NISTIR 8412

Results from a Black-Box Study for Digital Forensic Examiners

Barbara Guttman
Mary T. Laamanen
Craig Russell
Chris Atha
James Darnell

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8412

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8412

Results from a Black-Box Study for Digital Forensic Examiners

Barbara Guttman
Mary T. Laamanen
Craig Russell
Software and System Division
Information Technology Laboratory

†Chris Atha
††James Darnell
†National White Collar Crime Center
†† United States Secret Service

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8412

February 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Internal Report 8412
(February 2022)

National Institute of Standards and Technology Interagency or Internal Report 8412
Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8412, 58 pages (February 2022)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8412

Acknowledgements

Thanks to the members of the National Institute of Standards and Technology (NIST) scientific foundation review panel for digital investigations, John M. Butler, James R. Lyle, Corrine Lloyd, Christina A. Reed and Kelly Sauerwein for providing editorial feedback in drafting this report.

Thanks to Richard Ayers, James R. Lyle, Tracy Walraven, and Todd Zwetzig for providing feedback on the study design and workflow.

Thanks to the US Secret Service and the National White Collar Crime Center (NW3C) for providing their staff James Darnell and Chris Atha to develop the two test artifacts. James Darnell is currently the Chief Operations Officer, VTO Labs; at the time of this study he served at the Mobile Device Forensics Program Manager, United States Secret Service and provided the mobile case study. Chris Atha, is aTech Crimes Specialist at the National White Collar Crime Center (NW3C) and provided the hard drive case study.

Abstract

The National Institute of Standards and Technology (NIST) conducted a black-box study in conjunction with a scientific foundation review documented in *NISTIR 8354 – Digital Investigation Techniques: A NIST Scientific Foundation Review* (initially released as a draft report for public comments [1]). The purpose of the study was to evaluate the outcomes of mobile and hard-drive forensic results achieved on mock examinations based on the demographic characteristics of the participants. The demographic data related to an individual's workplace environment, education, and work experience. This study was open to anyone in the public or private sectors who work in the field of digital forensics. This document describes the methodology used in the study and a summary of the results.

Keywords

Black-box study; computer hard drive examination; digital examiner; digital forensics; mobile device examination; scientific foundation review.

TABLE OF CONTENTS

List of Tables

List of Figures

Executive Summary

The black-box study was designed and conducted to understand how the work environment, education level, training, and job experience of digital examiners would impact the analysis outcome from mock casework in digital investigations. The study featured disk images of two well established forensic tracks: a mobile device investigation and a computer hard disk examination. Participation in this study was open to anyone who self attested to conducting digital forensics as part of their employment duties. The registration process consisted of answering mandatory demographic questions and selection of two possible mock examinations, each with twenty-four multiple choice questions, designed by practitioners from the digital forensic field.

Two teams of multiple forensic practitioners crafted and reviewed the test scenarios and related questions, which contained varying levels of difficulty but were not overly exhaustive. Questions ranged from basic, such as identifying who the user of the phone had contacted, to advanced questions related to the use of the TOR browser which encrypts data to provide anonymity to users. The multiple-choice question format was used as a definitive way to capture results by providing the study participants with a list of potential outcomes for question. An additional intentional design decision made was to provide a "skip this question" option as a possible result for each of the multiple-choice questions. This was done to allow participants to answer each question and avoid having them guess an answer if time constraints or circumstances on their end did not allow them sufficient time to work through a complete analysis of a question.

The total number of participants who completed the study for both tests were small compared to the number of registered individuals. The small sample size of results from the mobile and hard drive tests results were not statistically significant to draw meaningful conclusions about the tactical and experiential efficacy of the individual.

Despite this limitation of the study, it demonstrated that digital forensic examiners could answer difficult questions related to the analysis of mobile phones and personal computers. Responses to the study underscored the size, variety, and complexity of the field. The study received responses from examiners working in international, federal, state, local governments, and private labs whose major work included law enforcement, defense, intelligence, and incident response/computer security. There were also many responses from people outside of these areas.

In future studies of forensic practitioners, the use of a black-box study format like this one can provide researchers a blueprint to help capture the state of the discipline. This approach of tethering the demographics of participants to their test outcomes provided a measure of insight into how structural vehicles such as work environments, educational levels and biases converge to affect investigative results.

1 Introduction

The National Institute of Standards and Technology (NIST) has conducted a series of scientific foundation reviews for multiple forensic science disciplines including DNA Mixture Interpretation, Firearm Examination, and Digital Investigation Techniques. "A scientific foundation review is a study that seeks to document and evaluate the foundations of a scientific discipline, that is, the trusted and established knowledge that supports and underpins the discipline's methods. These reviews seek to answer the question: "What empirical data exist to support the methods that forensic science practitioners use to evaluate evidence? [2]".

NISTIR 8354 – Digital Investigation Techniques: A NIST Scientific Foundation Review (initially released as a draft report for public comments) identifies and classifies the methods and techniques used by digital investigators. The review lists supporting literature (peer reviewed, if available) for validating the reliability of the methods and techniques used in the fields and seeks to determine whether these scientific approaches, and practices used for digital forensics are well supported and suitable for use[1].

NIST conducted a black-box study for digital forensic practitioners. This black-box study is a segment of the digital forensics scientific foundation review and was designed to evaluate the accuracy of digital discovery by examiners. Digital discovery is the process of acquiring, preserving, identifying, analyzing and reporting on digital information. This study aimed to measure and amalgamate the state of the practice and any contributing factors that influence the outcome of results. It sought to gain knowledge about the state of practice; it did not seek to establish an "error rate" for the field. The study did not achieve its full objectives, but was able to demonstrate the core capabilities of the field and to highlight the diverse nature of digital forensics as practiced.

The purpose of a digital forensic investigation is to determine if a device contains information that is useful for a criminal, civil or other investigation. The results can be used for conviction or exoneration. An investigation involves identifying, processing, extracting and documenting evidence that can be used in a court of law. Practitioners in this field rely on various tools and methods during an investigation which can impact their conclusions regarding the forensic data. This black-box study was conducted to see if outcomes reached by digitial investigators greatly differed based on question difficulty and self attested demographic descriptions. This document provides a summary of the study results.

1.1 Purpose and Scope

The purpose of the black-box study for forensic examiners was to evaluate the outcome of digital forensic practices used in both the public and private sectors. This was accomplished by measuring the performance of examiners when presented with a simulated digital forensic case. The study provides a sense of how accurately and uniformly digital evidence is examined by practitioners. Individuals who conduct digital examinations on computer hard drives or mobile phones as part of their work duties for law enforcement, criminal defense, intelligence, corporate security, incident response and other practices were invited to participate in this study. Potential participants were made aware of this study through a presentation at the American Academy of

Forensic Sciences in February 2020 and a NIST press release and GovDelivery email blast in June 2020.

This research was conducted in compliance with the Office of Management and Budget (OMB) Paperwork Reduction Act (PRA) and NIST Institutional Review Board (IRB) requirements.

1.2 Organization of this Document

This document presents the results from the blackbox study for digital forensic examiners. Section 3 provides an overview of the entire study, describing its design and format for capturing and recording the collected data. Sections 4 through 8 contain the findings from the mobile case scenario while Sections 9 through 12 cover the findings from the hard drive case scenario. Section 13 provides a conclusion to the entire study based on the results from both the mobile and hard drive study tracks.

2 Terms and Acronyms

Table 1. Terms and Acronyms

Digital artifacts	Objects that have a forensic value during an investigation and contain data or evidence that something has occurred. Digital artifacts include things like registry keys, files, timestamps, and event logs.
Digital discovery	The process of acquiring, preserving, identifying, analyzing and reporting on digital information
Disk partition	A logical division of the physical disk of a hard drive into segments. These segments are separated from other segments which could allow for storage of different files systems.
E01	A file extension used to identify an image file created using the Encase software.
Encase	A suite of forensic tools developed by Guidance Software. In forensic investigations the software is used to recover evidence from seized hard drives.
EWF	Expert Witness Format. The EWF files are a type of disk image. They can contain the contents and structure of an entire disk storage device.
File hash	A unique value assigned to the contents of a file. In digital forensic investigations it can be used to identify and filter out known files.
File signature	Data stored in a file used to identify its contents. This can include the extension of a file and the magic number. The magic number is the first few bytes stored at the beginning of a file that identifies the file type.
Galaxy 6	Samsung phone model

Image File	An electronic copy of the original evidence acquired during a forensic investigation. It is a copy of all the unaltered electronic information stored on a device, such as a fixed disk, removable disk, flash drive, etc.
JPG	A file with the extension JPG stores a digital image in a compressed format standardized by the Joint Photographic Experts Group.
Linux	An open-source operating system based on UNIX and released on September 17, 1991 by Linus Torvalds.
MAC	Media Access Control. This is a unique hardware identifying number known as an address that identifies each device on a network.
Magic file	A Linux file that contains lines that describe the magic numbers or unique identifiers used to identify file types.
Magic number	The first few bytes of a file that can be used to identify a particular type of file. These bytes can be used to determine a file type without using a file extension.
NirSoft	A unique collection of small and useful freeware utilities for analysis.
OSAC	The Organization of Scientific Area Committees for Forensic Science.
PDF	Portable Document Format. A file format that allows for sharing and printing saved files.
Playstore	The Google Playstore used to acquire apps on Android devices.
RAM	Random Access Memory. It is the temporary storage for all the data on a device needed at the current time or soon.
SD	Standard Deviation. A measure of how dispersed the data is in relation to the mean.
TOR	An open-source browser that encrypts data providing anonymity.
VIN	Vehicle Identification Number. An identifying number for a specific vehicle.
WiFi	WiFi is a collection of wireless network protocols based on the IEEE 802.11 standards. These standards are used for local area networking of devices and internet access using radio waves to exchange data.
WSL	Windows Subsystem for Linux. This is a feature of Windows 10 that enables you to run native Linus command-line tools.

3 Study Design

The criteria for the study were designed with the purpose to determine whether participants could report accurate and reliable results when examining data found on a hard drive or mobile phone. Participation in the study was voluntary and required respondents to complete an online consent form (see Appendix A) prior to completing a series of online survey forms used for data collection. If they accepted, participants were required to fill out a demographic survey form with questions related to their work environment and training experience (see Appendix B) as part of a registration process. Once the demographic survey form was submitted, and approved, participants were emailed instructions for completing a case scenario based on their selected test type of mobile, hard drive, or both. Approval to participate was based on the applicants providing verified email addresses that resided within searchable valid internet domain names. Respondents registered using emails from forensic organizations, academia and private addresses based on their job description and work setting.

As stated in the consent form, this study was not designed to be a proficiency test. Participants did not receive individual scores, nor is the answer key being published. The analysis for this study is based on the test scores of participants clustered by their self-attested categorizations collected during the registration process.

The study was open to anyone who wanted to participate. NIST checked that respondents' answers to the demographic questions matched the email address given. The email addresses were later erased. NIST elected to have open participation since this is the first study of this type. The field of digital forensics is large (see *NISTIR 8354 – Digital Investigation Techniques: A NIST Scientific Foundation Review* (initially released as a draft report for public comments [1]) that estimates a lower bound of 11,000 separate organizations conducting digital forensics. This number is far larger than the 400 crime labs in the US. Since the goal of the study was to look at the field as a whole, this open approach was selected.

3.1 Study Packet Materials

Each approved study participant was emailed instructions for completing a simulated case for either mobile phone, computer hard drive, or both as requested on their registration form. The instructions included the location for downloading a packet of test materials for the selected simulated case, comprising a disk image file containing the contents of the storage device to be examined and a worksheet. The worksheet included the case scenario and multiple-choice questions that centered on locating specific digital artifacts typical of a real investigation discovery in digital forensic casework.

The simulated cases were developed at the U.S. Secret Service (mobile case) and the National White Collar Crime Center (NW3C). These organizations provide training in digital forensics as well as regularly conducting casework and are thus familiar with developing simulated cases for training purposes. They also are familiar with the state of practice in digital forensics since many examiners are trained there.

The tests for this study were designed using a black-box model to assess the accuracy of an examiner's conclusions without considering how the conclusions were reached [3]. The tools and

methods used to answer each question were selected at the discretion of the study participants. It was estimated to take approximately two hours to complete the questions for each simulated case. At the completion of the test, the participants were directed to upload their results to an online feedback survey form that replicated the worksheet questions.

3.2 Simulated Cases

These case studies were created by digital forensic practitioners who are instructors in the field and designed to examine methods used within the field. The scenarios for the study involved a potential homicide and a potential theft of intellectual property. Results were reported as answers to a series of multiple-choice questions (see Appendix C and Appendix D). Each question was followed by a list of possible answers with an option to skip the question. The skip choice allowed an examiner to simply forgo making a choice without penalty. No conclusion could or would be drawn as to why the participant skipped a question.

4 Mobile Phone Study

Mobile device forensics is the acquisition, extraction, and analysis of digital data and digital artifacts from mobile devices such as mobile phones and tablets for investigative or legal purposes to discover and link data to events, actions, or people [4]. Forensics examiners need to understand the capabilities of mobile data extraction and the analysis tools and supported methods used in recovering data in an investigation.

According to the Scientific Working Group on Digital Evidence (SWGDE): "The level of extraction and analysis required depends on the request and the specifics of the investigation. Each acquisition level of mobile forensics has its own corresponding skill set, tool set, and risk. These levels are:

- Manual – A process that involves the manual operation of the keypad and handset display to document data present in the device's memory.
- Logical – A process that extracts individual files or objects.
- File System - A process that extracts files from a file system and may include data marked for deletion.
- Physical (Non-Invasive) – A process that provides physical acquisition of a device's data without requiring opening the case of the device.
- Physical (Invasive) – A software-based process that provides physical acquisition of a device's data requiring disassembly of the device providing access to the circuit board [5]."

As noted by Ayers et al.: "The forensic community faces a constant challenge to stay abreast of the latest technologies that may be used to expose relevant clues in an investigation [4]." To complete the mobile case study, participants needed some basic understanding of the mobile phone file structure and the skills to retrieve the data on the device. To provide answers to the questions, one needed to know the capability of forensic tools, and have a general understanding of digital forensics. A deep understanding of the Samsung Galaxy S6, its hardware and operating system details, were helpful but not required. The answers provided by a participant reflected their understanding of mobile device forensics and digital forensics in general. It is assumed that

individuals who conduct mobile forensics as part of their workplace duties would have the skill to complete the exam.

