs [22].

3.2.4. Survey

3.2.4.1 Survey Design

Based on the digital forensic tools/equipment list pool and interview content, the survey was designed by incorporating content from NIST CFTT's Computer Forensics Tools and Techniques Catalog. The validity of the survey content was confirmed by two experts who participated in the interviews and by the research team. Based on their feedback, the content of the survey was revised, and the revisions were refined in three rounds of final discussions. The survey targeted individuals with experience in operating digital forensic tools/equipment, which was reflected in the demographic questions. The survey items were structured around five main themes: preference for commercial digital forensic software, preference for commercial imaging devices, digital forensic tools and equipment that should be provided to individuals, digital forensic tools/equipment that should be provided to a five-person team, and the extent of digital forensic tool usage by function. From September 27 to November 8, 2021, the survey was distributed to approximately 200 digital forensics professionals across the country, and 124 responses were collected for analysis. The survey respondents were 107 males and 17 females, displaying a much higher proportion of males. The age distribution was as follows: 15 respondents in their 20s (12.1%), 50 respondents in their 30s (40.3%), 51 respondents in their 40s (41.1%), and 8 respondents in their 50s (6.5%). The majority of respondents were in their 30s and 40s. In terms of educational background, 2 respondents had an associate degree (1.6%), 58 had a bachelor's degree (46.8%), 55 had a master's degree (44.4%), and 9 had a doctoral degree (7.3%), with the majority holding a bachelor's or master's degree. Regarding affiliation, 61 respondents (58.1%) were from investigative agencies, 8 (6.5%) were from public sectors outside investigative agencies, 23 (18.5%) were from the private sector, and 13 (6.5%) were from other fields, with the majority working in investigative

agencies. Of the investigating agencies, 55 were police agencies. In terms of digital forensics experience, 17 respondents (13.7%) had less than 1 yr of experience, 21 respondents (16.9%) had between 1 and 3 yr, 21 respondents (16.9%) had between 3 and 5 yr, 30 respondents (24.2%) had between 5 and 10 yr, 31 respondents (25.0%) had between 10 and 20 yr, and 4 respondents (3.2%) had more than 20 yr. The largest groups were those with 5–10 and 10–20 yr of experience.

3.2.4.2 Results Analysis

3.2.4.2.1 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 quartile 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 Digitalcollector), ⑩ Blacklight (Cellebrite Inspector), ⑪ Intella, ⑫ Nuix, ⑬ Belkasoft Evidence Center, ⑭ PasswareKit, ⑮ Final Forensic, ⑯ Final Mobile Forensic, ⑰ XRY, ⑱ Oxygen, ⑲ Forensic Explorer, ⑳ CIP, DFAS, DTsearch, Relativity. The analysis revealed that the tools with the highest usage frequency and preference (in the second quadrant) were: ① EnCase, ② FTK, ③ X-Ways, ④ AXIOM, ⑦ MD-Next, and ⑧ MD-RED.

Considering the scatter plot, assigning significance to tools near the intersection in the second quadrant was difficult; therefore, these tools were excluded from the list of preferred tools. The preference evaluation for commercial imaging devices was conducted based on frequency averages (33%) and preference averages (3.31) using quartile analysis. The commercial imaging devices were categorized as follows: ① Falcon (Neo), ② TX-1, ③ TaskForce, ④ TD-3, ⑤ SuperImager, ⑥ CFID, ⑦ Solo (3, 4, 5), ⑧ Magicube. The analysis revealed that the tool with both a high usage frequency and preference (in the second quadrant) was Falcon (Neo), as shown in Figure 3.

3.2.4.2.2 Evaluation Factors for Purchasing/Adopting Digital Forensics Software

The survey respondents were categorized into law enforcement, public sector, and private sector groups to analyze the importance of the evaluation factors when purchasing or adopting digital forensics software. Evaluation factors were categorized into 11 items: speed and performance, accuracy, integrity, reliability, verification and validation status, usability, product updates, training support, vendor support, maintenance costs, and initial acquisition costs. According to the survey results, the most important factors are reliability, integrity, and accuracy (< Figure 4 >).

3.2.4.2.3 Tool Preference by Professional Experience

Preferences for digital forensic tools were analyzed based on professional experience. The categories of professional experience were as follows:

Ⓐ Policy & Planning, Ⓑ Consulting & Advisory, Ⓒ Budget Management, Ⓓ Procurement & Equipment Management, Ⓔ Digital Forensic Analysis, Ⓕ Education & Lecture, Ⓖ Research & Development <Table 3>.

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 Cellebrite Digitalcollector (Macquisition), ⑩ Cellebrite Inspector (Blacklight), ⑪ Intella, ⑫ Nuix, ⑬ Belkasoft Evidence Center, ⑭ PasswareKit, ⑮ Final Forensic, ⑯ Final Mobile Forensic, ⑰ XRY, ⑱ Oxygen, ⑲ Forensic Explorer, ⑳ CIP, DFAS, DTsearch, Relativity.

The survey allowed for duplicate responses to the same item, and the average tool preferences based on professional experience were calculated and compared (Figure 5). Blank spaces in the table represent “Never used,” indicating no preference score for that item.

The tool preferences by professional experience are as follows:

- **Policy & Planning**: MD-Next, MD-RED, Belkasoft Evidence Center, Final Mobile Forensics, EnCase
- **Consulting & Advisory**: ⑧ MD-RED, ④ AXIOM, ⑦ MD-Next, ⑫ Nuix, DTsearch
- **Budget Management**: ⑳ CIP, 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 Forensic, ④ AXIOM

- **Digital Forensic Analysis**: MD-RED, MD-Next, X-Ways, AXIOM, and 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 confirming the tool preference priority based on professional experience, it was observed that certain tools (⑧ MD-RED, ⑦ MD-Next, ④ AXIOM, ③ X-Ways, ① EnCase) consistently emerged as preferred across multiple experience categories.

3.2.4.2.4 One-person Versus Five-person Tool/Equipment Analysis

The tool/equipment preferences for one- and five-person teams were analyzed using frequency and variance analysis methods. In frequency analysis, the responses were converted into numerical values: “Very necessary” was scored 5, “Necessary” was 4, “Neutral” was 3, “Not necessary” was 2, and “Hardly necessary” was 1. The average values and rankings were calculated. For one-person tools/equipment, the workstation for evidence collection and analysis had the highest average score of 4.80, whereas the office laptop had the lowest score of 3.37. For five-person tools/equipment, the workstation for evidence collection and analysis had the highest average score of 4.53, whereas the office desktop PC had the lowest score of 3.72 (<Table 4>).

