Pick a Tool, the Right Tool: Developing a Practical Typology for Selecting Digital Forensics Tools

GIAC (GCFA) Gold Certification

Author: J. Richard "Rick" Kiper, Ph.D., Richard.Kiper@leo.gov
Advisor: Sally Vandeven

Accepted: March 2018

Template Version September 2014

Abstract

One of the most common challenges for a digital forensic examiner is tool selection. In recent years, examiners have enjoyed a significant expansion of the digital forensic toolbox – in both commercial and open source software. However, the increase of digital forensics tools did not come with a corresponding organizational structure for the toolbox. As a result, examiners must conduct their own research and experiment with tools to find one appropriate for a particular task. This study collects input from forty six practicing digital forensic examiners to develop a Digital Forensics Tools Typology, an organized collection of tool characteristics that can be used as selection criteria in a simple search engine. In addition, a novel method is proposed for depicting quantifiable digital forensic tool characteristics.

1. Introduction

1.1. Purpose

The purpose for this research was to develop a typology for digital forensics tools so that a forensic examiner may be able to quickly assess and select a digital forensics tool appropriate for a particular task. To accomplish this goal, the study was guided by the following research question:

Which attributes would enable the accurate characterization and selection of a digital forensic tool?

It is important to note this research does not include the development of a technical implementation, such as an online search engine. Rather, the proposed typology of tool characteristics may be used as filterable criteria in existing spreadsheet lists or online collections such as the NIST Computer Forensics Tool Catalog (NIST, 2017).

1.2. Significance

In their survey research, Quick and Choo (2014) observed that "[a] major challenge to digital forensic analysis is the ongoing growth in the volume of data seized and presented for analysis" (p.273). Consequently, the proliferation of digital storage and communication devices has significantly increased the workload of digital forensic examiners who need access to appropriate forensics tools. The rapid expansion in the number and variety of digital forensics tools requires a method of selecting tools that is more efficient than those currently available. This study aims to develop a typology for digital forensics tools that facilitates selection based on a validated set of tool characteristics.

The remainder of this paper is organized as follows: In the next section, a review of the current literature provides context and background for the need to have a digital forensics tool typology. Next, research methods are summarized, followed by a discussion of findings. Finally, the paper presents implications, considerations for future work, and a conclusion. Appendices A, B, and C represent artifacts from the research and will be referenced throughout the paper.

2. Review of the Literature

A typology is a system used for categorizing things using more than one variable (Weil, Schleiter, & Tarlov, 1978). Typologies are useful for categorizing tools and have been implemented in the classification of a wide variety of tools, such as prehistoric tools (Wright, 1992), strategic analytical tools (Vaitkevičius, Merkys, & Savanevičienė, 2006), and simulation tools in modern medicine (Alinier, 2007). Typologies have even been used to categorize mapping tools for ecosystem services (Pagella & Sinclair, 2014) and communication tools for Corporate Social Responsibility (CSR) theories (Seele & Lock, 2015). Despite the popularity of typologies in nearly every field of practice, a typology for digital forensics tools was not found in the literature.

One of the reasons for this lack of organization in digital forensics tools could lie with the developers themselves. In justifying their typology for value stream tools, Hines and Rich (1997) noted that "authors have viewed their creations as *the* answer, rather than as a part of the jigsaw" (p.46, emphasis in the original). As a result, their existing "ill-defined and ill-categorized toolkit" (p.46) for value stream analysis needed organization to enable practitioners to select the appropriate tool. A similar problem is observed in the development of digital forensics tools. Several vendors often market their own tools as a complete solution, without consideration for the broader digital forensics landscape. Why would a typology be needed for selecting tools if each vendor believes its product has all the required features?

As discussed previously, many researchers have recognized the need for tool typologies in their own fields of science. The literature does not reveal why digital forensics should be an exception to this trend, as forensic examiners are practitioners who need a method for identifying and selecting appropriate tools. Indeed, researchers agree that "computer forensics experts need to make a significant decision with regard to the selection of an appropriate tool for digital evidence investigation" (Grigaliunas, Toldinas, & Venckauskas, 2017). A tool typology would facilitate that tool selection decision.