The mobile case scenario was developed by one of the authors of this report James Darnell, a professional in mobile forensics, and reviewed by a team of individuals who conduct mobile forensic investigations on a regular basis or have a broad understanding of digital forensics. The case scenario presented in the worksheet (see Appendix C) involved a potential murder. A Samsung Galaxy S6 cell phone found at the scene during evidence collection was the focal point of this scenario. A forensic image of the data stored on the phone was available for download [6] in a ZIP file format along with a PDF copy of the worksheet [7]. The questions were not designed as an exhaustive test, but its intent was to measure participants' ability to extract and interpret selected artifacts from the image of the mobile device. The test included 24 multiple choice questions (see Appendix C) based on the contents provided in the image file.

4.1 Mobile Case Questions

The multiple-choice questions in this study were designed to gain insight into the skill level of the study participants. These test questions were subjectively rated for degree of difficulty by a group of three digital forensic practitioners and classified as basic, intermediate, or advanced.

Table 2. Mobile Test Rating Definitions

Basic	These questions required some general understanding of digital forensics techniques (i.e., file hashing) and tools used for logically extracting data stored on the device, such as locating specific files.
Intermediate	These questions required an understanding of the file system structure for locating data to determine app usage, finding search terms within apps and skills to identify deleted entries.
Advanced	These questions required an understanding of the Android operating system and knowing the functions of specific apps. This included the relationship of the phone settings supported by service providers, searching across apps based on time and the storage of data for each individual app.

Eleven of the questions received the same rating by all reviewers with nine rated as basic, one rated as intermediate, and one rated as advanced. The remaining thirteen questions had mixed ratings with ten classified as basic or intermediate and three rated intermediate or advanced. The rating assigned to each of the questions is listed in column 4 of Table 3.

4.2 Summary of Mobile Case Answers

A total of seventy-seven (77) study participants returned results for the mobile case study. The responses to each question were grouped as correct, wrong, and skipped. Responses from the total population shows the following:

- Each participant logged at least one wrong answer.
- Twenty-five (25; or 32%) of the participants answered two questions incorrectly.
- Thirty (30; or 39%) participants never used the skip option.

Questions that were rated as basic listed the greatest number of correct answers. The number of correct answers decreased when questions were rated with higher degrees of difficulty. The one exception was *"There are many search terms recovered, one of which was deleted. What application was used in regard to the deleted search term?"* This question was rated basic but resulted in only nineteen (19; or 25%) correct answers, forty wrong answers (40 or 51.9%), and eighteen skipped answers (18 or 23.4 %) (see Table 3). The difficulty in answering this question could have been that finding the answer took multiple steps: the search terms needed to be recovered, the deleted term needed to be identified, and linked to the app used for deletion. This could also account for the higher skip rate on this question (see Table 3).

The question *"Regardless of how many were parsed by your tool(s), how many Wi-Fi access points did the phone log?"* was rated intermediate/advanced and received the highest number of wrong answers. Forensic tools often have the capability to extract and present data related to visited access points from the mobile device. The logged results could vary depending on the tool or if an individual manually searched for this data. No conclusions could be drawn on the tools or methods used to answer the question due to the blackbox study design.

One question received an advanced rating, *"The TOR browser was installed on the phone. When (date and time) was it last used?"* and was skipped the most. The answer could have been overlooked since the data may have listed multiple date and time entries. The key was to locate the last timestamp for when the app was used not necessarily the last entry in the log.

Table 3 lists the question and response totals for each of the categories, plus the question rating. The questions are ordered by the number of correct answers.

Table 3. Summary of Mobile Questions

Questions	Correct	Wrong	Skip	Rating
What program was used to discuss a potentially illegal transaction?	77 (100%)	0	0	Basic
What is likely the last name of the person with whom the phone's user was communicating regarding a potential trade of illegal goods?	77 (100%)	0	0	Basic
What email address is serves as the account for applications installed via the Playstore?	77 (100%)	0	0	Basic/Intermediate

Questions	Correct	Wrong	Skip	Rating
The file named 20190809-120201.jpg appears to be relevant to the case. In what city was this picture taken?	76 (98.7%)	1 (1.3%)	0	Basic
What was the phone's user researching?	75 (97.4%)	1 (1.3%)	1 (1.3%)	Basic
What did the user of the phone ask for via gmail?	75 (97.4%)	0	2 (2.6%)	Basic/Intermediate
To what time zone is the phone set?	74 (96.1%)	1 (1.3%)	2 (2.6%)	Basic
The user of the device viewed assorted posts on Instagram. One of them has a picture that includes an envelope. What country is listed on the return address area of the envelope?	72 (93.5%)	3 (3.9%)	2 (2.6%)	Basic
What file contains data to recover the phone's pattern password?	70 (90.9%)	7 (9.1%)	0	Basic
What phone number can be associated with this device?	70 (90.9%)	7 (9.1%)	0	Basic/Intermediate
The user placed a couple items in a shopping cart. What are they?	69 (89.6%)	2 (2.6%)	6 (7.8%)	Basic/Intermediate
Did the user try to map directions to where he was supposed to meet someone?	69 (89.6%)	6 (7.8%)	2 (2.6%)	Basic
What is the hash value for the partition that contains user artifacts?	65 (84.4%)	6 (7.8%)	6 (7.8%)	Basic/Intermediate
What was set as the phone's user name?	65 (84.4%)	11 (14.3%)	1 (1.3%)	Basic/Intermediate
Using the time zone settings for the location where the phone was recovered, when were searches for Orlando Springs Park (date and time) recorded on the phone?	65 (84.4%)	12 (15.6%)	0	Basic/Intermediate
What is the Bluetooth MAC address for the vehicle to which the phone was connected?	56 (72.7%)	16 (20.8%)	5 (6.5%)	Intermediate/Advance
What is the VIN number of the vehicle that connected to the phone via Bluetooth?	53 (68.8%)	17 (22.1%)	7 (9.1%)	Intermediate/Advanced
Did the phone's user download anything from Google docs?	52 (67.5%)	17 (22.1)	8 (10.4%)	Basic/Intermediate
Given your knowledge of best practices, were there any potential issues with the device extraction you discovered during your analysis?	50 (64.9%)	25 (32.5%)	2 (2.6%)	Basic/Intermediate
The TOR browser was installed on this phone. When (date and time) was it last used?	46 (59.7%)	7 (9.1%)	24 (31.2%)	Advanced

Questions	Correct	Wrong	Skip	Rating
What website was used with TOR to find a listing of deepweb markets?	43 (55.8%)	19 (24.7%)	15 (19.5%)	Intermediate
What was a search term conducted within Instagram?	39 (50.6%)	19 (24.7%)	19 (24.7%)	Basic/Intermediate
Regardless of how many were parsed by your tool(s), how many WI-FI access points did the phone log?	27 (35.1%)	48 (62.3%)	2 (2.6%)	Intermediate/Advanced
There were many search terms recovered, one of which was deleted. What application was used in regard to the deleted search terms?	19 (24.7%)	40 (51.9%)	18 (23.4%)	Basic

5 Mobile Correct Answer Distribution

From the total population of 394 study respondents registered for the mobile test, 19.5% or seventy-seven (77) mobile test-takers submitted results for analysis. This percentage of participation may be based on the voluntary nature of the study, ease of registration, and the availability of the testing materials and is expected for this type of survey which is consistent with other NIST formal surveys.

5.1 Mobile Correct Answers

The first metric used to interpret the data was based on the number of correct answers submitted by each participant. The aggregate score total of correct answers provided insight into the difficulty of the test and determined if skipped questions had an impact on overall results. The set of correct answer scores recorded for the population of mobile test-takers had a mean value = 19, standard deviation = 2.835, median = 19 and mode value = 22. The correct answer scores achieved on the mobile case study ranged from a high score of 23 down to the low score of 10. Figure 1 illustrates the number of study participants associated with the correct answer score.

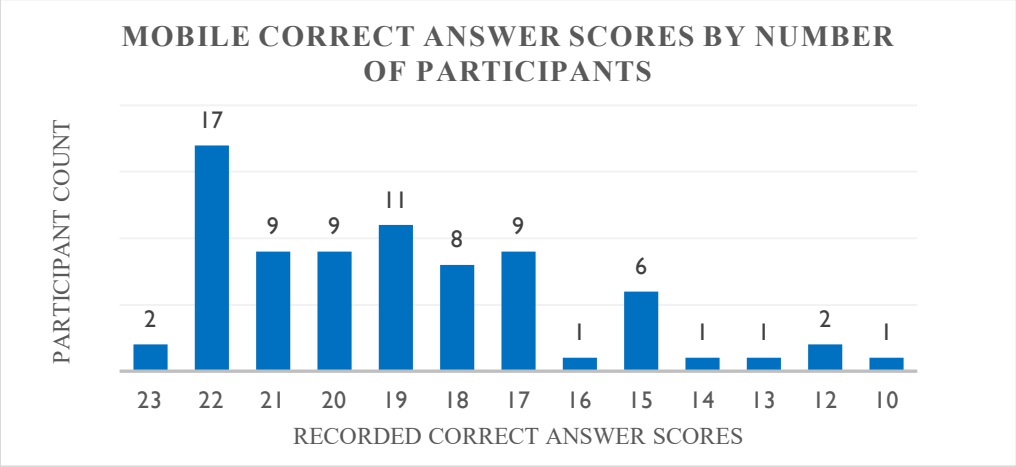

Figure 1. Correct Score Distribution

5.2 Mobile Participant Count Response

No one who took the mobile test answered all twenty-four questions correctly. When a question was missed was it due to a submitted wrong answer or the use of the skip option? The skip option reduced the need to guess an answer if the question proved challenging or time prohibited reaching a correct response. Multiple people could have the same correct answer score but record different wrong and skip results (see Figure 2).

A test score was calculated based on the set of correct answers, wrong answers, and skipped questions: test score = {correct, wrong, skip}. Figure 2 illustrates the difference in test score based on the use of the skip option, associated with the grouping of highest and lowest test scores. The use of the skip option varied for the set of test scores of 22, 21 and 12. For example, 17 participants achieved a score of 22. From this group, 15 individuals answered two questions incorrectly and two others returned one wrong and one skipped answer. The high score participants were less likely to use the skip option which could imply they were confident in the interpretation of the questions and achieving the correct result.

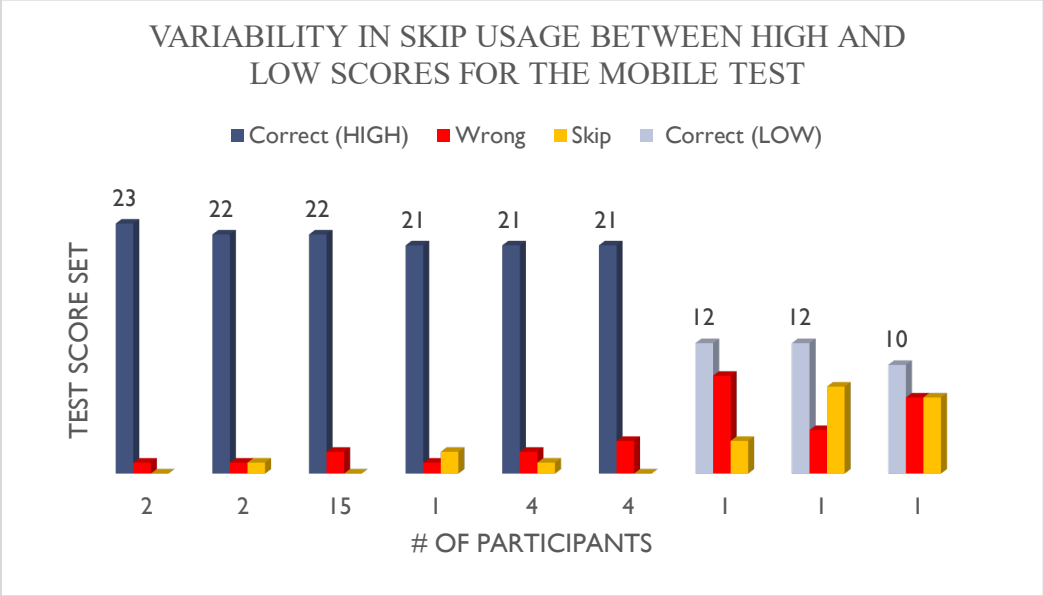

Figure 2. Mobile Test - Association of Skip Use in Highest/Lowest Score Clusters

Certain questions proved difficult for the participants who recorded the high and low scores as (see Figure 2). The following question was missed by both groups: "*There were many search terms recovered, one of which was deleted. What application was used in regard to the deleted search term?"* Of the 28 highest scorers, 8 got the answer correct, 16 returned a wrong answer and 4 skipped the question. Of the participants who scored 10 and 12, no one got the answer correct: two returned wrong answers and two skipped the question.

The three low scorers answered these two questions incorrectly: *"Using the time zone settings for the location where the phone was recovered, when were searches for Orlando Springs Park (date and time) recorded by the phone?"* and *"Regardless of how many were parsed by your tool(s), how many Wi-Fi access points did the phone log?"* Only three of the high scorers missed the first question and five missed the second question.

6 Study Demographics Question Analysis

The demographic information (see Appendix B) collected as part of the registration process was divided into two categories, workplace environment and individual work experience. The methods and techniques used in forensic investigations apply to different workplace disciplines such as law enforcement, criminal defense and prosecution, intelligence, civil, incident response, and computer security. These mandatory questions were designed to elicit insight into the workplace setting for this diverse field of practitioners.

The choices selected to these questions produced a self-attested description of the workplace, training, and skill level of the participants. The first category of questions focused on describing their workplace setting and official job duties. To study these responses, participants who completed the case studies were grouped based on their *Lab-type*. The average scores for correct, wrong, and skipped answers for each group were recorded and compared across groups.

The other workplace questions were used to determine if any differences in work setting and job duties impacted the average scores of each *Lab-type* group. The selections to these questions were counted and recorded based on the number of members in each group. These counts were used to identify general characteristics that could possibly influence the test scores.