Levene’s test for equality of variances was performed to verify whether there were significant differences in variances across groups, and this test was followed by a one-way analysis of variance (ANOVA). If the *p*-value was less than 0.05, Scheffé's post-hoc test was conducted (< Table 5 >). The results of the ANOVA and Scheffé post-analysis revealed differences in the following items: office desktop PC, damaged video/CCTV recovery/analysis, and Hex Editor. These results indicate that for one-person required tools/equipment, the investigation/agency group found office desktop PCs, damaged video/CCTV recovery/analysis, and Hex Editors more necessary than did the private sector group. The analysis of five-person team tools/equipment was conducted in the same manner as that for the one-person teams. For the “shared evidence collection and analysis laptop” item, Levene's test for equality of variances was not satisfied. Therefore, an independent sample *t*-test was performed. With a *p*-value less than 0.05, Dunnett’s T3 post-analysis showed that the *F*-value

was -2.057, meaning that the private sector group had a relatively higher need for this tool, compared with the investigation/agency group. For items such as “air purifier, color laser printer, temperature and humidity controller, hairdryer (for drying mobile phones), air compressor, electric screwdriver, JTAG emulator, soldering equipment set, Chip-Off device, and chip reader,” Levene's test for equality of variances was satisfied. The results of the ANOVA and Scheffé's post-analysis indicated that the investigation/agency group had a relatively higher need for these items. These results suggest that when handling digital evidence, the investigation/agency group requires a more elaborate environmental configuration during the preprocessing phase than does the private sector group. A frequency analysis was conducted for the number of workstations, laptops, PCs, office laptops, office PCs, and monitors, based on the one-person and five-person criteria (<Table 6>). The results showed that for the analysis workstations, two units were required: for analysis laptops, one unit for one person and two units for five people; for analysis PCs, one unit for one person and more than four units for five people; for office laptops, one unit was needed; and for office PCs, one unit was required.

The average scores for each item were compared between the one-person and five-person criteria (<Table 7>). The results indicated that for all items, the average score for the five-person criteria was significantly higher ($p < 0.001$). In particular, the difference between the “Number of Evidence Collection and Analysis Laptops (1-Person) vs. Number of Shared Evidence Collection and Analysis Laptops (5-Person)” and “Number of Evidence Collection and Analysis PCs (1-Person) vs. Number of Shared Evidence Collection and Analysis PCs (5-Person)” showed Cohen′s d values of -0.984 and -0.992, respectively, indicating a large effect size. These results suggest that the need for shared equipment for five-person teams is much greater than that for one-person teams.

A multiple response format was used in the survey of digital forensic tools required by one person. EnCase received the highest number of responses, with 116 participants selecting it, and this was followed by X-Ways, FTK, and AXIOM (Figure 6). In addition to the survey items, there were suggestions that analytical utilities outside the listed tools were needed. Among the mobile digital forensic tools required by one person, MD-Red, MD-Next, Final Mobile Forensic, UFED, and AXIOM were the most frequently cited.

3.2.4.2.5 Tool Usage by Analysis Target/Function

The use of digital forensic tools to analyze targets and functions was explored. Analysis targets and functions were categorized based on the NIST Computer Forensics Tools and Techniques Catalog (< Table 8 >).

The post-analysis results showed significant differences in targets and functions (< Table 9 >).

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

The Remote Function/Remote Forensics function was used more by the private sector group than by the law enforcement group. Overall, the law enforcement/investigation group used digital forensic analysis tools for image, mobile, social media, VoIP, and communication/account forensics more frequently than did the private sector group.

4. Research Results

4.1. Digital Forensic Tools/Equipment Lists for One-person and Five-person Teams

The final digital forensic tool/equipment lists for the one-person and five-person teams were derived. These lists were presented to assist each group in establishing digital forensic laboratories. Table 10 lists these parameters. Items that can be packaged together, or those for which there is little difference in purchase costs when considering the budget, are listed in a set format. Although certain items may not be necessary for each institution, the lists were designed to encompass as many standardized elements as possible for both the one-person and five-person team setups. Open-source tools that did not incur additional costs were excluded.

4.2. Implications and Limitations

A standardized list of tools/equipment was created to encompass both the public and private sectors; therefore, the estimated costs may be higher than the actual costs required to set up a digital forensics lab. Hence, it is necessary to select and reflect on the items derived from the list based on the size, mission, and role of each organization. Additionally, the pricing policies for digital forensic commercial products in the Korean market may differ from those available overseas. For instance, domestic markup rates may vary because of exchange rates, which

could result in prices being higher than those abroad. Thus, acknowledging these differences and considering price fluctuations since this study was conducted are important. Furthermore, items such as office furniture and other equipment are of various types, and unlike digital forensic tools, there is no option for selecting a specific product. Therefore, the average price range of products available in domestic settings was considered. In terms of the types of digital forensic tools, analysis demands, and interviews with current professionals revealed that computers and mobile devices are the most heavily used, whereas devices such as drones and IoT devices have less demand and were not considered. The differences between this study and the previous research are as follows. First, based on Korean cases, we gathered insights from current and former personnel involved in digital forensics and reflected these views in our research. Through focus group interviews, we gathered opinions from the perspective of actual users on which tools were most commonly used and what additional equipment was needed. Next, the study expanded the list of digital forensic tools to include all the potential items needed to establish a digital forensics lab. We also visited investigative agencies and appraisal institutions specializing in digital forensics to conduct on-site inspections and interviews to address gaps in the process. Additionally, we conducted a survey of 124 digital forensics professionals to analyze their preferences for tools and equipment. Finally, the derived list and estimated budget from this research were presented to those involved in the establishment of digital forensics labs, who provided feedback to further refine the list and minimize any gaps.

5. Conclusion

This paper presents a list of the tools and equipment required to establish a DFL in South Korea. Additionally, the necessary budget items for the adoption of these tools and equipment in organizations with two or fewer people as well as five or fewer people were calculated. The maximum estimated budget for setting up a DFL is approximately $300,795 for a two-person organization and $585,700 for a five-person organization. The major contribution of this study is that it not only considers the acquisition of digital forensic tools and equipment but also evaluates additional budget requirements related to other secondary factors. For instance, interior design elements, such as internal construction, are often overlooked by many organizations. However, considering media exposure and the spread of outcomes related to digital forensics, incorporating aesthetic elements during a functional setup is crucial, as noted