Simply providing a list of tools is seldom useful. Typically, digital forensics tools are characterized by an operating system platform, license type, version, and vendor. Even more comprehensive lists are limited to these metadata (See, for example, www.forensicswiki.org/wiki/Tools and en.wikipedia.org/wiki/List_of_digital_forensics_tools). These tool listings usually include short descriptions of the tools, but text descriptions cannot be "racked and stacked" for sorting and filtering. A more useful (and agreed upon) lexicon of tool characteristics is needed to enable the searching and selecting of tools for specific tasks.

To explain how forensic examiners should think about forensic tasks, Brian Carrier (2003) defined categories of forensic analysis types based on abstraction layers of data. He defined abstraction layers as physical media (e.g., sectors), media management (e.g., partitions), file system, and application. According to Carrier, digital forensics tools act upon digital devices to translate data from one layer to another and to present the data in a way that is useful to the investigator. Considering how forensic tools act on data abstraction layers is an effective starting point for the development of a typology.

The SANS Investigative Forensic Toolkit (SIFT) Workstation is a powerful collection of open source forensic tools distributed by the SANS Institute. In describing the capabilities of the Workstation, SANS lists tool characteristics such as file system support, evidence image support, and partition table support (Lee, 2014). In terms of understanding the function of the tools, these feature categories can be very useful. However, these categories do not answer questions regarding types of output, skills required to use the tools, or how well tools generate reports for court purposes, which is one of the chief duties of a digital forensics professional (NICCS, 2017).

In their attempt to organize the body of knowledge relating to cyber forensics, Brinson, Robinson, and Rogers (2006) created a cyber forensics ontology, which they describe as a classification scheme that "creates a common definition among a domain of information within a certain area" (p.37). They considered technical aspects of the field (i.e., hardware and software) as well as the professional aspects (i.e., law, academia, military, and private sector) in building their ontology. Because the researchers were organizing "common areas for specialization and certification" (p.37), they devoted only a small portion of their hierarchy to software analytical tools, which they simply grouped into proprietary versus open source tools. For the purposes of this study, such a broad characterization of tools is considered an incomplete typology because it is too general to be used as selection criteria for digital forensics tools.

Perhaps the most sophisticated attempt to provide a digital forensics tool selection system may be found in the online Computer Forensics Tool Catalog, maintained by the National Institute of Standards and Technology (NIST, 2017). Organized by 29 forensic tool "functionalities," this online search tool is powered by several filterable fields. These "technical parameters" contain multi-selectable lists of values but the parameters themselves are not common across all tool functionalities. For example, the "disk imaging" functionality has a searchable parameter of "digest hash algorithms" while the "hash analysis" functionality has a similar parameter called "supported hash algorithms," but with different values. The functionality descriptions and technical parameters (and their values) comprise what NIST calls a "Forensic Tool Taxonomy" (NIST, 2017).

Although the NIST tool catalog provides an effective parameter-based search mechanism for digital forensics tools, it is inconsistent and somewhat cumbersome to use. For example, sometimes items listed in "functionalities" seem to describe forensic processes (e.g., Email Parsing, File Carving) while others could be understood as artifact types or topic areas (e.g., Cloud Services, Social Media). Also, as noted previously, most technical parameters are exclusive to a particular functionality so a user must first know to select the functionality before being presented with any parameters for searching. Finally, even the parameters that are common across functionalities do not have consistent names. For example, a parameter may be listed as "Platform" in some functionalities but it appears as "Tool host OS / runtime environment" in others. The inconsistencies in the NIST tool catalog may be due to the crowdsourcing nature of how it is built and updated. On the website, NIST publicly elicits new suggestions for additional functionalities and modifications to their taxonomy (NIST, 2017).

Grigaliunas, Toldinas, and Venckauskas (2017) built upon the limited typology of Brinson, Robinson, and Rogers (2006) to create a transformation model that would enable a user to exploit the NIST tool catalog using the digital forensics XML library created by Garfinkel (2012). Although their research did not result in a specific tool, Grigaliunas, Toldinas, and Venckauskas (2017) proposed that future work on their research could include an “intelligent agent” that would search the NIST tool catalog based on their transformed classification scheme. However, they did not suggest how such a search mechanism would be validated. In fact, a validation of NIST’s Forensic Tool Taxonomy itself could not be found in the literature.