The analysis of the training and experience questions were based on the total population of participants for both the mobile and hard drive tests. Each question had a set number of possible choices used to describe an individual's education, training classes, years of work experience and job responsibilities. The data collected for each question was categorized based on the choices selected by test participants. Each category was analyzed using two factors, the first was the number of participants and the second was the average correct, wrong, and skipped scores. The questions provided insight into an individual's skill level and how their work experience might attribute to their test results.

7 Mobile Case Study Results

The demographic information was linked to the scoring results on the mobile case study. The results from the relationship between the questions and average test scores are listed below.

7.1 Laboratory-type Comparison for Mobile

To understand the relationship between test scores and demographic workplace descriptions, the population of test-takers were broken into groups based on their laboratory type selections. Table 4 provides a summary of the sample population groups with the largest being *Federal*, with 20 members, and *Other* the smallest with 5 members. A comparison of the groups shows the average score for each based on the sum of correct test answers achieved by the participation count. Four of the groups (*Federal*, *Private*, *Local/Tribal*, *Foreign*) scored similar averages to

the grand mean of 19 for the total population. The correct answer scores recorded by the *Federal* and *Local/Tribal* groups show a similar range of correct answer scoring based on the standard deviation values. The worse performing group was *Other* with the lowest member participation, lowest average = 16.6 and highest standard deviation = 9.98.

Table 4. Mobile Laboratory Type Comparison

Lab-Type	*# of participants*	*Sum of correct answers*	*Average*	*SD*
Federal	20	383	19.2	2.25
Private	18	348	19.3	2.91
Local Tribal	14	271	19.4	2.34
State	10	186	18.6	3.50
Foreign	10	191	19.1	2.64
Other	5	83	16.6	9.98

The laboratory groups provided overall similar averages for correct, wrong, and skipped answers to the questions. Figure 3 graphs each laboratory group's average scores for correct, wrong, and skipped answers. The least successful was the group *Other* group that returned 3 of the lowest scores and missed and skipped the most questions.

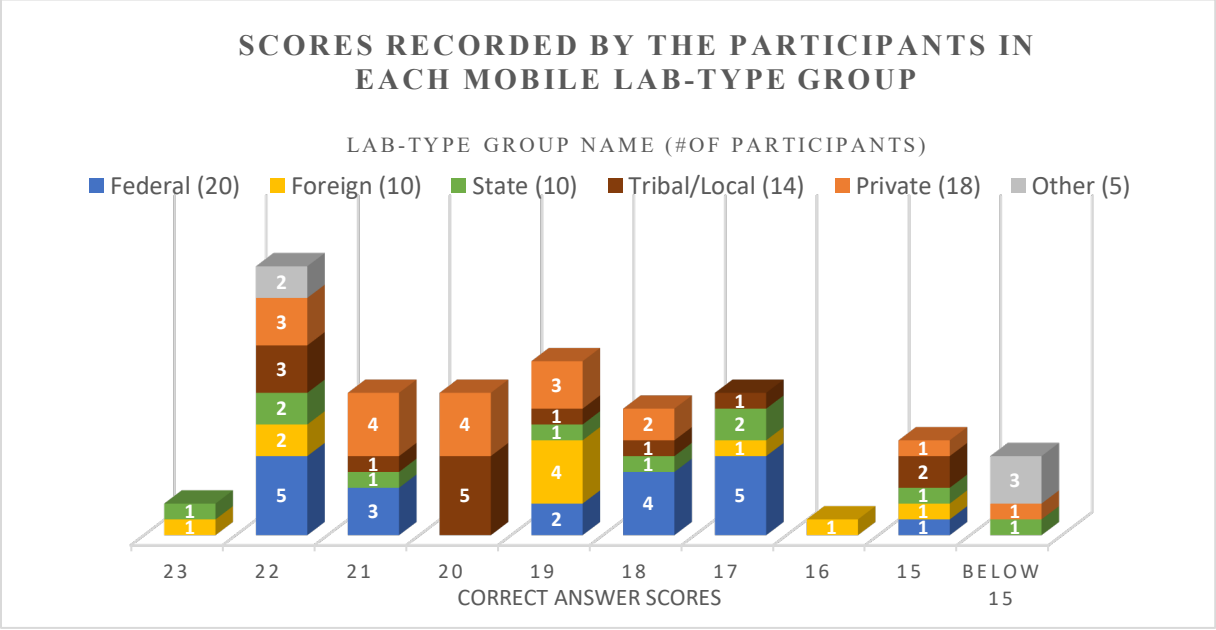

Figure 3. Average Scores by Laboratory Type for Mobile Response

The additional demographic questions provided more details about an individual's work environment. These questions were included in the study to provide a detailed view of an individual's work setting in relationship to the laboratory type. The study was open to anyone conducting digital investigations world-wide. One of the questions was where their laboratory was located. From the total population of mobile study participants 66.2% chose lab location = USA and 33.8% chose lab location = International.

Another question dealt with lab size. How many people work at your job setting? The small lab size choice was selected the most with a total count = 40. Figure 4 shows the relationship of the *Lab-type* group and the question dealing with the local laboratory size. Each bar below represents their selections.

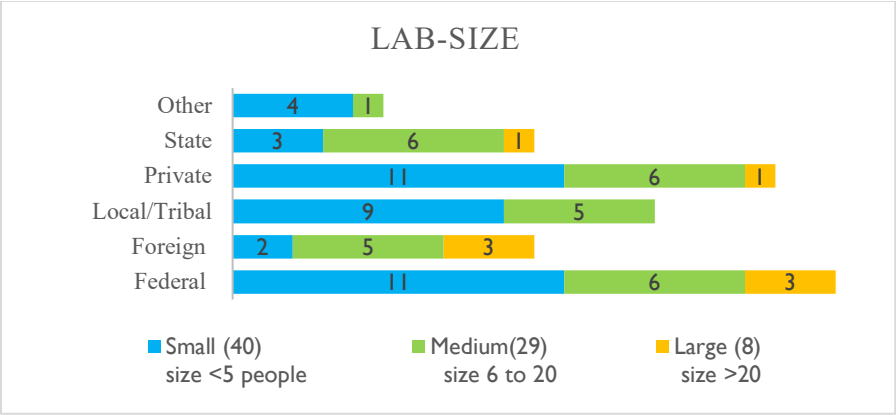

Figure 4. Mobile Response - What is the size of your local lab?

Another survey question was *What is the primary type of work?* Forty-six participants selected *Law enforcement* and one participant selected *intelligence or similar* as their work-type. Figure 5 shows the relationship between the *Lab-type* group and their primary type of work. Each bar below represents their selections.

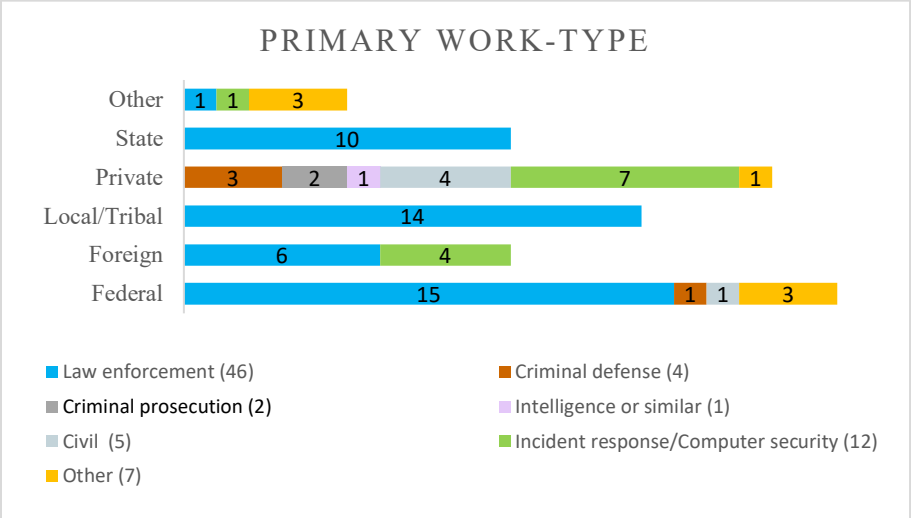

Figure 5. Mobile Response - What is your primary work-type?

"Accreditation is used to verify that laboratories have an appropriate quality management system and can properly perform certain test methods (e.g., ANSI, ASTM, and ISO test methods) and apply calibration parameters according to their scopes of accreditation[8]." One survey question queried if an individual worked in an accredited laboratory. Forty-nine participants responded '*No'* to this question. Figure 6 shows the relationship between the *Lab-type* group and the lab accredited question. Each bar below represents their selections.

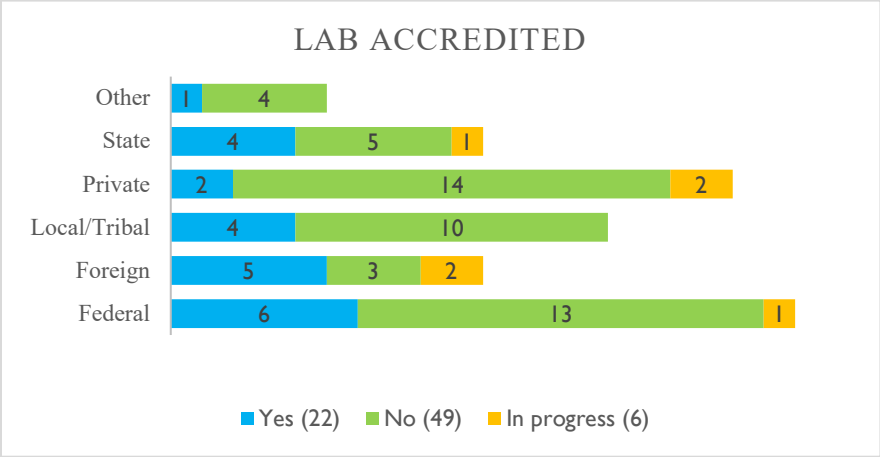

Figure 6. Mobile Response - Is your lab accredited?

7.2 Mobile Education and Experience Analysis

As part of the registration process, respondents were required to answer questions about their training, education, and work experience. These questions were designed to provide some insight into the professional development of the study participants. Did a participant's education, on the job training and work experience impact their results on the mobile test? Was there an emphasis on training since the field of digital forensics needs to evolve with the changes in technology? Individuals gain institutional knowledge over time which can strengthen their skills. Did years of service as an examiner result in better scores? The demographic questions were not exhaustive but were presented to provide some insight into the background of the participants.

The results from the demographic questions showed that 77% of the total population (77) of participants listed themselves as full time practitioners. Additional details collected from the demographic questions dealing with the education, work experience and training are provided below. Each question is listed as a sub-heading. The choices for each question were used to group participants from the total population and the results for highest correct average, lowest wrong average and the lowest skip average are listed using the italicized group name. The pie chart shows the percentage of participants for each grouping and the clustered bar chart show the average of correct, wrong, and skipped answers based on a group's selection.

7.2.1 Mobile Response - *How many years have you worked as an examiner/analyst?*

Figure 7 shows that there were more participants who indicated they had greater than 10 years of work experience. The scoring results were highest correct average = 19.77, lowest wrong average = 3.16 and lowest skip average = 1.06 was recorded by those with *More than 10 years of work experience* .

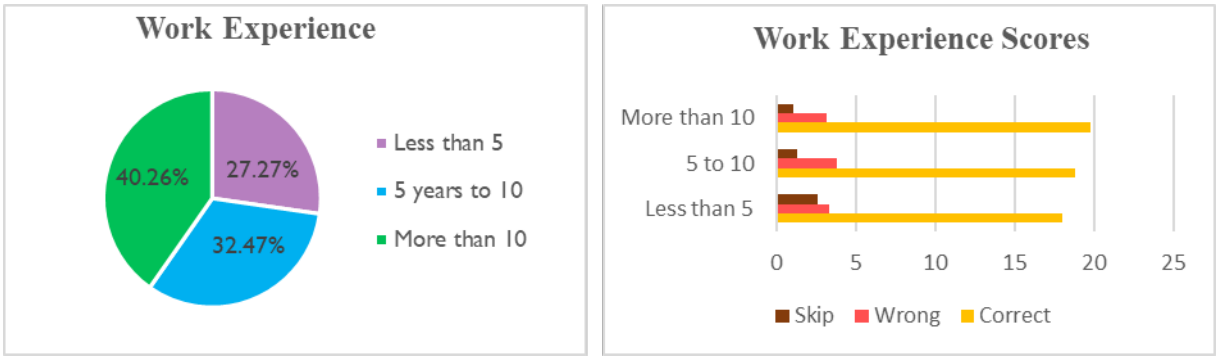

Figure 7. Mobile Response - Work Experience

7.2.2 Mobile Response - *What is your level of education?*

Most participants had a bachelors or graduate degree (Figure 8). The scoring results were highest correct average = 19.63 and lowest skip average = 1.0 among those with a *Graduate* level of education, and lowest wrong average = 2.71 recorded by those with *Associates* degrees. Only one participant indicated having a doctorate degree which is not represented on the scoring chart.

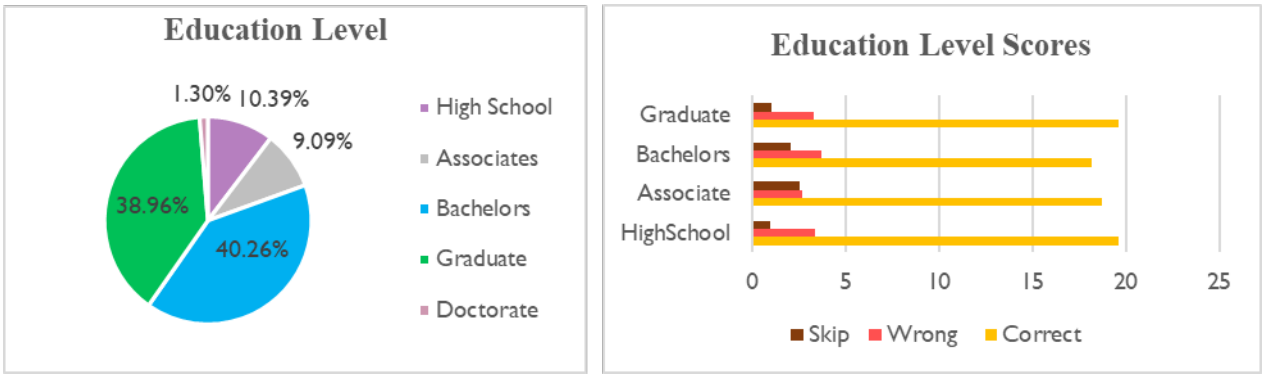

Figure 8. Mobile Response - Education Level

7.2.3 Mobile Response - *What was your focus area of educational study?*

The sample size for the groups choosing *Computer Science*, *Criminal Justice /Forensic Science* or *Other* were similar (Figure 9). The scoring results were highest correct average = 19.5 and the lowest skip average = 1.3 by those with a *Criminal Justice/Forensic Science* education, and the lowest wrong average = 3.79 by those with an *Associates* degree.