by professionals in the field. This study actively reflects on these insights. Furthermore, spatial layout considerations are addressed. Rather than assuming only a designated area, we focused on dividing the space based on a digital forensic workflow, such as field deployment, reception/pre-processing, storage, participation/observation, and analysis, to derive the necessary tools and equipment. Additionally, office environment elements that support digital forensic functions are considered. The significance of this research lies in its provision of practical standards for the implementation of digital forensic functions, based on the assumption of available personnel and space by identifying the maximum elements that can be constructed within these conditions. However, this study has limitations. As this study is based solely on the Korean context, there may be differences in the derived list and budget, compared with international practices. Additionally, although user preferences were considered, the study lacked a thorough verification of objective quantitative indicators with which to assess the tools. There are also limitations to the survey, which was conducted in 2021 and therefore may not reflect the latest trends. The fundamental issues of securing budgets and personnel must be explored further in future research. This study used surveys to derive an overall list of tools and equipment that represent a methodological approach. However, several aspects require further investigation. These include examining the factors that influence tool selection, such as subscription-based payment models (e.g., for FTK or AXIOM) and the burdens that these may impose, the preferred tools and usage levels based on the volume of evidence processed, and changing preferences for tools/equipment over time, as well as comparing preferences across different subgroups by segmentation. Future research should address the differences between the preferred and actual tools used by digital forensics professionals. In addition, discussions regarding tool/equipment lists in relation to the operational direction of DFLs are required. For example, the tools and equipment required for a DFL in a local police department may differ from those required to handle national security-related cases. Special investigation officers also have different tools and equipment requirements, depending on the field. Furthermore, the analyses of tools/equipment preferences based on the type of case and the differences between departments with high personnel turnover and those with stable staffing are important. Statistical data on tools and equipment based on digital evidence analysis reports could also be valuable. Moving forward, comparing past and present data would be beneficial, particularly in studying the paradigm shift toward clouds or AI forensics.

References

[1] Lyle, J. R., et al., Digital Investigation Techniques: A NIST Scientific Foundation Review, OSAC DE Quality Task Group Report, Dec. 2022.

[2] Sunde, N., Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation, Master's thesis, Norwegian University of Science and Technology, 2017.

[3] ENFSI, Best Practice Manual for the Forensic Examination of Digital Technology, ENFSI-BPM-FIT-01, ver.01, Nov. 2015.

[4] INTERPOL, INTERPOL Global Guidelines for Digital Forensics Laboratories, INTERPOL, Lyon, 2019.

[5] SWGDE, SWGDE Framework of a QMS for DME-FSSPs, Sep. 2017.

[6] SWGDE, SWGDE Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence, May. 2010.

[7] International Organization for Standardization, ISO/IEC 17025:2017 — General Requirements for the Competence of Testing and Calibration Laboratories, ISO, Geneva, 2017.

[8] Lawrence, T., Karabiyik, U., Shashidhar, N., "Equipping a Digital Forensic Lab on a Budget", Proceedings of the 6th International Symposium on Digital Forensic and Security (ISDFS), IEEE, 2018, pp. 1–6.

[9] O'Connor, R. V., "Software Selection: Towards an Understanding of Forensic Software Tool Selection in Industrial Practice", International Journal of Technology, Policy and Management, vol. 5, no. 4, 2000, pp. 311–329.

[10] Hibshi, H., Vidas, T., Cranor, L., "Usability of Forensics Tools: A User Study", Proceedings of the 6th International Conference on IT Security Incident Management and IT Forensics, IEEE, 2011.

[11] Nodeland, B., Belshaw, S., "Establishing a Criminal Justice Cyber Lab to Develop and Enhance Professional and Educational Opportunities", Security and Privacy, vol. 3, no. 5, 2020, e123.

[12] Roman, R. F. M., Loja, N. M., Novillo, J. P., Piña, J. I., "Digital Forensics Tools," International Journal of Applied Engineering Research, vol. 11, no. 19, 2016, pp. 9754–9762.

[13] NIST, Computer Forensic Tool Catalog.

[14] Ghazinour, K., et al., "A Study on Digital Forensic Tools," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), IEEE, 2017.

[15] Padmanabhan, R., et al., "Comparative Analysis of Commercial and Open Source Mobile Device Forensic Tools," Proceedings of the 9th International Conference on Contemporary Computing (IC3), IEEE, 2016.

[16] Jang, Y.-S., National Police Agency: Digital Forensics Laboratory Standard Design Study, 2017, p. 129.

[17] Hassan, N. A., "Computer Forensics Lab Requirements," in Digital Forensics Basics: A Practical Guide Using Windows OS, 2019, pp. 69–91.

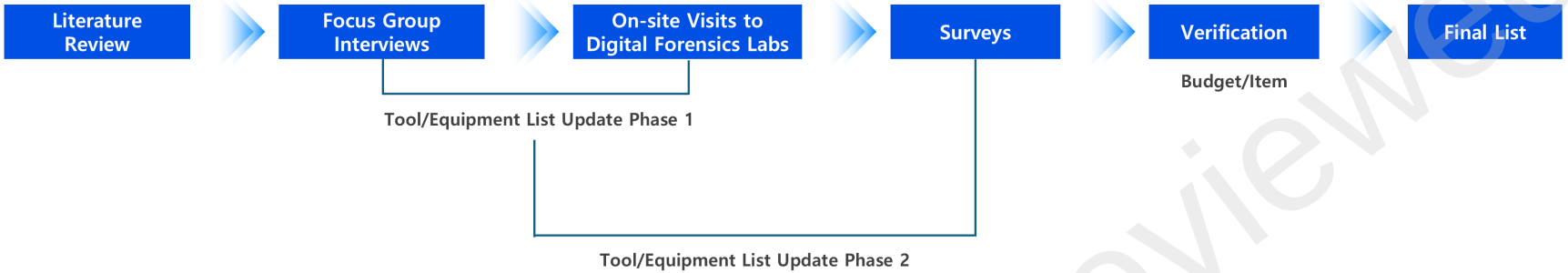
[18] Morgan, D. L., The Focus Group Guidebook: Focus Group Kit 1, Sage Publications, Thousand Oaks, CA, 1998.