A typology entails putting things into groups according to how they are similar so that objects within the typology may be readily retrieved. For the domain of digital forensics tools, such a construct has not been fully developed or validated in the literature. This study aims to develop an easy-to-use, practical typology that facilitates the selection of digital forensics tools based on user-specified attributes.

3. Methods

The goal of this study was to develop a typology that facilitates the selection of digital forensics tools. It was desired that the typology be constructed with input from subject matter experts (SMEs) – specifically, digital forensic examiners who select tools on a regular basis.

3.1. Phase 1: Foundational responses

Data were collected in three phases. In the first phase, a series of interviews were conducted with thirteen (13) practicing digital forensic examiners who were personally known to the researcher and work for a variety of public and private sector organizations. This group of SMEs represented examiners with significant work experience as well as technical specialties.

In developmental research (whose goal is to develop a product to solve a problem), a group of six to ten experts is typically required to achieve consensus (Landeta, Barrutia, & Lertxundi, 2011; Kiper, 2016). Therefore, the number of participants in this study was more than sufficient to produce meaningful results. Five of the experts participated by e-mail and eight were personally interviewed.

To elicit their opinions regarding how they select digital forensics tools, each expert was asked to respond to the same prompt:

> *Imagine an investigator gives you a sealed container, and the only thing you know is that there is digital evidence inside to be analyzed. What questions do you ask yourself (and the investigator) when deciding which kind of software tool you will need to analyze the data inside?*

If the participant felt the question was unclear, then they were asked one or more follow up questions:

- Which actions do software forensic tools perform on data?
- How would you categorize the types of data touched by forensic tools?
- How would you categorize the types of output or results produced by these tools?
- After finding a tool, what information is most useful to see in its description?

After the interview phase of data collection was completed, the responses were analyzed for patterns and a list of candidate attributes (and sample values) was developed as a result (see Appendix A). Section Four provides a full discussion of the findings. These forensic tool criteria provided the basis for the next phase of data collection.

3.2. Phase 2: Voting on tool features

The second phase of data collection consisted of an online survey that asked participants to select the ten most important tool characteristics from the list developed in Phase One. A total of 46 participants responded to the survey, which was advertised on a digital forensics website and a cybersecurity listserv. The survey instrument (see Appendix B) included multi-selectable checkboxes for each characteristic, and the results were compiled for analysis. Participants were asked to select their top ten choices in order to limit the number of judgments (Bolger & Wright, 2011), but the compiled, final list consisted of more than ten characteristics. Tool characteristics that received significant numbers of "votes" were included in the final typology.

3.3. Phase 3: Rating tools on selected features

During the third phase of data collection, participants were asked via survey to rate a list of twelve (12) forensic tools based on quantifiable characteristics identified in Phase One. Quantifiable characteristics are those that are difficult to represent as discrete values (such as *Output Quality*) for the purpose of building selection criteria. The ratings were used to construct a series of two-dimensional graphs, with the tools falling into one of four distinct quadrants. The research of Vaitkevičius, Merkys, and Savanevičienė (2006) found this method to be an effective way to graphically communicate the characteristics of their strategic analysis tools typology.

As described in Section Four, the survey items for Phase One and Two were combined into one survey, which was marketed to the broader digital forensics community. The survey remained open for two weeks, and 46 participants responded.

4. Findings and Discussion

4.1. Phase 1: Responses to open-ended questions

Thirteen digital forensic examiners participated in the first phase of the study. The participants represented both public and private sector organizations in six different U.S. states. Participants were practicing examiners with several years of experience.

The participants' task during this phase of the research was to identify the characteristics of digital forensic tools that could be used as selection criteria. For consistency, the experts answered a standardized prompt – whether responding by e-mail or during an in-person interview:

> *Imagine an investigator gives you a sealed container, and the only thing you know is that there is digital evidence inside to be analyzed. What questions do you ask yourself (and the investigator) when deciding which kind of software tool you will need to analyze the data inside?*

After listening to (or reading) the prompt, each participant provided detailed feedback. An analysis of these data produced several categories of tool characteristics, and the frequency of the participants' mention of these attributes was recorded in a spreadsheet (see Appendix A). Categories, proposed values, and the total frequency of digital tool characteristics are summarized in Table 1.