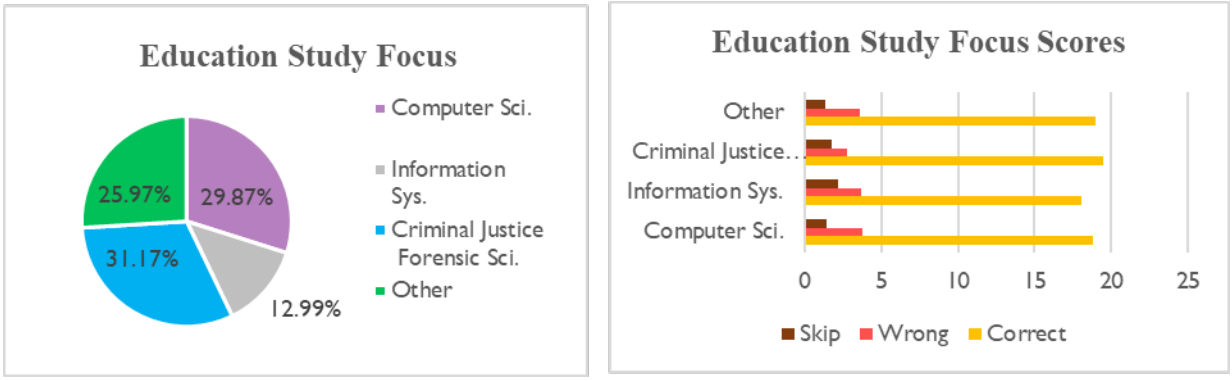

Figure 9. Mobile Response -Education Study Focus

7.3 Mobile Training Analysis

These questions were included to determine the impact of additional external lab related task and training of case study participants. Most of the participants indicated that they testified in court as part of their workplace duties. This responsibility places greater emphasis on training individuals to keep current on techniques and evolve one's skill set as technology changes. Training sources appear to be based on certification programs from tool vendors and professional associations. No one chose the independent self-study choice when linked to certification.

Another question dealt with taking proficiency testing which can be used to evaluate individual skill in discovering and analyzing digital artifacts. "In addition, these tests can be used to verify that a laboratory's forensic analytical operations are effective, and that the quality of the work is being maintained."[9] The high response to taking a proficiency test for this field of work indicates the value in testing the skills needed to effectively perform the job duties.

7.3.1 Mobile Response - *Have you ever testified in court as a digital examiner expert?*

The participants who indicated they testified in court scored higher than the those who have not testified in court (Figure 10). The scoring results were highest correct average = 20.5, lowest wrong average = 3, and lowest skip average = 0.5 by those that answered '*Yes'* to having experienced a court room setting *More than a year ago.*

Figure 10. Mobile Response - Testify in Court

7.3.2 Mobile Response - *Have you completed a certification program as a digital forensic examiner?*

Ninety-two percent (92%) of participants completed a certification program (Figure 11). Tool vendor certification programs would focus on the use of a specific tool developed for digital examinations. A professional certification would indicate that an individual demonstrated the skill and experience for conducting a digital forensic examination. The scoring results were highest correct average = 19.26, lowest wrong average = 3.30, and lowest skip average = 1.30 by those who completed a certification program from a *Professional Assoc./Agency*.

Figure 11. Mobile Response - Certification

7.3.3 Mobile Response - *Have you passed a proficiency test in the last 5 years?*

Seventy-one percent of the participants indicated taking a proficiency test (Figure 12). The scoring results with the highest correct average = 19.53 lowest wrong average = 3.29, and lowest skip average = 2.22 by those answering '*Yes'* to pass a proficiency test. There was only one participant who chose the '*No'*. *Attempted but didn't pass* and was not included in the score graph.

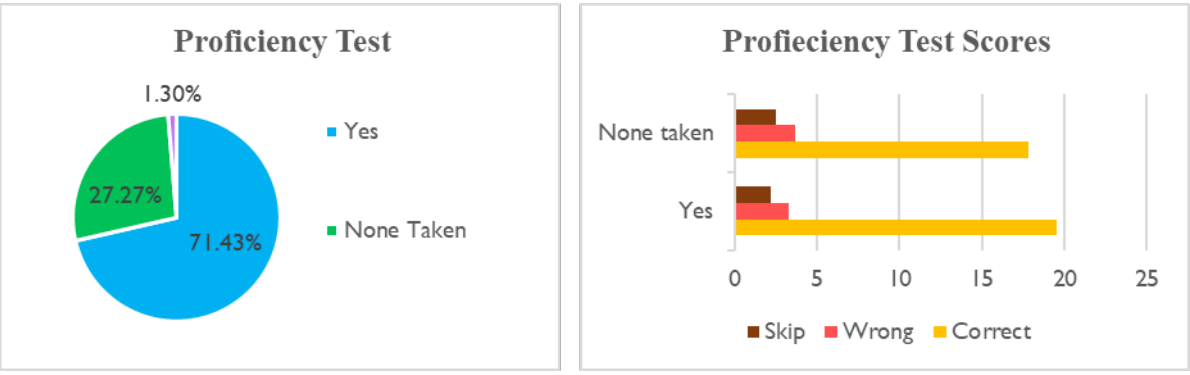

Figure 12. Mobile Response - Proficiency Test

8 Summary of the Mobile Case Study

The list below highlights the finding from the mobile case study.

- There were seventy-seven registered individuals who returned results to the mobile case study.
- Fifty-three participants who took the mobile study also took the hard drive one.
- Five participants chose lab-type as *Other*. Three of the five recorded low scores of twelve, thirteen and fourteen (see Table 4).
- There was no statistical difference in the correct average score based on grouping participants by their lab group due to the small sample sizes (see Table 4).
- Seventy-one percent of participants were not working for an accredited lab (see Figure 6).
- The grouping of participants based on work experience were similar in size. The group with more than ten years had the best scores (see Figure 7).
- Eighty percent of participants had a higher education degree and studied computer science, criminal justice, or forensic science (see Figure 8).
- Seventy-one percent of participants testified in court at some time (see Figure 10).
- Ninety-two percent of participants have completed a certification program (see Figure 11).
- Seventy-one percent of participants passed a proficiency test in the past five years (see Figure 12).
- Fifty-three percent of participants had more than forty hours of vendor-based training and more than forty hours of other external training within the past five years.

9 Hard Drive Case Study

Computer forensics utilizes methods to acquire, extract, and analyze digital data. That data can exist in two states on a computerized device as persistent and volatile. The goal is to preserve the integrity, confidentiality, and availability of the collected evidence needed for legal purposes. Persistent data is stored on a hard drive or other medium and is available when the computer is turned off. Volatile data is stored temporarily and exists in registries, cache, and random-access memory (RAM). Examiners need to knowledgeable of methods and tools available to capture both types of data [10].

"Computer forensic science differs from most traditional forensic disciplines because the evidence that is examined and the available techniques used by examiners are products of a market driven private sector. A digital examiner may receive different evidence with each case. They need to be familiar with a variety of methods and tools needed to conduct a thorough investigation based on different computer types. Some differences are:

- Operating systems which is the software responsible for executing application, scheduling tasks, and controlling attached devices. Operating systems vary among manufacturers.
- Applications may be unique based on the operating system.
- Storage methods may be unique[11]."

To complete the hard drive case study participants needed to be familiar with the E01 file format also known as the Expert Witness Format (EWF) developed by EnCase from Guidance Software. The E01 file holds various types of acquired digital evidence such as a disk image from a suspect hard drive or other external media.

The hard drive case study was developed by one of the authors of this report, Chris Atha, a digital forensic examiner, and reviewed by a team of individuals who conduct computer forensic investigations as part of their workplace duties. The case study described a scenario regarding potential stolen intellectual property that was stored on a computer running the Microsoft Windows 10 operating system. It involved an investigation by its internal computer security team of a new employee suspected of wrongdoing.

The design for this hard drive case study follows that of the black-box study for digital examiners as described in Section 3 "Study Design". The forensic image of the data for the hard drive portion of the study was available in ZIP file format [12] along with a PDF copy [13] of the worksheet. The questions were not designed as an exhaustive test, but its intent was to measure participants' ability to extract and interpret selected artifacts from the E01 image of the hard drive image. The test included 24 multiple choice questions (Appendix D) based on the contents provided in the image file.

9.1 Hard Drive Case Questions

The hard drive survey questions were rated by three individuals who work as digital examiners and have experience examining Windows 10 images. They were asked to rate the questions as basic, intermediate, and advanced based their work experience using the following definitions (see Table 5).

Table 5. Hard Drive Test Rating Definitions

Basic	These questions required an understanding of the Window 10 operating system, file naming and techniques such as file hashing. The answers could be found by importing the hard drive image into a general-purpose forensic tool.
Intermediate	These questions required an understanding of the file system and location of log and system configuration files.
Advanced	These questions required more advanced skills such as string searching based on character set encodings.

There were 24 questions in total with 13 rated basic, 7 intermediate and 1 advanced. Three of the questions received a mix rating of basic or intermediate. The 4 questions with the greatest number of wrong and skip responses were rated as intermediate and advanced.

Table 6 lists the question and response totals for each of the categories, plus the question rating. The questions are ordered by the number of correct answers.

9.2 Summary of Hard Drive Case Answers

A total of one-hundred-two (102) study participants returned results for the hard drive case study. The responses to each question were grouped as correct, wrong, and skipped. Responses from the total population shows the following:

- Everyone logged at least one wrong answer.
- Eighteen participants never used the skip option.

Questions that were rated as basic listed the greatest number of correct answers. The number of correct answers decreased when questions were rated with a higher degree of difficulty. The question *The application C:\ProgramData\SamsungApps\SamsungPortableSSD.exe was accessed. How many times was it in "focus"?* was incorrectly answered the most times. Answering this question required an understanding of the Windows Registry UserAssist key. Every GUI based program launched from the desktop is tracked in this registry key. The UserAssist data would include information on whether the application was run from the executable file or shortcut (LNK file), the GUI interaction counts, and execution time for the file. The test question was based on directly launching the executable file. Another possible explanation could be the difference in terminology used to different analysis tools. For example, the NirSoft open source utility names the "focus" artifact as count or counter depending on the utility version.

The question *Are any Korean (Hangul) word processor documents stored on "Strongwill.E01"? If so, what is modified time of the last document accessed?* was incorrectly answered more than 50% of the time. This question was rated intermediate and required knowledge of stored file types. In evaluating the image file for this question examiners needed to know about stored artifacts of the Windows Subsystem for Linux (WSL). The WSL core binaries contain the magic file, *\Users\user\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc\LocalState\rootfs\usr\lib\file\magic.mgc,* used to identify Hangul documents. Most commercial tools return this file signature as an actual document causing a false positive result.

What is the installation size of "Microsoft One Drive" in bytes? received the most skipped answer scores. This question, rated intermediate, required the ability to search the registry for information regarding installations. An application install size is often different than the size of the installed executable.

Table 6. Summary of Hard Drive Questions

Questions	Correct	Wrong	Skip	Rating
What is the MD5 hash sum of "Strongwill.e01"?	102 (100%)	0	0	Basic
What is the name of the examiner who created "Strongwill.e01"?	102 (100%)	0	0	Basic
What are the total number of sectors of the system?	102 (100%)	0	0	Basic
What version of Microsoft Windows is installed?	102 (100%)	0	0	Basic
What is the name of the primary User Account of this system?	101 (99%)	1 (1%)	0	Basic
What is the modified UTC time for "notimetosaygoodbye.docx"as listed by the metadata?	99 (97%)	2 (2%)	1 (1%)	Basic
A file may have been uploaded to HTTPS://www.virustotal.com. If this occurred, what is the SHA-256 hash sum of the uploaded file?	98 (96%)	0	4 (4%)	Intermediate
What is the installation date of the Windows Operating system? Answer in UTC.	97 (95%)	1 (1%)	4 (4%)	Basic
Locate the file named "supersizeme.exe". What is the logical file size of this file in bytes?	97 (95%)	0	5 (5%)	Basic
On what date did the first successful login utilizing RDP occur on this system?	95 (93%)	4 (4%)	3 (3%)	Intermediate
This operating system is currently set to what time zone?	93 (91%)	4 (4%)	5 (5%)	Basic
A photograph depicting a black Labrador retriever can be found on the primary partition of the system. What, if any location information can be obtained from the EXIF data associated with the image.	91 (89.2%)	10 \ 8%)	1 (1%)	Basic

Questions	Correct	Wrong	Skip	Rating
What is the filesystem of the Virtual Hard Drive located on the primary partition of the system?	90 (88.2%)	8 (7.8%)	4 (4%)	Basic
The application "SamsungPortableSSD.exe" may have been accessed through the Explorer GUI. If this event occurred, what is the volume serial number of the drive where the application run process originated from?	87 (85.3%)	7 (6.8%)	8 (7.8%)	Intermediate
What is the build number of the Microsoft Windows installation?	82 (80.4%)	18 (17.6%)	2 (2%)	Basic
Located on the primary users' desktop is a file with the name "file.exe". What is this specific file type?	79 (77.4%)	22 (21.6%)	0	Basic/Intermediate
Does it appear that any of the following instances of malware are present on the system?	72 (70.6%)	15 (14.7%)	15 (14.7%)	Intermediate
What is the volume name of the Virtual Hard Drive that exists on the system?	66 (64.7%)	35 (34.3%)	1 (1%)	Basic
What is the last time the application "BASH.exe" was run? Answer in UTC-24hr format	64 (62.7%)	15 (14.7%)	23 (22.6%)	Basic/Intermediate
The computer operator may have used the Windows terminal application to calculate the MD5 hashsum of the file. If this occurred, what is the name of the file as indicated by the Windows terminal Application?	53 (51.9%)	27 (26.5%)	22 (21.6%)	Intermediate
The computer user named "user" may have navigated to the "Downloads" directory using "Explorer". If this occurred, what is the date of the last access time?	49 (48%)	25 (24.5%)	28 (27.5%)	Basic/Intermediate
Are any Korean (Hangul) word processor documents stored on "Strongwill.E01"? If so, what is modified time of the last document accessed?	31 (30.4%)	56 (54.9%)	15 (14.7%)	Intermediate
What is the installation size of "Microsoft One Drive" in bytes?	19 (18.6%)	17 (16.7%)	66 (64.7%)	Intermediate
The application C:\ProgramData\Samsung Apps\Portable SSD\SamsungPortableSSD.exe was accessed. How many times was it in "focus"?	12 (11.8%)	81 (79.4%)	9 (8.8%)	Advanced

10 Hard Drive Correct Answer Distribution

From the total population (450) of study respondents, who registered for the hard-drive test, 23.7% or one-hundred-two (102) individuals submitted results for analysis. This percentage met our estimation for participation based on the voluntary nature of the study, ease of registration, and the availability of the testing materials. Twenty-five (25) more individuals returned hard-drive results as opposed to the mobile.