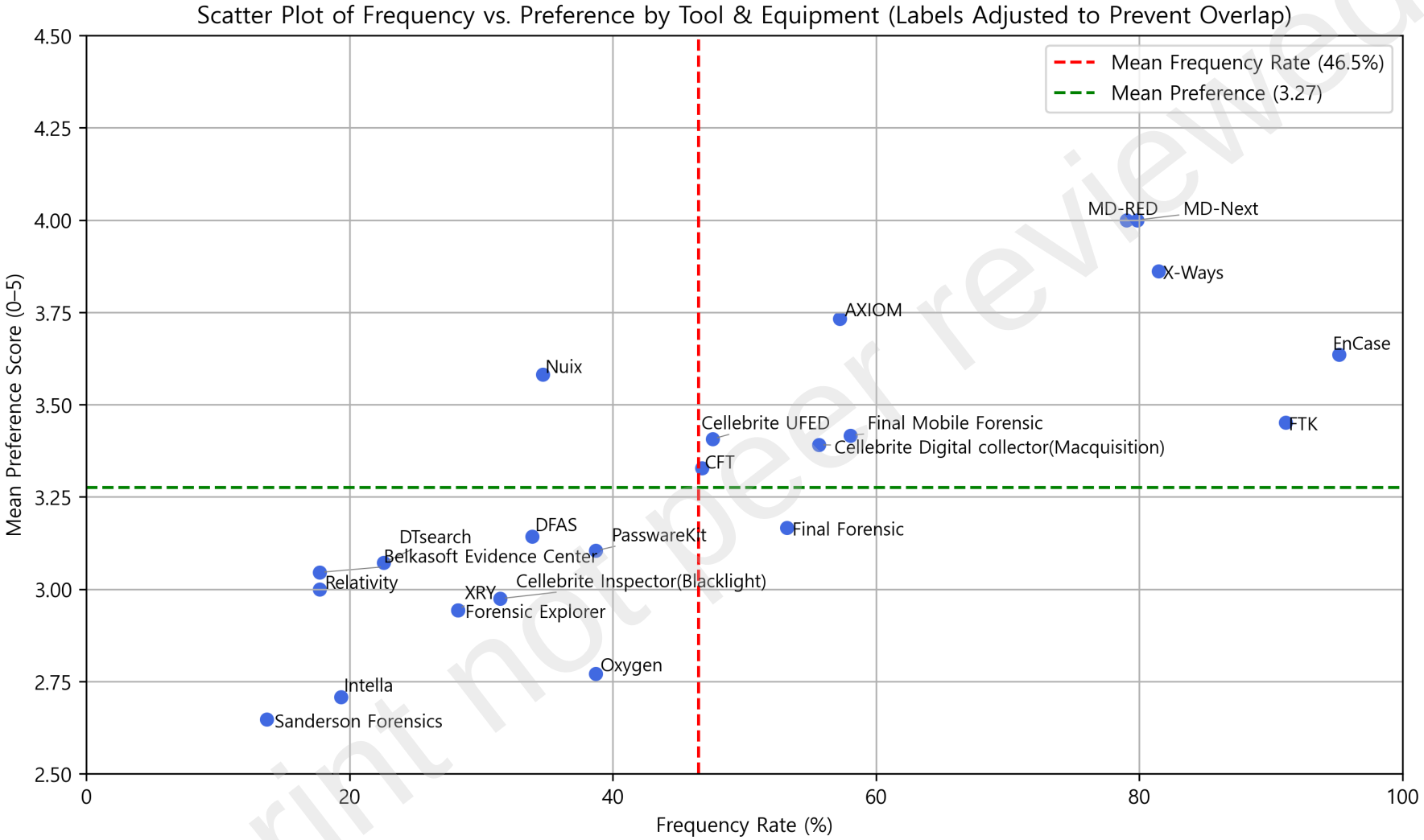
[19] Morgan, D. L., Focus Groups as Qualitative Research, (Translated by the Korean Society of Qualitative Research in Nursing), Gunja Publishing House, 2007, p. 42.

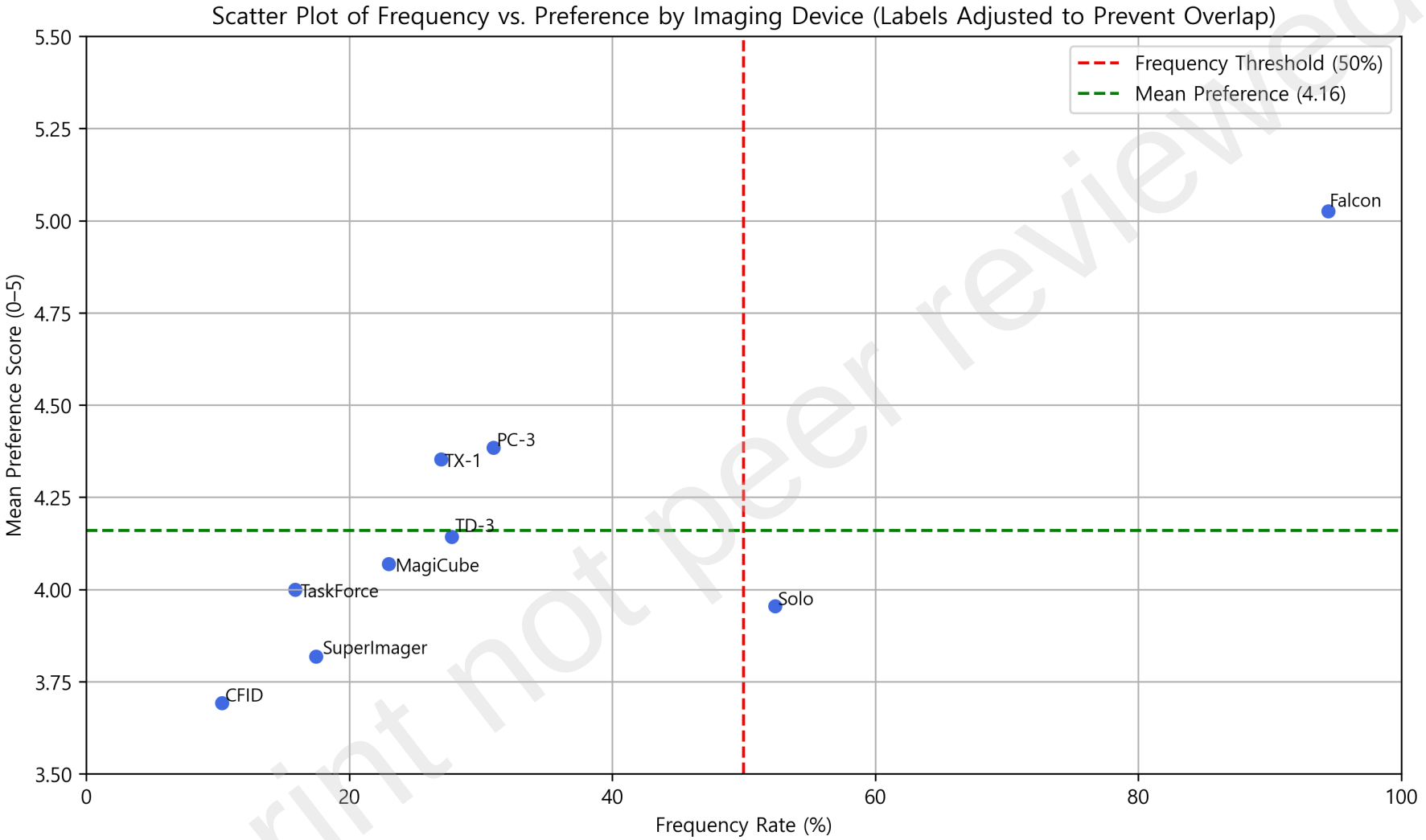
[20] Shin, S.-M., Park, H.-M., Kim, G.-B., "A Study on the Methods of Building Tools and Equipment for Digital Forensics Laboratory," Journal of Information and Security, vol. 22, no. 5, 2022, pp. 21–35.