When considering how to select the appropriate digital forensic tool, the expert participants most frequently mentioned issues relating to the subject device, the data on the device, the quality of the tool output (or report), and the ability of the tool to parse the subject data for relevant artifacts. The relative popularity of these tool characteristics is reflected in Table 1.

CATEGORY and Proposed VALUES	Totals
The Subject Device	
Device type (Mobile device, HDD, SSD, optical media, flash media, unknown)	12
Required Interfaces (Hardware, Software-bootable media)	1
Device state (Live/running vs. turned off)	2
The Subject Data	
File System (NTFS, FAT, HFS+, APFS, Ext, Proprietary)	11
Operating System (Windows, MacOS, iOS, Linux, Proprietary)	11
Amount of data	3
General Tool Characteristics	
Runtime OS (Windows, MacOS, iOS, Linux, Proprietary)	2
Bootable from removable media	1
Memory requirements	2
Processing speed (before analysis can begin)	8
Output format (Raw data, tech report, runtime/reader tool, etc.)	10
Required skill for use (Simple GUI, difficult GUI, command line)	8
Cost (Open source, individual/group licensing)	4
Exam Focus (All-in-one vs. artifact-focused only tool)	7
Pre-analytical Features - Ability to perform:	
Write-blocking	2
Data-at-rest acquisition	5
Live memory acquisition	1
Indexing	1
Hash verification	2
Decryption/Decoding of Obfuscated data	6
Bypass passwords	1
Advanced features (e.g., Rebuild RAIDs, acquire from cloud, VMs, enterprise discovery)	4
Processing Features - Ability to parse/extract:	
File types (Multimedia, documents, databases, archives, executables)	10
File artifacts (PCAPs, logs, VMs, Internet History)	8
OS Artifacts (Registry, plists, sqlite databases)	8
Inactive data (Unallocated space, deleted items, slack space)	7
Descriptive information	
Versions/Updates	2
Supported formats	2
Analytical features (e.g., Applying filters, sorts, labels, bookmarks)	1
Scalable/customizable (i.e., with user-developed plugins)	2
Support for foreign languages (Tool interface and subject data)	1
Limitations/erroneous data reports/bug reports	6
Tool co-dependencies (i.e., you must first mount with Tool A to analyze with Tool B)	1
User ratings	1
Validity as judged by the forensic community	3
Admissibility in court	2

Table 1. Summary of Phase 1 Responses.

Some of the participants' responses were not relevant to the task of tool selection. For example, some participants indicated they would want to know if the subject device had been damaged or tampered with. Others wanted to know whether the evidence was original, rather than a logical or forensic copy. These issues, while important, could not be used effectively as selection criteria for a digital tool.

Some of the participants said they would want to know tool-related information such as scalability, co-dependencies, and limitations. Again, these are attributes that are not easily represented in drop-down lists used to filter searches for digital tools. However, it would be useful information to have in a tool *description* – after a person has found the tool via standard selection criteria. Therefore, this type of information was listed in Table 1 under the *Descriptive Information* category.

4.2. Phase 2: Results of tool characteristic survey

To validate the results from Phase One and expand the number of participants in the study, a Google Forms Survey was constructed. To elicit input from a population of digital forensic experts, the survey was advertised in the GIAC Advisory Board listserv, as well as on the popular aboutdfir.com website, an online resource for digital forensics and incident response. The survey was open for two weeks and 46 individuals participated.

The first part of the survey (see Appendix B) presented participants with the list of characteristics generated by Phase One, preceded by the following instruction:

> *Which of the following are the TEN MOST IMPORTANT characteristics when selecting a digital forensics tool? In other words, what are the ten most important things YOU would like to know about a forensic tool or the subject device in order to decide whether you should use a particular tool for the device?*

The form enforced a "ten selections" rule, so all participants were required to identify exactly ten tool characteristics. Asking the participants to anonymously identify their top ten choices avoided a group-think mentality (where *everything* is seen as important) while providing enough variety in responses to generate meaningful conclusions. The results are summarized in Table 2.