10.1 Hard Drive Correct Answers

The first metric used to interpret the data was the number of correct answers submitted by each participant. The aggregate score total of correct answers provided insight into the difficulty of the test and determined if skipped questions had an impact on overall results. The set of correct answer scores recorded for the population of hard drive test-takers had a mean value =18.451, standard deviation = 2.346, median = 19 and mode value = 19. Figure 13 illustrates the distribution of correct answers submitted by the total population of participants The correct answer scores achieved on the mobile case study ranged from a high score of 23 down to the low score of 12. Figure 13 illustrates the number of study participants associated with the correct answer scores.

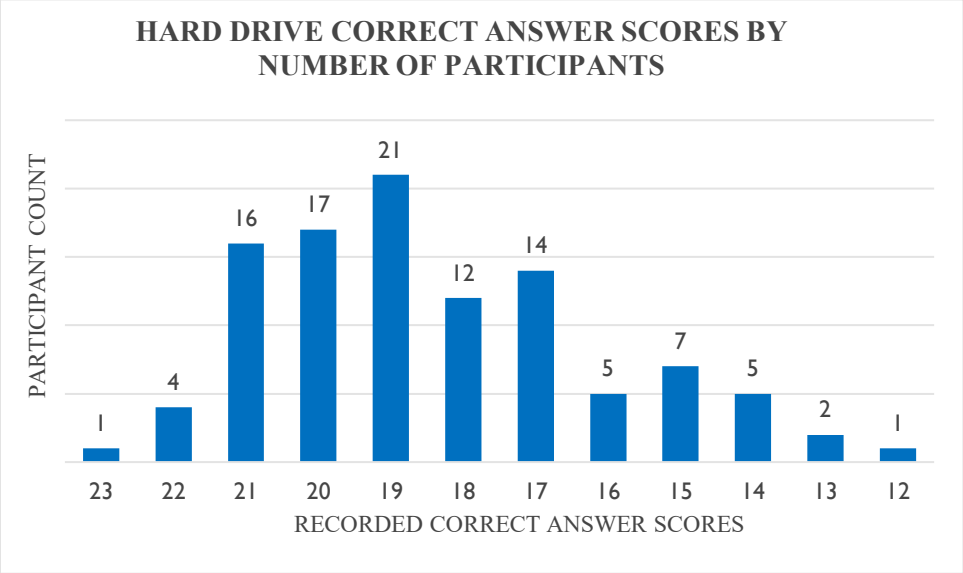

Figure 13. Hard Drive Correct Score Distribution

10.2 Hard Drive Participant Count Response

No one who took the hard drive test answered all twenty-four questions correctly. When a question was missed, was it due to a submitted wrong answer or the use of the skip option? The skip option reduced the need to guess an answer if the question proved challenging or time prohibited reaching a correct response. Multiple people could have the same correct answer score but record different wrong and skip results

A test score is calculated based on the set of correct answers, wrong answers, and skipped questions: test score = {correct, wrong skip}. Figure 14 illustrates the difference in test scoring

based on the use of the skip options associated with the high and low test scores. The use of the skip option varied for the set of test scores of 21, 14 and 13. For example, 16 participants achieved a score of 21. From that group, 12 individuals used the skip option twice, 3 individuals used the skip option once, and one person never used the skip option. The high score participants were less likely to use the skip option which could imply they were confident in the interpretation of the questions and achieving the correct result.

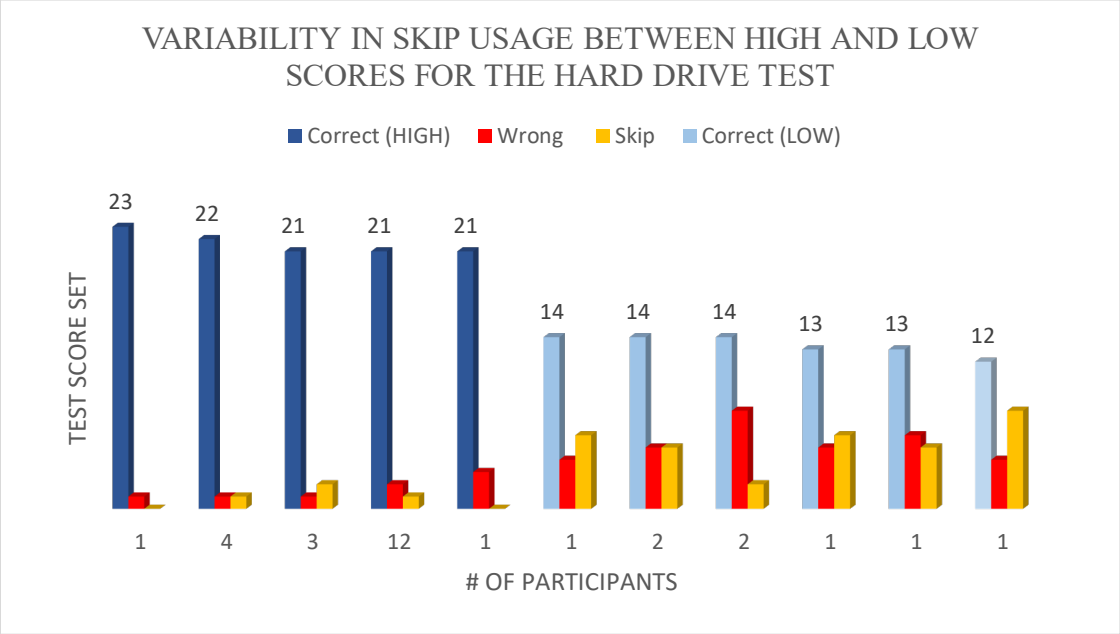

Figure 14. Hard Drive - Association of Skip Used in Highest/Lowest Score Clusters

This question had the most wrong answers recorded by participants with the high and low scores (see Figure 14): "*The application C:\ProgramData\Samsung Apps\Portable SSD\SamsungPortableSSD.exe was accessed. How many times was it in focus?"* Sixteen of the individuals with the highest scores and seven with the lowest scores gave the wrong answer. This question was skipped the most by both groups: "*What is the installation size of the Microsoft One Drive in bytes?"* Thirteen individuals with highest scores and six with the low scores used skip.

11 Hard Drive Case Study Results

The demographic information was used to evaluate any impact on the scoring results from the hard drive case study. For an overview of the demographic questions and analysis approach, see Section 6 "Study Demographic Question Analysis."

11.1 Laboratory Type Comparison for Hard Drive

To understand the relationship between test scores and demographic workplace descriptions, the population of test-testers were broken into groups based on their laboratory type selections. Table 7 provides a summary of the sample population groups with the largest being *Private*, with 36 members, and *Other* the smallest with 7 members. A comparison of the groups shows the

average score for each was based on the sum of correct test answers achieved by the participation count. Three groups (*Federal*, *Foreign, State*) scored similar averages to the grand mean of 18.451 for the total population. Two groups (*Private, Local/Tribal*) achieved the highest average correct answer score of approximately 19.

Table 7. Hard Drive Laboratory Type Comparison

Lab-Type	*# of participants*	*Sum of correct answers*	*Average*	*SD*
Private	36	683	19	1.95
Federal	23	421	18.3	2.44
Foreign	14	258	18.4	2.95
State	12	221	18.4	2.07
Local/Tribal	10	190	19	1.56
Other	7	109	15.6	2.70

The laboratory groups returned scores that were more clustered between the grouping. Figure 15 below shows similar correct answer averages from the *Foreign*, *State* and *Federal* groups. The *Local/Tribal* and *Private* groups average results were similar for all question returns of correct, wrong, and skipped. The *Other* group was the least successful with the most wrong answers.

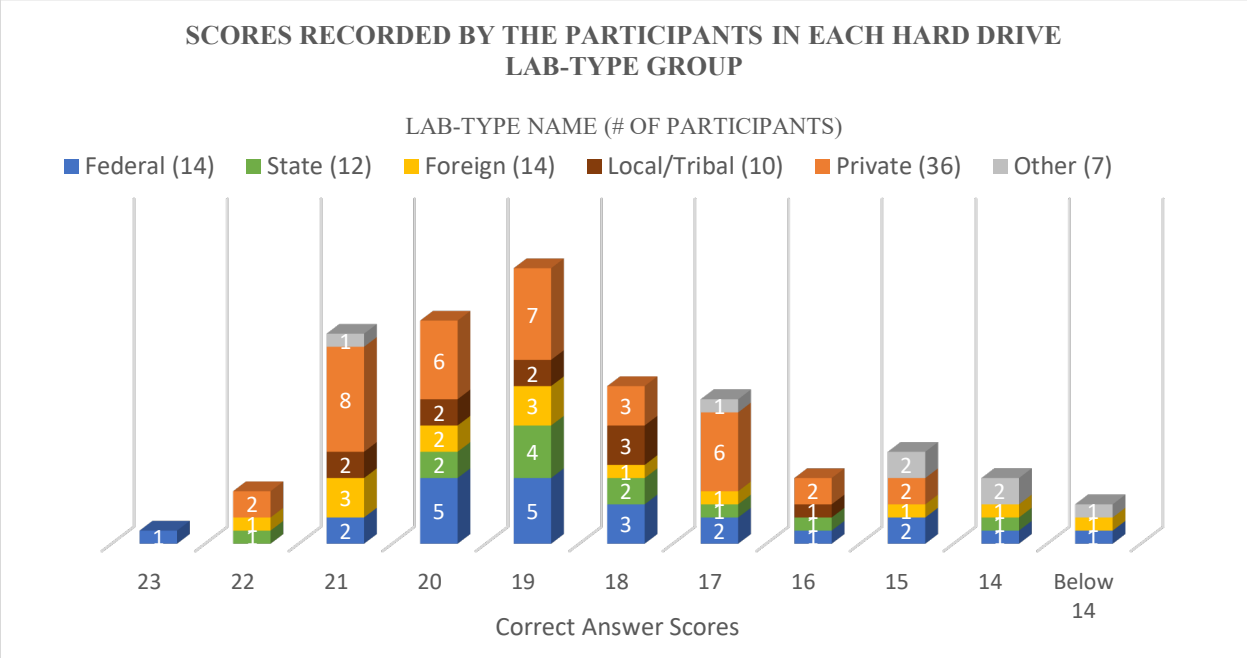

Figure 15. Average Scores by Laboratory Type for Hard Drive Response

The additional demographic questions provided more details about an individual's work environment. These questions were included in the study to provide a detailed view of an individual's work setting in relationship to the laboratory type. The study was not limited to

national participants and was open to anyone conducting digital investigations. One of the questions was where their laboratory was located. From the total population of mobile study participants 55.8% chose lab location = USA and 44.2% chose lab location = International.

Another question dealt with lab size. How many people work at your job setting? The small lab size choice was selected the most with a total count of 57. Figure 16 shows the relationship between the *Lab-type* group and the question dealing with the local laboratory size. Each bar below represents their selections.

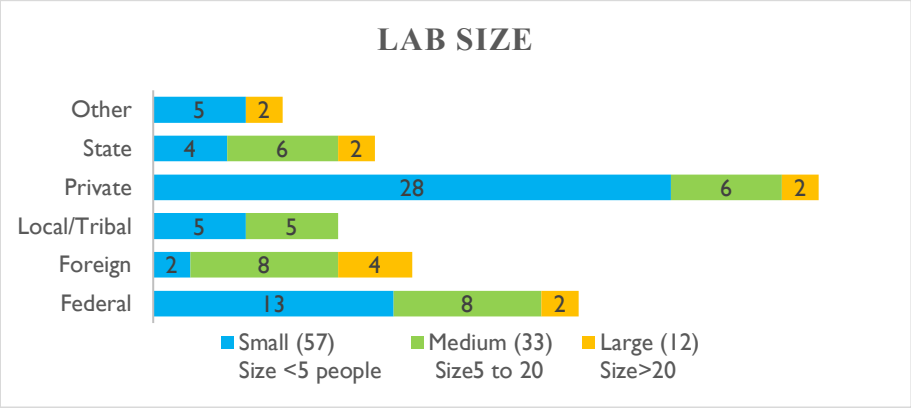

Figure 16. Hard Drive Response - What is the size of your local lab?

Another question was *What is the primary type of work?* Forty-nine participants identified *Law enforcement* as the primary work-type. Participants in the *State* and *Local/Tribal* groups exclusively chose *Law enforcement* as their primary work-type. Figure 17 shows the relationship between the *Lab-type* group members and their primary type of work. Each bar below represents their selections.