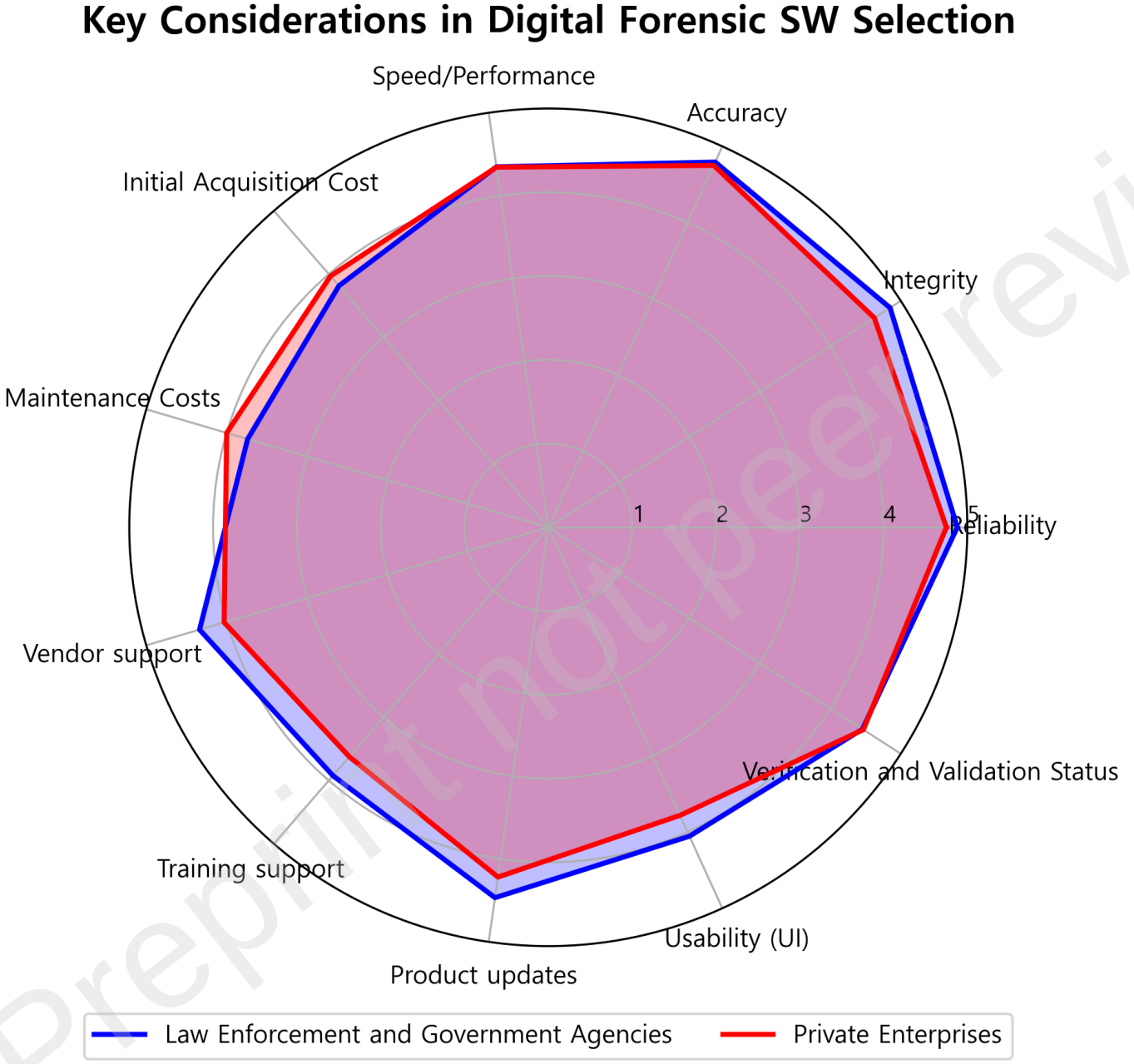
[21] Shin, S.-M., Hong, J.-W., Kim, G.-B., "A Study on the Optimization of Digital Forensics Laboratory Infrastructure," Journal of Digital Forensics, vol. 23, no. 1, 2023, pp. 45–62.

[22] Supreme Prosecutors' Office, Research on the Standard Model for Building a Digital Forensic Laboratory, SPO, Seoul, 2021.