Ranking the characteristics by raw votes yields a hierarchy of sorts. According to the survey participants, a tool's *parsing capabilities* are the most important characteristics to consider when selecting a digital forensic tool. These are followed immediately by features that pertain to the *subject device* and the *data* on the subject device. The characteristics with the largest number of votes roughly correspond to those with the largest number of mentions in the Phase One interviews, thus providing a measure of validity for those results.

At two places in the data there exists a point drop off of five points (26 to 21 and 10 to 5), indicating where delineating groups may be appropriate. Consequently, Table 2 may be divided into three sections: the critical characteristics for tool selection (indicated in green), the less critical but important characteristics (indicated in blue), and the rest of the characteristics, which could be included in tool descriptions as mentioned previously.

Categories of Tool Characteristics	Votes
PARSING CAPABILITIES: OS Artifacts (Registry, plists, sqlite databases, etc.)	37
PARSING CAPABILITIES: File artifacts (PCAPs, logs, VMs, Internet History, etc.)	34
PARSING CAPABILITIES: Inactive data (Unallocated space, deleted items, slack space, etc.)	31
PARSING CAPABILITIES: File types (Multimedia, documents, databases, archives, executables, etc.)	30
SUBJECT DATA: File System (NTFS, FAT, HFS+, APFS, Ext, Proprietary)	29
SUBJECT DATA: Operating System (Windows, MacOS, iOS, Linux, Proprietary)	27
SUBJECT DEVICE: Device type (Mobile device, HDD, SSD, optical media, flash media, etc.)	26
SUBJECT DEVICE: Device state (Live/running vs. turned off)	21
PRE-ANALYSIS FEATURES: Decryption/Decoding of Obfuscated data	21
GENERAL TOOL CHARACTERISTICS: Runtime OS (Windows, MacOS, iOS, Linux, Proprietary)	19
PRE-ANALYSIS FEATURES: Live memory acquisition	19
GENERAL TOOL CHARACTERISTICS: Processing speed (before analysis can begin)	18
PRE-ANALYSIS FEATURES: Write-blocking	17
SUBJECT DATA: Amount of data	16
PRE-ANALYSIS FEATURES: Hash verification (Individual file or whole disk)	15
PRE-ANALYSIS FEATURES: Advanced (e.g., Rebuild RAIDs, acquire from cloud, VMs, enterprise discovery)	15
PRE-ANALYSIS FEATURES: Bypass passwords	14
PRE-ANALYSIS FEATURES: Indexing	12
PRE-ANALYSIS FEATURES: Data-at-rest acquisition	10
SUBJECT DEVICE: Required Interfaces (Hardware, Software-bootable media)	5
GENERAL TOOL CHARACTERISTICS: Bootable from removable media	5
GENERAL TOOL CHARACTERISTICS: Memory requirements	4
Other	4

Table 2. Summary of Phase 2 Survey Responses.

Four of the 46 participants utilized the "Other" selection and "Comments" field to offer additional ideas. One participant reiterated the need for write-blocking the evidence.

A second participant disputed the need to differentiate between live data and data-at-rest. A third mentioned “data culling” with no further explanation. Finally, one participant offered a brief commentary:

> In general, I consider most 'static' capabilities you've listed to be uninteresting. Things will change, and static capabilities cannot change, except at the whim of the tool manufacturer. An extremely important element to me is architecture: how can I add capabilities? ...While monolithic tools are fine to cut ones teeth on, they are not a place to live *unless* the manufacturer can keep up the pace.

This well-articulated need for the tool to be scalable or customizable was captured in the relevant *Descriptive Information* numbers of Table 1, thus lending more validity to the Phase One data. The results of the Phase Two data collection form the basis of the forensic tool typology described in Section 4.4.