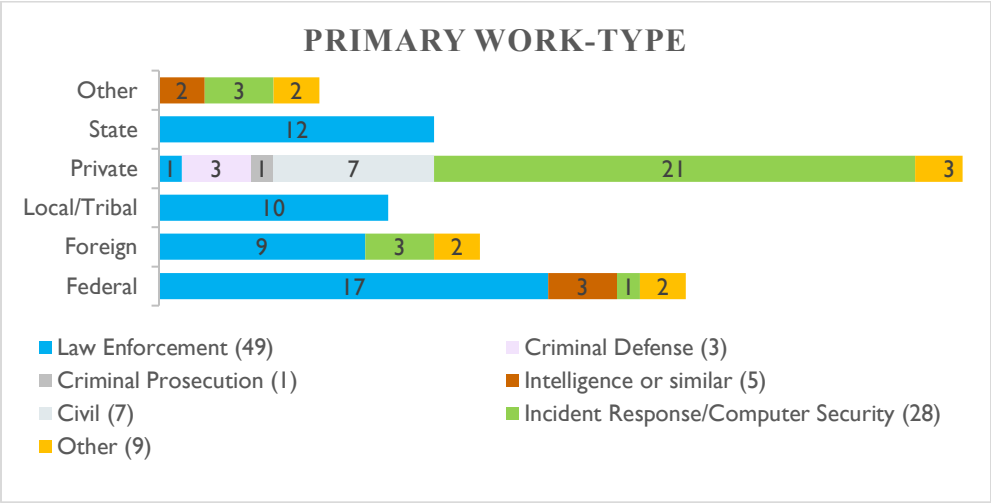

Figure 17. Hard Drive Response - What is your primary work-type?

One survey question queried if an individual worked for an accredited laboratory. Twenty-five individuals indicated they did, and 68 participants responded '*No'*. Figure 18 shows the relationship between the *Lab-type* group and the lab accredited question. Each bar below represents their selections.

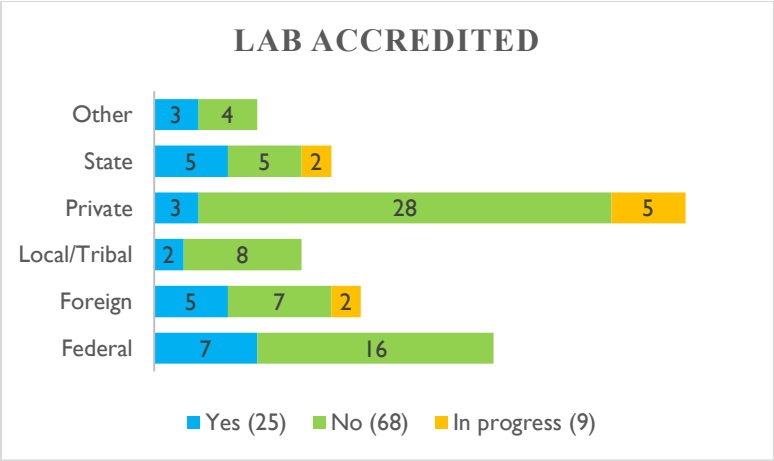

Figure 18. Hard Drive Response - Is your lab accredited?

11.2 Hard Drive Education and Experience Analysis

The demographic questions were designed to provide insight into the professional development of individuals based on years of service and educational training.

The results from the demographic questions showed that 77% of the total population (102) listed themselves as full time practitioners. Additional details collected from the demographic questions dealing with the education, work experience and training are provided below. Each question is listed as a sub-heading. The selections for each question were used to group participants from the total population and the results for highest correct average, lowest wrong average and the lowest skip average are listed using the italicized group name. The pie chart shows the percentage of participants for each grouping and the clustered bar chart show the average of correct, wrong, and skipped answers based on a group's selection.

11.2.1 Hard Drive Response - *How many years have you worked as an examiner/analyst?*

The pie chart shows the number of participants in each work experience group had similar correct average scores for work experience (Figure 19). The scoring results were highest correct average = 18.67 and lowest skip average = 1.73 was recorded by those with *More than 10 years of work experience*, and the lowest wrong average = 3.23 by those with *Less than 5 years of work experience.*

Figure 19. Hard Drive Response - Work Experience

11.2.2 Hard Drive Response - *What is your level of education?*

Most participants had a bachelors or graduate degree (Figure 20). A total of 83 participants indicated that they had a higher-level degree. The response scoring results were highest correct average = 18.79 and lowest skip average = 1.95 by among those with a *Graduate* level of education, with lowest wrong average = 2.67 recorded by those with *Associates* degrees.

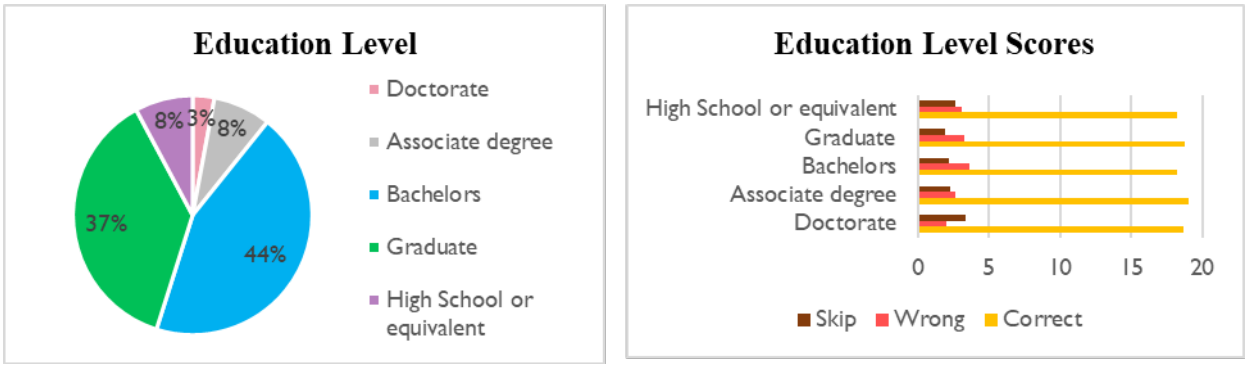

Figure 20. Hard Drive Response - Education Level

11.2.3 Hard Drive Response - *What was your focus area of educational study?*

The sample size for the groups choosing *Computer Science*, *Criminal Justice /Forensic Science* or *Other* were similar (Figure 21). The scoring results were highest correct average = 18.76 by those with a *Computer Science* education, lowest wrong average = 2.62 by *Other*, and lowest skip average = 1.67 by those who studied *Information Systems.*

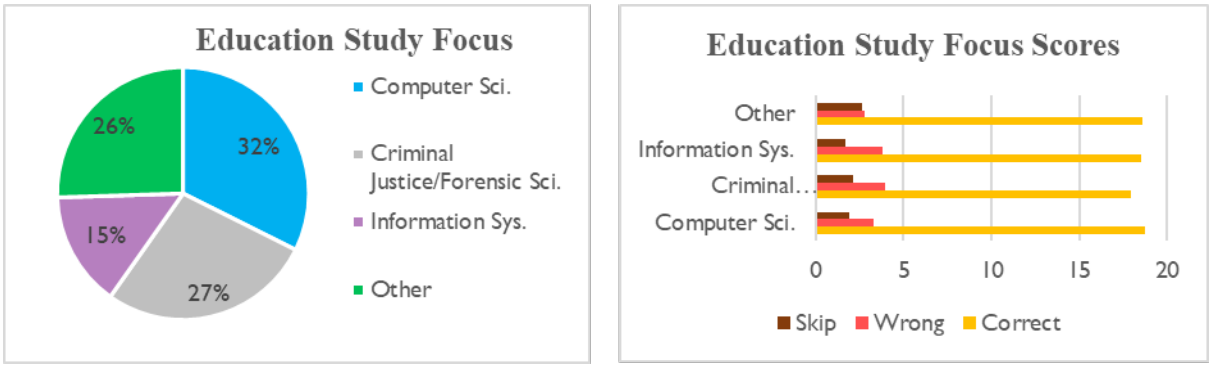

Figure 21. Hard Drive Response - Education Study Focus

11.3 Hard Drive Training Analysis

These questions were included to determine the impact of additional external lab related task and training of case study participants. Most of the participants indicated that they testified in court as part of their workplace duties. This responsibility places greater emphasis on training individuals to keep current on techniques and evolve one's skill set as technology changes. Training sources appear to be based on certification programs from tool vendors and professional associations. No one chose the independent self-study choice when linked to certification.

Another question dealt with taking proficiency testing which can be used to evaluate individual skill in discovering and analyzing digital artifacts "In addition, these tests can be used to verify that a laboratory's forensic analytical operations are effective, and that the quality of the work is being maintained[9]." The high response to taking a proficiency test for this field of work indicates the value in testing the skills needed to effectively perform the job duties.

11.3.1 Hard Drive Response - *Have you ever testified in court as a digital examiner expert?*

The participants who indicated they testified in court scored higher than those who have not testified in court (Figure 22). The scoring results were highest correct average = 18.74 and lowest skip average = 1.65 by those that answered '*Yes'* to having experienced a court room setting *(more than a year)*, with the lowest wrong average = 3.06 by those who chose '*Yes' (in past year)* to testifying in court.

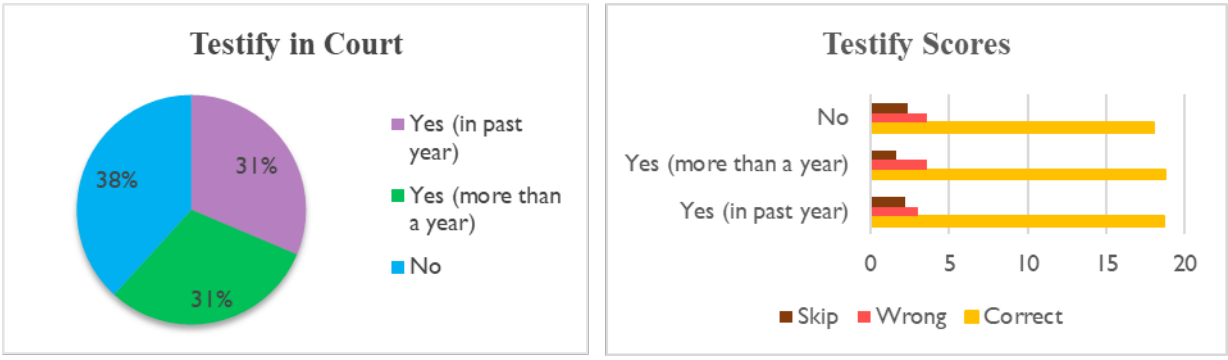

Figure 22. Hard Drive Response - Testify inCourt

11.3.2 Hard Drive Response - *Have you completed a certification program as a digital forensic examiner?*

Ninety-six percent (96%) of participants completed a certification program (Figure 23). Tool vendor certification programs would focus on the use of a specific tool developed for digital examinations. A professional certification would indicate that an individual demonstrated the skill and experience for conducting a digital forensic examination. The scoring results were highest correct average = 19.05, lowest wrong average = 3.01, and lowest skip average = 1.03 by those who completed a certification program from a *Professional assoc./agency*.

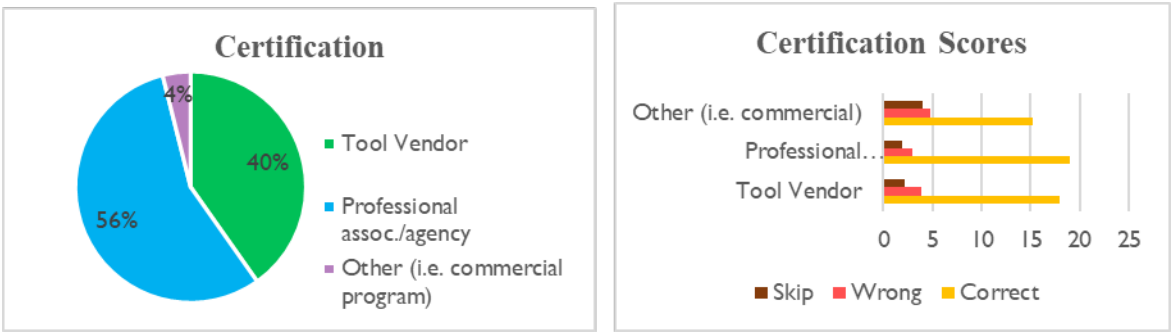

Figure 23. Hard Drive Response - Certification

11.3.3 Hard Drive Response - *Have you passed a proficiency test in the last 5 years?*

Seventy-five percent (75%) of the participants indicated taking a proficiency test (Figure 24). The scoring results were highest correct average = 18.67 lowest wrong average = 3.25, and lowest skip average = 2.07 by those who chose '*Yes'* to passing a proficiency test. There was only one participant who chose the '*No'*. *Attempted but didn't pass* option and was not included in the score bar graph.

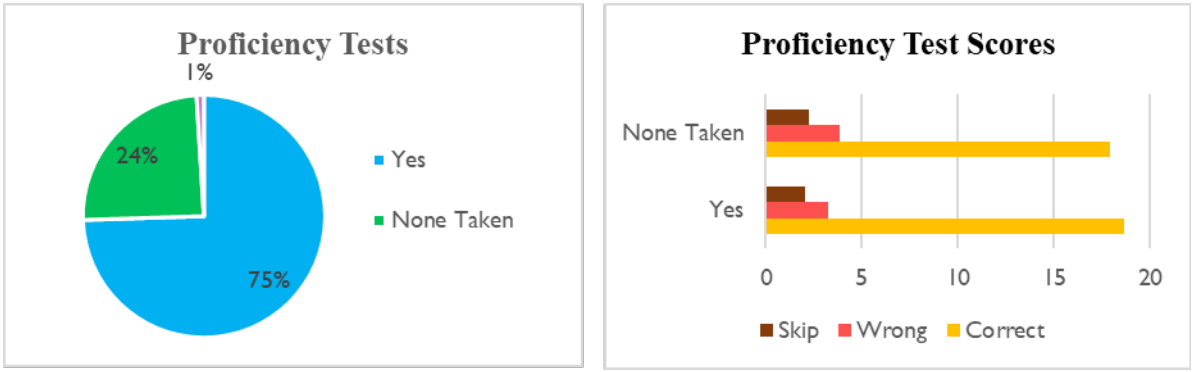

Figure 24. Hard Drive Response - Proficiency Test

12 Summary of Hard Drive Study

The list below highlights the finding from the hard drive case study.