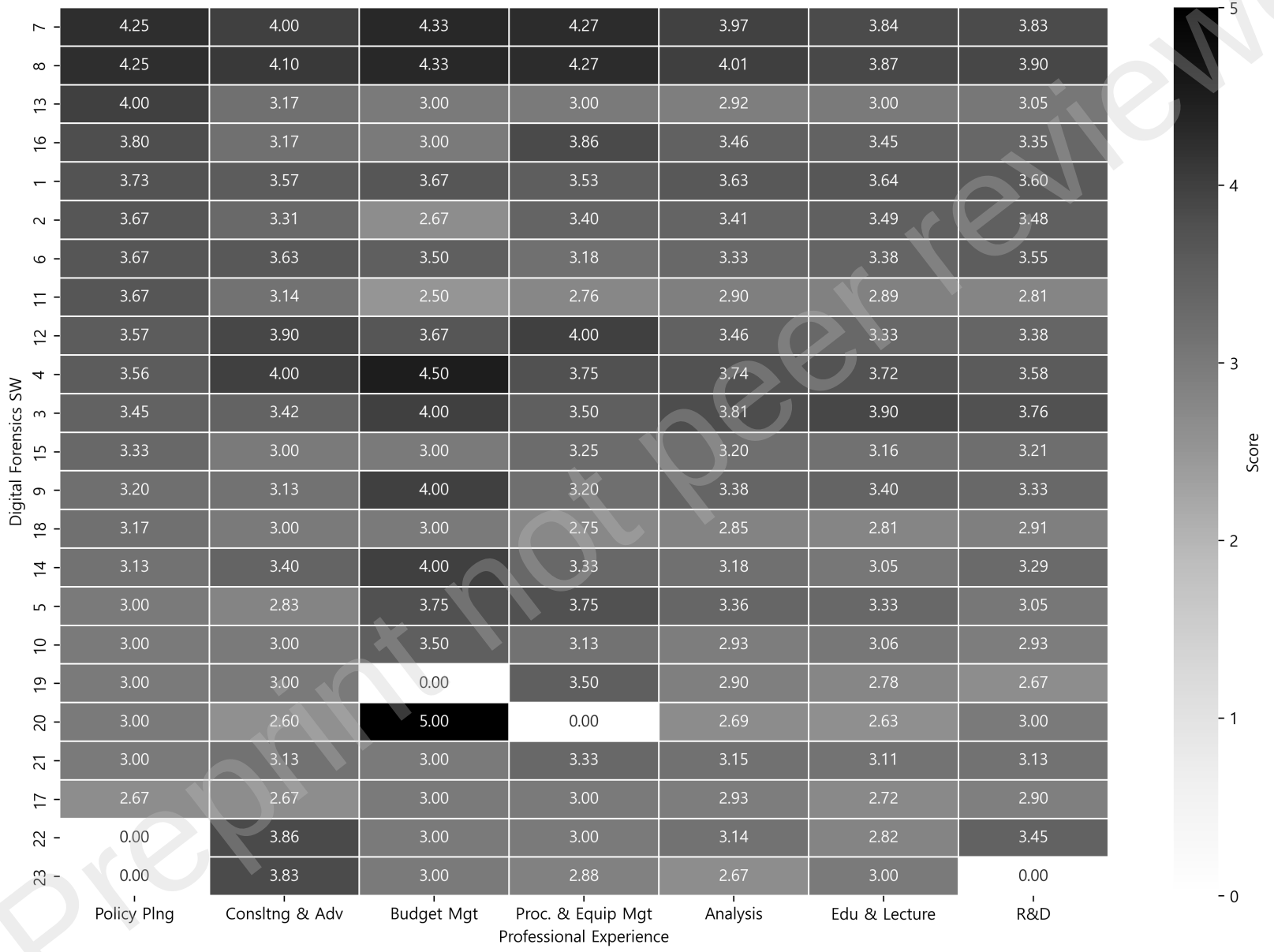








Preference Scores by Professional Experience and Digital Forensics SW



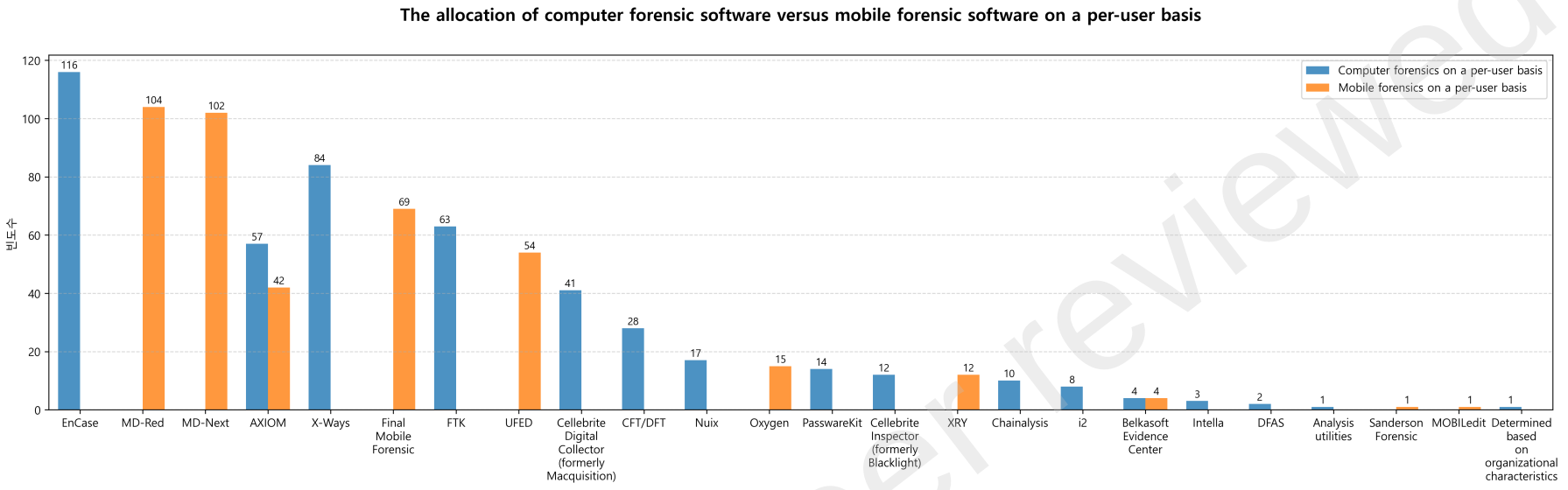


Table 1. General Information of Focus Group Interview Participants

No	Gen	Age	Affiliation	Position	Exp (Years)	Round
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

Table 2. On-site Visits to Digital Forensics Labs and Interview Summary

No	Type	Date	Number of Members (People)	Method
1	Law Enforcement Agency	2021.6.18	5	On-site Visit/Interview
2	Analysis/Appraisal Agency	2021.9.15	4	On-site Visit/Interview
3	Law Enforcement Agency	2021.9.17.	4	Interview
4	Law Enforcement Agency	2021.9.24	4	On-site Visit/Interview
5	Law Enforcement Agency	2021.10.11	20 or more	On-site Visit/Interview
6	Law Enforcement Agency	2021.10.27	4	On-site Visit/Interview

Table 3. Descriptive Statistics of Respondents' Professional Experience

Professional Experience	Number of Individuals	Percentage (%)	Professional Experience	Number of Individuals	Percentage (%)
Policy Plng	15	6.60%	Analysis	93	40.60%
Consltng & Adv	14	6.10%	Edu & Lecture	47	20.50%
Budget Mgt	4	1.70%	R&D	35	15.30%
Proc. & Equip Mgt	21	9.20%	Total	229	100.00%

Table 4. Frequency Analysis of Required Tools/Equipment (Individual Versus Five-member Teams)

Category	Individual							Five-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	7	68	37	9	7	3	4.29	5
PC for Evidence Collection and Analysis	61	30	20	5	8	4.06	8	58	34	17	10	5	4.05	8
Collection and Analysis Office Laptop	22	32	51	9	10	3.37	10	44	32	27	13	8	3.73	9
Office Desktop PC	28	35	47	7	7	3.56	9	44	33	24	14	9	3.72	10
Monitor	90	23	10	0	1	4.62	5	53	43	16	8	4	4.07	7
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

Table 5. Scheffé Post-hoc Test Results (Required Tools/Equipment for Individual Versus Five-member Teams)