- There were one-hundred-two registered individual who returned results to the hard drive case study
- Fifty-three participants who took the hard drive test also took the mobile one.
- Seven participants chose lab-type as *Other*. Three of the seven recorded low scores of thirteen and fourteen. The lowest score of twelve was recorded by an individual with a lab-type of *Foreign* (see Table 7).
- There was no statistical difference in the correct average score based on grouping participants by their lab group due to the small sample sizes.
- The largest laboratory group was classified as private (see Table 7).
- Seventy-six percent of participants were not working for an accredited lab (see Figure 18).
- There was an even distribution of the hard drive participants based on work experience from less than five years to more than ten years (see Figure 19).
- Eighty-four percent of participants had a higher education degree (see Figure 20).
- Sixty-two percent of participants testified in court at some time (see Figure 22).
- Ninety-six percent of participants have completed a certification program (see Figure 23).
- Seventy-five percent of participants passed a proficiency test in the past five years (see Figure 24).
- Forty-five percent of participants had more than forty hours of vendor-based training and more than forty hours of other external training within the past five years.

13 Blackbox Study Conclusion

Digital forensics is not a field that can be described by the results of one study. It is a complex discipline with many variables, and processes that are practiced in various laboratory settings.

This study was conducted to gain a generalized understanding of the field of digital forensics. Our design was narrowed and focused using an online canvas survey approach to include practitioners from various forensic disciplines in addition to examiners with strict law enforcement duties. The study's use of mobile and hard drive mock test case materials helped identify performance outcomes of the examiners that participated in this activity. The canvas survey questions were written in a format that allowed for grouping participants based on their workplace and training experience. We evaluated the results from the case studies in relation to the participants' survey responses to try and identify common attributes that impacted the outcomes achieved on the tests. The results from this comparison were not strong enough to draw definitive conclusions for the digital forensic field.

Summary Key Takeaways

Despite the limitations of the study, two key takeaways about the state of the digital evidence discipline emerged:

- Digital forensics examiners showed that they can answer difficult questions related to the analysis of mobile phones and personal computers. Questions ranged from basic, such as identifying who the user of the phone had contacted, to advanced questions that related to the use of the TOR browser.
- The response to the study underscored the size, variety, and complexity of the field. The study received responses from examiners working in international, federal, state, local government, and private labs whose major work included law enforcement, defense, intelligence, and incident response/computer security. There were also responses from people outside of these areas.

13.1 Recruitment Key Takeaways

This is the first black box study of digital forensic examiners and was limited in scope. We noted the following limitations, but there may be more. We do not know if these participants are representative of the digital forensic community as a whole.

- The recruitment for study participants was curtailed by the cancellation of in-person events during the COVID-19 pandemic. Face to face interaction is an important part of outreach.
- Many digital evidence labs saw increased workloads due to the increase in computer crime associated with the pandemic.
- Some examiners and labs did not receive permission from their organization or chose not to participate based on concerns about how the study would be used.
- We chose to allow anyone to participate. Our methodology for excluding non-digital forensic examiners or for verifying their demographic information was limited to checking that they had a valid email address at an organization. We could not verify the

professional status of every test participant. The questionnaire response and acknowledgement were the only data points at our disposal.
- While we received many responses to the study (511) with a 50% split between US and international labs, this number is very low compared to our estimate of a lower bound of 11,000 separate organizations conducting digital forensics (*NISTIR 8354 – Digital Investigation Techniques: A NIST Scientific Foundation Review* (initially released as a draft report for public comments) [1]).

13.1.1 *Recruitment Lessons Learned*

- Our test respondents ranged from those who identified themselves as independent, part-time examiners to those individuals who work for law-enforcement agencies on a full-time basis. This broad scope of self-attested representation was reflected in our survey results. Future studies should provide an enhanced data collection methodology that controls user input that is specialized and targeted to specific forensics disciplines for improving community outcomes. A more targeted recruitment process could be implemented by contacting specific labs to participate in a study. This would help in verifying an individual's professional status.
- Gathering demographic information from examiners was valuable in understanding this diverse field. In this study, we generalized the selection options to the questions. For example, the training questions were altered from specific training programs (using real name and locations) to the general category of vendor and agency-based training programs. We felt we could not provide a complete list of training programs based on the scope of our study. Future work could use this same approach but format the questions in a manner that refines the data collection in a targeted manner.

13.2 Key Takeaways using Case Scenarios

- The study is not representative of casework.
    - We used a multiple-choice answer key format to make scoring easier, but this required questions with multiple plausible answers that could not be reverse engineered by searching for the terms. This made the test more artificial than actual casework.
    - We used two scenarios that could support basic, intermediate, and advanced questions. This made the scenarios more difficult than most casework. Digital forensics is a complex field containing multiple sub-disciplines. We limited the study to only two scenarios; this does not address the depth nor the breadth of the field.

13.2.1 *Lessons Learned using Case Scenarios*

- While the study is not an exhaustive representation of the field, it does provide a start for understanding digital forensics and provides a framework for additional studies to gain further insights for strengthening the digital forensic field.
- The case scenarios were a key part of the study. There was a strong interest from study respondents to acquire these materials for self-study. Research could focus on identifying

gaps in testing materials for different disciplines and developing publicly available materials that best meet the community needs.

13.3 Key Takeaways on Results

- Quality control techniques and attributes normally associated with improved performance did not seem to make a difference in this study. The only attribute that correlated with improved score performance was the completion of a certification program (see Figure 11, Figure 23).
- Most of the answers to the basic question for both test types were correct. These questions focused on the skills and knowledge needed for discovering files by applying forensic techniques. Knowing how to apply file discovery techniques in this instance could be transferable to other file types. This implies that basic operations, such as finding text messages, call logs, and child sexual exploitation material are being done correctly in the field.
- Digital forensic examinations can be very complex. Given that no respondents correctly answered all the questions, there is a need to further study what types of analysis are most difficult and whether this affects casework or is an artifact of the set up for this particular study.

13.3.1 *Lessons Learned on Results*

The overall performance of the participants covered a wider scoring range than expected (see Figure1, Figure 13). Even with the ability to skip questions, participants regularly gave incorrect answers indicating that they guessed, misinterpreted the question, or lacked skills to know the correct answer.Given the low number of participants and other limitations of the study, it is not possible to correlate the results of the study with the field as a whole. It does suggest that a more rigorous and focused future study would be valuable.

Next Steps

Some possible next steps are:

- A series of targeted assessments that address a limited number of skills, or types of labs, or examiners. Based on the results of the study reported here, significant lead time would be needed for such future studies.

- A study of why the demographics were not correlated with performance. We note that the OSAC DE Subcommittee [14] is performing a study of quality control in digital forensics labs. Their study consists of a series of interviews of lab managers and customers addressing the usefulness of various quality measures in terms of timely and accurate outcomes that assist in investigative processes and impact court proceedings.

References

[1] Lyle, James R., et al., "NISTIR 8354-Draft Digital Investigation Techniques: A NIST Scientific Foundation Review"; Currently in press and not yet available on line.

[2] Butler, John M., et al., "NISTIR 8225, NIST Scientific Foundation Reviews", December 2020; available at https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8225.pdf (accessed December 7, 2021).

[3] OSAC Technical Series 0004 Human Factors in Validation and Performance Testing of Forensic Science; March 2020; available at https://www.nist.gov/system/files/documents/2020/05/22/OSACTechSeriesPub_HF%20in%20Validation%20and%20Performance%20Testing%20of%20Forensic%20Science_March2020.pdf (accessed December 7, 2021).

[4] Ayers, R., et al., "Guidelines on Mobile Device Forensics", NIST Special Publication 800-101, 2014; available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf (accessed December 7, 2021).

[5] Scientific Working Group for Digital Forensics SWGDE Best Practices for Mobile Device Evidence Collection & Preservation Handling and Acquisition_v1.2 2020-09-17; available at https://www.swgde.org/documents/published (accessed December 7, 2021).

[6] NIST Mobile Case Scenario Image; available at https://s3.amazonaws.com/docs.nsrl.nist.gov/de_blackbox_study/mobile_test/UFED_Samsung_GSM_SM-G920A_Galaxy_S6_2019_08_13_(001).zip, SHA1=43a7a27638020e2593d540186edc0e5f398a608b, December 2020 (accessed December 7, 2021).

[7] NIST Mobile Case Scenario Worksheet; available at https://s3.amazonaws.com/docs.nsrl.nist.gov/de_blackbox_study/mobile_test/nist_mobile_test_questions.pdf, SHA1=c908963e6460205decd49be46696fd6f96573d6b, December 2020 (accessed December 7, 2021).

[8] NIST National Voluntary Laboratory Accreditation Program; available at https://www.nist.gov/accreditation (accessed December 7, 2021).

[9] Scientific Working Group for Forensic Anthropology (SWGANTH) Proficiency Testing Issue date: 08/02/2012 Revision:0; available at https://www.nist.gov/system/files/documents/2018/03/13/swganth_proficiency_testing.pdf (accessed December 7, 2021).

[10] Computer Forensics; US-CERT; available at https://us-cert.cisa.gov/sites/default/files/publications/forensics.pdf (accessed December 7, 2021).

[11] Noblett, Michael G, et.al, *Forensic Science Communication*, October 2000 – Volume2 – Number 4; available at https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm (accessed December 7, 2021).

[12] NIST Hard Drive Case Scenario Image File, hard drive image; available at https://s3.amazonaws.com/docs.nsrl.nist.gov/de_blackbox_study/hard_drive_test/HardDrive-002.zip, December 2020 (accessed December 7, 2021).

[13] NIST Hard Drive Case Scenario Worksheet; available at https://s3.amazonaws.com/docs.nsrl.nist.gov/de_blackbox_study/hard_drive_test/NIST_HardDriveQuestions_V2.pdf (accessed December 7, 2021).

[14] OSAC DE Subcommittee; available at https://www.nist.gov/osac/digitalmultimedia-scientific-area-committee (accessed December 7, 2021).

Appendix A: Study Consent Form

The consent form used to register participants for the sudy.

NIST Blackbox Study for Digital Examiners

NIST is conducting a blackbox study to evaluate the accuracy and reproducibility of digital discovery by digital examiners. Participation is open to digital examiners who conduct hard drive or mobile examinations as part of their official duties.

Listed is a brief summary of key information to describe the research study you are being invited to participate in. You will find more detailed information explained later in the informed consent section.

• Voluntary Consent: You may be eligible to participate in this research study. Taking part in this study is completely voluntary and you can withdraw at any time.
• Purpose: This survey will assist the forensic community in assessing the accuracy, reproducibility and repeatability of conclusions reached by digital examiners as part of their digital discovery process.
• Duration: We anticipate that your participation in this research study will take approximately 2 hours to complete.
• List of Procedures and Activities: You will be asked to complete an online survey about your current work place environment (i.e. lab type, number of examiners, examination types) and background information (i.e. education, training) followed by an off-line simulated case analysis. The simulated cases are designed for computer hard drive and/or a mobile phone analysis. Your answers to this analysis will be tallied through our NIST online survey form.
• Risks or Discomforts; Reasonable, expected benefits: We do not anticipate any risks with your participation in this study. It will require some of your time to complete the study analysis and survey forms. This study is important to the forensic community because it may well increase continual trust in the current progression of digital analysis methods.

NOTICE
OMB Control #0693-0033
Expiration Date: 07/31/2022

This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be 10 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the National Institute of Standards and Technology. Attention: Barbara Guttman (barbara.guttman@nist.gov).

NEXT

Blackbox Survey for Digital Examiners Informed Consent Form

Principal Investigator: Barbara Guttman
Study Title: Blackbox Study for Digital Examiners
Study Site(s): National Institute of Standards and Technology, Gaithersburg Md 20899

Introduction: This document in its entirety is called an informed consent form. Please read this information carefully and take your time making your decision. Ask the researcher or study staff to discuss this consent form with you, please ask him/her to explain any words or information you do not clearly understand. The nature of the study, risks, inconveniences, discomforts, and other important information about the study are provided. You are being asked to take part in a research study that we intend to be solely voluntary by application. Participates interested in this research include only people who choose to take part in this study.

Purpose of the study: The purpose of this study is to identify and evaluate the body of scientific evidence that underlies the methods and practices used when conducting digital forensic examinations.

Why are you being asked to take part?
This study is targeting individuals who conduct digital examinations on computer hard drives or mobile phones as part of their workplace duties. The participation pool is broad due to this discipline. You may be conducting digital exams for the purposes of law enforcement, criminal defense, intelligence, corporate security, incident response and other reasons.

Study Procedures: The initial step in this study is for participants to fill-out a survey with workplace and background questions. We estimate this step to take 10 minutes to complete. We are seeking information on your workplace environment such as the lab type, size location and accredited status. This is followed by a section with questions on the participants background like years of work experience, education level, educational study focus, training, testing and certifications.

At the end of the survey, you will be asked to provide your work email address. We will email you with a registration id and instructions for downloading the images needed for conducting an analysis on a simulated case for a hard drive or mobile device. Once you have completed the off-line examination, you will need to return your answers to this study through another survey form. Your responses to this portion of the study will be linked to your registration id. It is estimated to take about 2 hours per image to perform this analysis.

Total Number of Participants: About 150 individuals will take part in this study by NIST.

Alternatives / Voluntary Participation / Withdrawal: You do not have to participate in this research study. You should only take part in this study if you want to volunteer. You should not feel that there is any pressure to take part in the study. You are free to participate in this research or withdraw at any time. There will be no penalty or loss of benefits you are entitled to receive if you stop taking part in this study. If at any time you choose to withdraw, all data you provide during the data collection phase will be deleted and will not be included in the final study analysis. You can choose to enroll in this study by completing the first survey (work type and background questions) and not complete the off-line simulation test without penalty.

Risks or Discomfort: This research is considered minimal risk. That means that the risks associated with this study are the same as what you face every day. There are no known additional risks to those who take part in this study. There is also a very small risk that someone who is not authorized could get access to the data we have stored about you. However, we describe how we will protect your privacy and confidentiality in a later section of this consent form.

Benefits: You will receive no benefit(s) by participating in this research study.
Compensation: You will receive no payment or other compensation for taking part in this study.
Costs: It will not cost you anything to take part in the study.

Privacy and Confidentiality: We will keep your study records private and confidential. The test results will be confidential. Respondents will not receive test scores, nor will we publish the answer key. The only direct identifier for this study is your work email address. We will use this data point to verify that you work in the type of lab you described. Once the data collection for the study is complete we will delete your email and the system used to manage the registration ids will be deleted. All answers to the questions provided in this study will not be able to be associated with either an individual or a specific lab.