Category		Avg		F	Post-hoc	Group		Mean Diff	Std. Error	Sig	95% Conf. Int.	
		A	B			I	J				L	U
Required Tools/ Equipment per Person	Office Desktop PC	3.73	3.09	8.773*	S	A	B	0.63	0.21	0.004*	0.22	1.05
	Damaged Video/CC TV Recovery & Analysis SW	4.17	3.31	15.793*	S	A	B	0.86	0.25	0.000*	0.37	1.35
	Hex Editor	4.27	3.78	5.634*	S	A	B	0.49	0.23	0.019*	0.04	0.94
Required Shared Tools/Equipment for Five People	Laptop for Evidence Collection & Analysis	4.2	4.56	-2.057*	D	A	B	-0.37	0.18	0.043*	-0.72	-0.02
	Air Purifier	4.34	3.75	9.924*	S	A	B	0.59	0.2	0.002*	0.19	0.99
	Color Laser Printer	4.07	3.59	6.354*	S	A	B	0.47	0.2	0.013*	0.08	0.86
	Temperature and Humidity Control Device	4.02	3.56	5.562*	S	A	B	0.46	0.19	0.020*	0.08	0.84
	Hair Dryer (for Mobile Phone Drying)	3.72	3.25	4.770*	S	A	B	0.47	0.21	0.031*	0.06	0.88
	Air Compressor	3.57	3.16	4.452*	S	A	B	0.41	0.2	0.037*	0.02	0.8
	Electric Driver	4.25	3.81	5.768*	S	A	B	0.44	0.21	0.018*	0.02	0.86
	JTAG Emulator	4.02	3.38	9.216*	S	A	B	0.65	0.23	0.003*	0.18	1.11
	Soldering Equipment Set	3.75	3.28	4.251*	S	A	B	0.47	0.23	0.041*	0.01	0.93
	Chip-Off Device	3.84	3.19	8.068*	S	A	B	0.65	0.23	0.005*	0.19	1.11
	Chip Reader	3.92	3.44	5.026*	S	A	B	0.49	0.22	0.027*	0.04	0.93

※ **Post-Hoc: S (**Scheffe), **D (**Dunnett T3) / **95% Confidence Interval: L (**Lower Bound), **U (**Upper Bound)

Table 6. Required Number of Workstations, Laptops, and Monitors (Individual Versus Five-member Teams)

Category	Individual						Five-member Teams					
	A	B	C	D	E	Avg	A	B	C	D	E	Avg
Number of Workstations for Evidence Collection and Analysis	3	13	56	51	1	1.726	32	31	40	17	4	2.565
Number of Laptops for Evidence Collection and Analysis	1	1	14	104	4	1.121	30	20	40	25	9	2.298
Number of PCs for Evidence Collection and Analysis	1	3	17	85	18	1.065	35	20	32	23	14	2.315
Number of Office Laptops	1	0	3	86	34	0.774	20	9	28	52	15	1.734
Number of Office PCs	1	0	4	104	15	0.935	20	8	25	53	18	1.669

Table 7. Paired *t*-test and Cohen's *d* Results (Individual Versus Five-member Teams)

Item Pairs	Mean Difference	*p*-value	Cohen's *d*	Significance	Effect Size
Person 01 versus Five People 01	-0.839	0.000	-0.666	Significant	Medium
Person 02 versus Five People 02	-1.177	0.000	-0.984	Significant	Large
Person 03 versus Five People 03	-1.250	0.000	-0.992	Significant	Large
Person 04 versus Five People 04	-0.960	0.000	-0.783	Significant	Medium–Large
Person 05 versus Five People 05	-0.734	0.000	-0.581	Significant	Medium

※ **Small:** < 0.2, **Medium:** < 0.5, **Large:** < 0.8

※ **01:** Number of Workstations for Evidence Collection and Analysis, **02:** Number of Laptops for Evidence Collection and Analysis, **03:** Number of PCs for Evidence Collection and Analysis, **04:** Number of Office Laptops, **05:** Number of Office PCs

Table 8. Categorize Tools/Equipment by Digital Forensics Analysis Target/Function

Analysis Targets	Functions
Analysis Targets were classified into: • Cloud Service Forensics • Database Forensics • Drone Forensics • Computer Forensics Tools (Mac) • Computer Forensics Tools (Win) • GPS Forensics • Image Forensics (Video & Graphics) • Infotainment & Vehicle Forensics • Instant Messenger Forensics • Mobile Forensics (Device 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 Function/Remote Forensics • Steganography Analysis

	• String Search • Video Format Conversion • Web Browser Analysis • WiFi Analysis • Windows Registry Analysis • Forensic Boot Environment (Live CD/USB)

Table 9. Post-hoc Analysis Results (Use of Tools by Digital Forensic Target or Function)

Category		Avg		F	Post-hoc	Group		Mean. Diff	Std. Error	Sig	95% Conf. Int.	
		A	B			I	J				L	U
Target of Analysis	Image Forensics (Video & Graphics)	3.43	2.72	8.024*	S	A	B	0.72	0.23	0.005*	0.26	1.17
	Mobile Forensics (Acquisition, Analysis, and Triage)	4.65	4.09	2.311*	D	A	B	0.56	0.24	0.026*	0.09	1.03
	Social Media Forensics	3.23	2.62	4.290*	S	A	B	0.6	0.27	0.040*	0.06	1.15
	Video Analysis Forensics	3.7	2.47	22.308*	S	A	B	1.23	0.26	0.000*	0.71	1.75
	VoIP Forensics	2.22	1.78	4.202*	S	A	B	0.44	0.2	0.043*	0.04	0.84
	Communication & Account Forensics	2.7	2.16	2.179*	D	A	B	0.54	0.24	0.033*	0.06	1.02
Analytical Function(s)	Hardware Write Blockers	4.4	3.97	4.088*	S	A	B	0.43	0.23	0.045*	-0.01	0.88
	Image Analysis (Video & Graphics)	3.85	2.94	12.785*	S	A	B	0.91	0.25	0.001*	0.41	1.41
	Remote Forensics	2.27	2.81	-2.132*	D	A	B	-0.54	0.25	0.039*	-1.04	-0.05
	Video Format Conversion	3.03	2.31	7.518*	S	A	B	0.72	0.26	0.007*	0.21	1.23

※ **Post-Hoc: S (**Scheffe), **D (**Dunnett T3) / **95% Confidence Interval: L (**Lower Bound), **U (**Upper Bound)

Table 10. Suggested Items and Budget for Digital Forensics Lab Setup (Individual Versus Five-member Teams)

Category			Item	Unit	Unit Price (USD)	Individual		Five-member Teams	
						Qty	Amount (USD)	Qty	Amount (USD)
Computer	HW		• Workstation (with built-in write blocker)	EA	10,000.0	2	20,000	5	50,000
			• Monitor (with privacy filter attached)	EA	266.7	6	1,600.2	15	4,000.5
			• Office Desktop PC	EA	666.7	2	1,333.4	3	2,000.1
			• Office Laptop	EA	2,000.0	2	4,000	3	6,000
	SW (Commercial)	Computer Forensic	• EnCase	Copy	5,333.3	1	5,333.3	1	5,333.3
			• AXIOM	Copy	7,333.3	1	7,333.3	1	7,333.3
			• X-Ways	Copy	3,066.7	1	3,066.7	1	3,066.7
			• DFT(CFT)	Copy	0	1	0	1	0
			• FTK	Copy	5,666.7	0	5,666.7	1	5,666.7
		Infra/ Support	• Vmware • MS-Office / Windows or Mac OS	Copy	533.3	2	1,066.6	2	1,066.6
	Accessories		• Driver Kit	**Set**	146.7	1	146.7	3	440.1
			• HDD Docking Station	EA	46.7	1	46.7	3	140.1
			• M.2 Docking Station	EA	66.7	1	66.7	2	133.4
			• Cables	**Set**	33.3	1	33.3	3	99.9
			• Hard Drive for Evidence Duplication (1 TB)	EA	56.7	5	283.5	10	567
			• Hard Drive for Evidence Duplication (2 TB)	EA	66.7	5	333.5	20	1,334
			• Hard Drive for Evidence Duplication (4 TB)	EA	133.3	5	666.5	10	1,333
			• External SSD (2 TB)	EA	366.7	4	1,466.8	10	3,667
			• USB Drive (OTG-Compatible / 64 GB)	EA	26.7	20	534	20	534
			• USB Drive (OTG-Compatible / 128 GB)	EA	40.0	20	800	20	800
			• DVDs for Evidence Submission (100 discs)	EA	30.0	1	30	3	90
			• External ODD (Optical Disc Drive)	EA	53.3	1	53.3	3	159.9
			• KVM Switch	EA	200.0	2	400	5	1,000
Mobile	Mobile Forensic (Commercial)		• MD-Next	Copy	22,000.0	1	22,000	2	44,000
			• MD-RED	Copy	56,666.7	1	56,666.7	2	113,333.4
			• Cellebrite UFED 4 PC	Copy	19,333.3	1	19,333.3	2	38,666.6
			• Final Mobile Forensic	Copy	66,666.7	1	66,666.7	2	133,333.4
			• Mobile Analysis Tools for On-Site Investigations	Copy	30,000.0	1	30,000	2	60,000
	Accessories		• Mobile Phone Cables • SD Card and USIM Reader • Multi-Charger for Mobile Phones • Storage Pouches	Set	266.7	1	266.7	3	800.1
	Field Kit		• High-Performance 17-in Laptop for Field • Wireless Keyboard and Mouse • Portable Printer • Various Cables, Gender Converters, Pliers, Driver Kit, Flashlight, Multi-tap • Anti-Static Bags/Cases • External Storage Devices (SSD, HDD) • External USB/CD-ROM Drive • Bootable USB/CD Media • Portable Bag, Carrier, or Storage Box • Hardware Write Blocker (External) • Notepad and Writing Instruments	Set	4,666.7	2	9,333.4	4	18,666.8
Evidence Photography			• Camcorder	EA	733.3	1	733.3	1	733.3
			• GPS Watch	EA	933.3	1	933.3	1	933.3
			• Lighting Equipment	EA	66.7	1	66.7	1	66.7
			• Evidence Display Board	EA	66.7	1	66.7	1	66.7
			• Capture Board	EA	200.0	1	200	1	200
Imaging Equipment			• Falcon Neo	EA	5,866.7	1	5,866.7	3	17,600.1
			• TX-1	EA	4,333.3	1	4,333.3	2	8,666.6
Reception/Preprocessing			• Security Evidence Bag, Faraday Bag • Anti-Static Bags • Sealing Labels, Stickers	Set	1,433.3	1	1,433.3	1	1,433.3
Storage			• Evidence Storage Boxes	Set	100.0	1	100	3	300
			• Evidence Storage Cabinets	EA	400.0	1	400	3	1,200
			• Forensic Tools/Equipment Cabinet	EA	400.0	2	800	4	1,600
			• Fireproof Safe	EA	533.3	1	533.3	2	1,066.6
Participation/Observation			• LED TV (75 in)	Unit	2,666.7	1	2,666.7	1	2,666.7
			• Wireless Keyboard/Mouse Set	Unit	66.7	1	66.7	1	66.7
			• Video Switch	Unit	2,000.0	1	2,000	1	2,000

Category	Item	Unit	Unit Price (USD)	Individual		Five-member Teams	
				Qty	Amount (USD)	Qty	Amount (USD)
IT/Network	• Switch/Router (Including Installation & Auxiliary Costs)	Unit	3,333.3	1	3,333.3	1	3,333.3
	• Network Rack	EA	333.3	1	333.3	1	333.3
	• NAS (Including HDD)	Unit	3,333.3	1	3,333.3	1	3,333.3
	• Color Multifunction Printer	Unit	400.0	1	400	3	1,200
Security	• CCTV	Unit	666.7	2	1,333.4	2	1,333.4
	• CCTV Monitor	Unit	200.0	1	200	1	200
	• CCTV NVR	Unit	400.0	1	400	1	400
	• Electronic Door Lock	Unit	200.0	2	400	2	400
Office Furniture/Miscellaneous	• Forensic Lab Main Desk	EA	333.3	2	666.6	10	3,333
	• Forensic Lab Assistant Desk	EA	266.7	2	533.4	10	2,667
	• Forensic Lab Office Chair	EA	266.7	2	533.4	7	1,866.9
	• Conference Table	EA	266.7	0	0	1	266.7
	• Conference Chair	EA	266.7	0	0	6	1,600.2
	• Observation Room Table	EA	266.7	1	266.7	1	266.7
	• Observation Room Chair	EA	266.7	4	1,066.8	8	2,133.6
	• Large TV for Conference Room (75 inches)	EA	2,666.7	0	0	1	2,666.7
	• Refrigerator	EA	533.3	0	0	1	533.3
	• Coffee Machine	EA	533.3	0	0	1	533.3
	• Air Purifier	EA	400.0	1	400	4	1,600
	• Multifunction Printer	EA	666.7	1	666.7	1	666.7
	• Copier	EA	1,000.0	0	0	1	1,000
	• Shredder	EA	533.3	1	533.3	1	533.3
Interior Construction	• Interior and Network Construction (Including Wall Installations/Removal, Raised Flooring, Acoustic Panels, Etc.)	Package	13,333.3	1	13,333.3	1	13,333.3
Total Price (USD)					**300,793.3**		**585,696.7**