Certain people may need to see your study records. Anyone who looks at your records must keep them confidential. These individuals include Barbara Guttman, the Principal Investigator and the research team. Your identity will be protected to the extent permitted by law, including the Freedom of Information Act. We may publish what we learn from this study. If we do, we will not include your name. We will not publish anything that would let people know who you are. Total confidentiality cannot be guaranteed, since all security measures have vulnerabilities and may be compromised.

Future use of research data: We will not retain your information for future research after this study.

Relevant research results: The overall results and findings from this study will not be shared with you. Respondents will not receive test scores results nor will the answer key be published. We will publish a report of our findings at the end of this study.

If you have any questions, concerns or complaints about this study, call Barbara Guttman at (301) 975-4207.
If you have questions about your rights as a participant in this study, or have complaints, concerns or issues you want to discuss with someone outside the research team, call the Human Subjects Protection Office at (301) 975-5445.

I freely give my consent to take part in this study. I understand that this is an online consent form and that by choosing yes on this form means that I am agreeing to take part in the research. Do you consent to participate in this study? *

- ◯ Yes
- ◯ No

BACK NEXT

Appendix B: Demographic Survey

The registration questions used in the NIST Blackbox Study for digital examiners.

Workplace and Work type

What is the size of your local lab?

Small (less than 5 people)
Medium (6 to 20 people)
Large (more than 20)

What is the size of your lab system?

Medium (less than 20)
Large (more than 20)
Not applicable

What is your lab type?

Federal
State
Local/Tribal
Foreign (non-US) Government
Private/Independent
Other

What is the primary type of work?

Law enforcement
Criminal defense
Criminal prosecution
Intelligence or similar
Civil
Incident response/computer security
Other

Is your lab accredited?

Yes
No
In progress

Lab location?

USA
International

Training and Experience

How many years have you worked as an examiner/analyst?

Less than 5 years
5 years to 10 years
More than 10 years

What is your level of education?

High School (or equivalent)
Associate degree
Bachelors
Graduate (Masters)
Doctorate

What was your focus area of educational study?

Computer Science
Information Systems
Criminal justice or forensic science
Other

Are you a full-time examiner?

Yes
No

Have you ever testified in court as a digital examiner expert?

Yes (with in the past year)
Yes (more than a year ago)
No

How much training as an examiner have you acquired?

Tool vendor based with over 40 hours in last 5 years
Tool vendor based with less than 40 hours in last 5 years
Other external training over 40 hours in last 5 years
Other external training under 40 hours in last 5 years

Have you completed a certification program as a digital forensic examiner?

Tool vendor certification
Professional association/agency or other non-vendor certification
Other
Independent self study

Have you passed a proficiency test in the last 5 years?

Yes
No. I attempted but did not pass
None taken

Appendix C: Mobile Case Scenario

The simulated case study scenario and questions used in the mobile testing part of NIST black box study for digital examiners.

Scenario: On 8/13/19, on a report of a dead body, police responded to the Rock Springs area in Florida. At that location, police recovered the body of an apparent homicide victim. Included among items seized that day was a powered off Samsung S6 G920a phone. The police placed the phone in a faraday bag and submitted it for an examination.

Continuing 8/13/19, an examiner charged the battery of the phone and completed a physical extraction of its contents.

You are to complete an analysis on the extracted data. You are to use all tools you deem appropriate. You have full search authority to find anything that, among other items of investigative interest, identifies the phone's user, with whom the phone's user was communicating, and any potential illegal activity with which the phone's user was involved.

1. What is the hash value for the partition that contains user artifacts?

A. AEB075D6ED6A9FB005FEF8DB6B712E12D0131361F0583DE746494A19377 FB102
B. 7B5EF155A6E07AD4D5C67FAA65F715552CDB4D5CDA2E8C45B8104E0F63A 84EB4
C. 7A8797B97987D7987EE98787A798F97877632220D262514E97754FB986355DC79
D. 9ED5F6783B2F58ADAEC753CD08B1A01F421DC0727DABFE4250AE45E9F93D736 D
E. Skip

2. What was set as the phone's user name?

A. UserID1
B. Jdtest
C. Jd tester
D. Jd.cvult
E. Skip

3. What program was used to discuss a potentially illegal transaction?

A. Whatsapp
B. Gmail
C. Burner
D. KiK
E. Skip

4. To what time zone is the phone set?

A. America/Chicago
B. America/Los Angeles
C. America/Goose_Bay

D. America/New_York
E. Skip

5. The file named 20190809_120201.jpg appears to be relevant to the case. In what city was this picture taken?

A. Orlando
B. Dallas
C. Miami
D. Tulsa
E. Skip

6. Regardless of how many were parsed by your tool(s), how many Wi-Fi access points did the phone log?

A. 8
B. 6
C. 2
D. 4
E. Skip

7. What file contains data to recover the phone's pattern password?

A. Gesture.key
B. PasswordKeeper_ATT.apk
C. com.google.android.gms.auth.confirm.CredentialsState
D. accounts.db
E. Skip

8. The TOR browser was installed on this phone. When (date and time) was it last used?

A. 8/9/2019, 2:55 PM
B. 8/12/2019, 6:55 PM
C. 8/12/2019, 10:55 PM
D. 8/9/2019, 6:55 PM
E. Skip

9. What phone number can be associated with this device?

A. (918)236-0870
B. (202)538-9455
C. (321)257-9720
D. (571)386-1265
E. Skip

10. What is likely the last name of the person with whom the phone's user was communicating regarding a potential trade of illegal goods?

A. Aarseth
B. Ohlin
C. Vincent

D. Eikemo
E. Skip

11.What was the phone's user researching?
A. Hitman for hire
B. Airfare
C. Credit card fraud
D. Drug and firearm prices
E. Skip

12.What email address serves as the account for applications installed via the Play store?
A. olve.eikemo.777@gmail.com
B. jd.cvult@gmail.com
C. 12025389455@s.whatsapp.net
D. 19182360870@s.whatsapp.net
E. Skip

13.Did the user try to map directions to where he was supposed to meet someone?
A. Yes
B. No
C. Skip

14.What website was used with TOR to find a listing of deepweb markets?
A. www.therecoveryvillage.com
B. www.deepwebsiteslinks.com
C. www.silkroad.com
D. www.whoishostingthis.com
E. Skip

15.What is the VIN number of the vehicle that connected to the phone via Bluetooth?
A. 1B3EEGHKDK9393980
B. 1C4RAHAB7HC693271
C. 1BDJDW737DH282828
D. None of the above
E. Skip

16.What is the Bluetooth MAC address for the vehicle to which the phone was connected?
A. 00:54:AF:68:D4:F4
B. 00:25:DE:33:D4:A1
C. 9C:B6:D0:FD:8C:E0
D. None of the above
E. Skip

17.There were many search terms recovered, one of which was deleted. What application was used in regard to the deleted search term?

A. Chrome
B. TOR
C. Instagram
D. Play Store
E. Skip

18.The user of the device viewed assorted posts on Instagram. One of them has a picture that includes an envelope. What country is listed on the return address area of the envelope?

A America
B Norway
C. Sweden
D. Russia
E. Skip

19.What was a search term conducted within Instagram?

A. burzum
B. ar15
C. mayhemband
D. All of the above
E. Skip

20.What did the user of the phone ask for via gmail?

A. Location of meeting
B. WiFi password
C. Olve's whats app number
D. Extension on loan
E. Skip

21.The user placed a couple items in a shopping cart. What are they?

A. Records
B. Firearms
C. Drugs
D. All of the above
E. Skip

22.Using the time zone settings for the location where the phone was recovered, when were searches for Orlando Springs Park (date and time) recorded by the phone?

A. 8/10/2019 12:35 PM
B. 8/12/2019 5:30 PM
C. 8/10/2019 4:35 PM
D. Both A and B
E. Skip

23.Did the phone's user download anything from Google docs?

A Yes
B No
C Skip

24.Given your knowledge of best practices, were there any potential issues with the device extraction you discovered during your analysis?

A. Yes
B. No
C. Skip

Appendix D: Hard Drive Case Scenario

The simulated case study scenario and questions used in the hard drive testing part of NIST black box study for digital examiners.

Scenario: Upon hiring a new software developer, a company issued a Windows 10 based laptop to a new employee. Within four weeks of starting the new role, the employee was observed writing a social media post about purchasing a new highend electric car that was inconsistent with their salary. In addition, the employee called in sick after just a few days on the job. The internal security team tasked with monitoring the social media accounts of their employees observed what appeared to be an attempt to sell intellectual property to someone within the Asian Pacific region. The security team retrieved the laptop and acquired an image of the disk drive to conduct a search for digital evidence.

Examine the resulting E01 File (Strongwill.E01x) and answer the questions below.

1. **What is the MD5 hash sum of "Strongwill.e01"?**
   A: b5ae724f3c01a1daf94be64aa2cde231
   B: b89989fd98f89d898a989d927346473
   C: dbe1301e2d1345038db84a25d4f5718e
   D: 9bacc29977891c009c3cea53c12cf93f
   E: Skip

2. **What is the name of the examiner who created "Strongwill.e01"?**
   A: Examiner (Blank no data input upon image creation)
   B: Strongwill
   C: R. C. Ahtac
   D: J. D. Nicks
   E: Skip

3. **What are the total number of sectors of the system?**
   A: 265148416
   B: 298989898
   C: 203984938
   D: 209839399
   E: Skip

4. **What version of Microsoft Windows is installed?**
   A: Windows 10 Personal (Home)
   B: Windows 10 Enterprise Evaluation
   C: Windows Server 2019 Themed as windows 10
   D: Windows 7 Service Pack 2
   E: Skip

5. **What is the build number of the Microsoft Windows installation?**
   A: 18362
   B: 5D356
   C: 19H1
   D: 1903
   E: Skip

6. **What is the installation date of the Windows Operating system? Answer in UTC.**
   A: 8/21/2019 5:22:04 AM
   B: 7/22/2019 7:19:04 AM
   C: 1/1/2001 00:00:00 AM
   D: 6/10/1990 11:34:02 AM
   E: Skip

7. **The application "SamsungPortableSSD.exe" may have been accessed through the Explorer GUI. If this event occurred, what is the volume serial number of the drive where the application run process originated from?**
   A: C6783AB1
   B: C9382CD2
   C: C6783BA1
   D: C8372DA9
   E: Skip

8. **This operating system is currently set to what time zone?**
   A: EST
   B: EDT
   C: PDT
   D: CST
   E: Skip

9. **What is the volume name of the Virtual Hard Drive that exists on the system?**
   A: HIDDEN
   B: PRIVATE
   C: SECRET
   D: VHD
   E: Skip

10. **What is the filesystem of the Virtual Hard Drive located on the primary partition of the system?**
    A: FAT32
    B: APFS
    C: NTFS
    D: FAT16
    E: Skip

11. **What is the name of the primary User Account of this system?**
    A: user
    B: test
    C: users
    D: windows
    E: Skip

12. **A file may have been uploaded to HTTPS://www.virustotal.com. If this occurred, what is the SHA-256 hash sum of the uploaded file?**
    A: acd946343893c33d15a1e82e6fe4c8d5f6518518bfb7d04f70b0b8bdb3775356
    B: 60662a8971a0509ded01240408ffd21fb379ee13b4aff5a3fe79f16748b91f10
    C: cc351446b9c1d9da3a6a8a676af961f55c7b00d1b8fe4b3ff9c851d1e39c3029
    D: 38ec73a46e7a6a7171c91dc003d135f01134e2311a5e868c797a1c8eaeb62583
    E: Skip

13. **The application C:\ProgramData\Samsung Apps\Portable SSD\SamsungPortableSSD.exe was accessed. How many times was it in "focus"?**
    A: 1
    B: 2
    C: 3
    D: 4
    E: Skip

14. **Located on the primary users' desktop is a file with the name "file.exe". What is this specific file type?**
    A: Portable Executable 32
    B: Word Document Extended
    C: Mach-0 X86_64
    D: ELF Binary Executable
    E: Skip

15. **Locate the file named "supersizeme.exe". What is the logical file size of this file in bytes?**
    A: 35,696
    B: 43,029
    C: 25,756
    D: 45,988
    E: Skip

16. **A photograph depicting a black Labrador retriever can be found on the primary partition of the system. What, if any, location information can be obtained from the EXIF data associated with the image?**
    A: No location information can be ascertained
    B: General location information can be ascertained
    C: Direct Latitude and Longitude can be ascertained
    D: Multiple Latitudes and Longitudes can be ascertained
    E: Skip

17. **What is the installation size of "Microsoft One Drive" in bytes?**
    A: 151119
    B: 198312
    C: 141449
    D: 100000
    E: Skip

18. **On what date did the first successful login utilizing RDP occur on this system?**
    A: 11/27/2018
    B: 07/27/2019
    C: 10/09/2019
    D: 07/22/2019
    E: Skip

19. **Does it appear that any of the following instances of malware are present on the system?**
    A: Code-red
    B: Locky
    C: Magecart
    D: No evidence of any potential malware
    E: Skip

20. **What is the modified UTC time for "notimetosaygoodbye.docx"as listed by the metadata?**
    A: 2019-10-09T20:05:00Z
    B: 2013-03-22T19:34:00Z
    C: 2019-03-09T09:44:00Z
    D: 2019-03-22T19:44:00Z
    E: Skip

21. **The computer user named "user" may have navigated to the "Downloads" directory using "Explorer". If this occurred, what is the date of the last access time?**
    A: The user did not access this directory.
    B: 10/7/2019
    C: 10/1/2019
    D: 10/19/2019
    E: Skip

22. The computer operator may have used the Windows terminal application to calculate the MD5 hashsum of the file. If this occurred, what is the name of the file as indicated by the Windows terminal Application?

A: iis.png
B: desktop.ini
C: hashme.txt
D: notimetosaygoodbye.doc
E: Skip

23. Are any Korean (Hangul) word processor documents stored on "Strongwill.E01"? If so, what is modified time of the last document accessed?

A: No Hangul Word Processor Documents contained within "Strongwill.E01"
B: 7/22/2019
C: 7/21/2019
D: 10/19/19
E: Skip

24. What is the last time the application "BASH.exe" was run? Answer in UTC-24hr format.

A: 10/06/2019 16:42:38
B: 10/07/2019 16:43:28
C: 10/07/2019 04:43:28
D: 10/10/2019 04:43:28
E: Skip