4.3. Phase 3: Results of tool rating survey

The purpose of the study’s third phase was to develop a way to graphically represent certain characteristics of digital forensic tools. Participants were asked to rate a list of 12 forensic tools based on *quantifiable* characteristics identified in Phase One (see Table 1 characteristics highlighted in pink). In short, participants were asked to rate each tool (on a scale from 1 to 5), in the four dimensions described below. The participants selected "Don't Know" for those items for which they were unfamiliar.

- **REQUIRED SKILL** - Tools on one end of the spectrum require in-depth command line skills, while other tools have point-and-click GUIs. However, not all GUIs are intuitive for the user.
- **OUTPUT QUALITY** - Some tools spit out raw data, which can be imported into another format for readability, while other tools provide an interactive, reader-friendly report for review and presentation. And there is everything in between.
- **COST** - The cost to acquire and use a tool ranges from free (generally open-source) to very expensive licensing agreements.
- **EXAM FOCUS** - Some forensic tools focus on a particular artifact, or a group of artifacts, while other tools are considered a "one-stop shop" for analyzing a variety of artifacts.

The Phase Three collection of data was accomplished using the same survey form that collected Phase Two data (see Appendix C). The survey design enabled the quick rating of tools in each of the dimensions, so Phase Two and Phase Three data collection was combined into one survey. Combining the surveys eliminated the need to re-advertise for participants in a second survey, thus saving time in data collection.

The survey form enforced the rule that participants rate each tool in every dimension or select "Don't Know" as a response. The responses are summarized in Table 3, which reflects the average participant rating for each tool dimension with respect to each tool. Participants gave FTK Imager the lowest rating (1.9) for *Required Skill,* meaning it is the easiest tool to use. The most difficult tool to use (3.9) was Volatility, likely due to its command line interface and required knowledge of its plugins (see www.volatilityfoundation.org). F-Response received the lowest marks (2.3) for *Output Quality* while Internet Evidence Finder (IEF) excelled in this area (4.0). It is noteworthy that IEF provides a "portable case" feature that enables an examiner to create a stand-alone, interactive copy of the examination results with many of the search/sort/filter capabilities of the full IEF application (see www.magnetforensics.com).

Free or open-source tools scored lowest in the *Cost* dimension (1.1-1.2), while EnCase and FTK/LAB were rated most expensive (4.6 and 4.2, respectively). Finally, in the *Exam Focus* dimension, the participants scored SkypeAlyzer lowest (1.6), meaning it is most focused on a single type of artifact. On the other hand, EnCase, FTK/LAB, and X-ways all tied for the top score (4.0) and are therefore considered all-in-one tools.

	Participant Ratings for Digital Forensic Tools											
Tool Dimensions	**Autopsy**	**EnCase**	**Foremost**	**FTK/LAB**	**F-Response**	**FTK Imager**	**IEF**	**Redline**	**RegRipper**	**SkypeAlyzer**	**Volatility**	**X-Ways**
REQUIRED SKILL (1-very easy, 5-very difficult)	2.7	3.6	3.1	3.0	2.8	1.9	2.1	2.8	2.7	2.2	3.9	3.8
OUTPUT QUALITY (1-raw data, 5-interactive report)	3.1	3.2	2.7	3.7	2.3	2.7	4.0	3.3	2.7	3.2	2.7	3.3
COST (1-very cheap/free, 5-very expensive)	1.2	4.6	1.5	4.2	3.1	1.1	3.7	1.3	1.1	1.8	1.2	3.0
EXAM FOCUS (1-artifact-focused, 5-All-in-one tool)	3.2	4.0	2.0	4.0	2.7	2.6	3.2	2.7	1.9	1.6	2.6	4.0

Table 3. Summary of Phase 3 Survey Ratings.

As with the first half of the survey (Phase Two collection), several participants provided comments along with their ratings in the second half of the survey (Phase Three collection). Some respondents suggested additional tools that should have been considered, such as Rekall Agents, Axiom, Paraben, and Nuix. Others took issue with the term *Output Quality*, as they expressed a higher interest in the accuracy of the tool output rather than the user-friendliness of a generated report. Finally, a participant suggested that the *Cost* dimension should include the price of training, as well as the cost of time wasted using a tool that does not perform as expected.

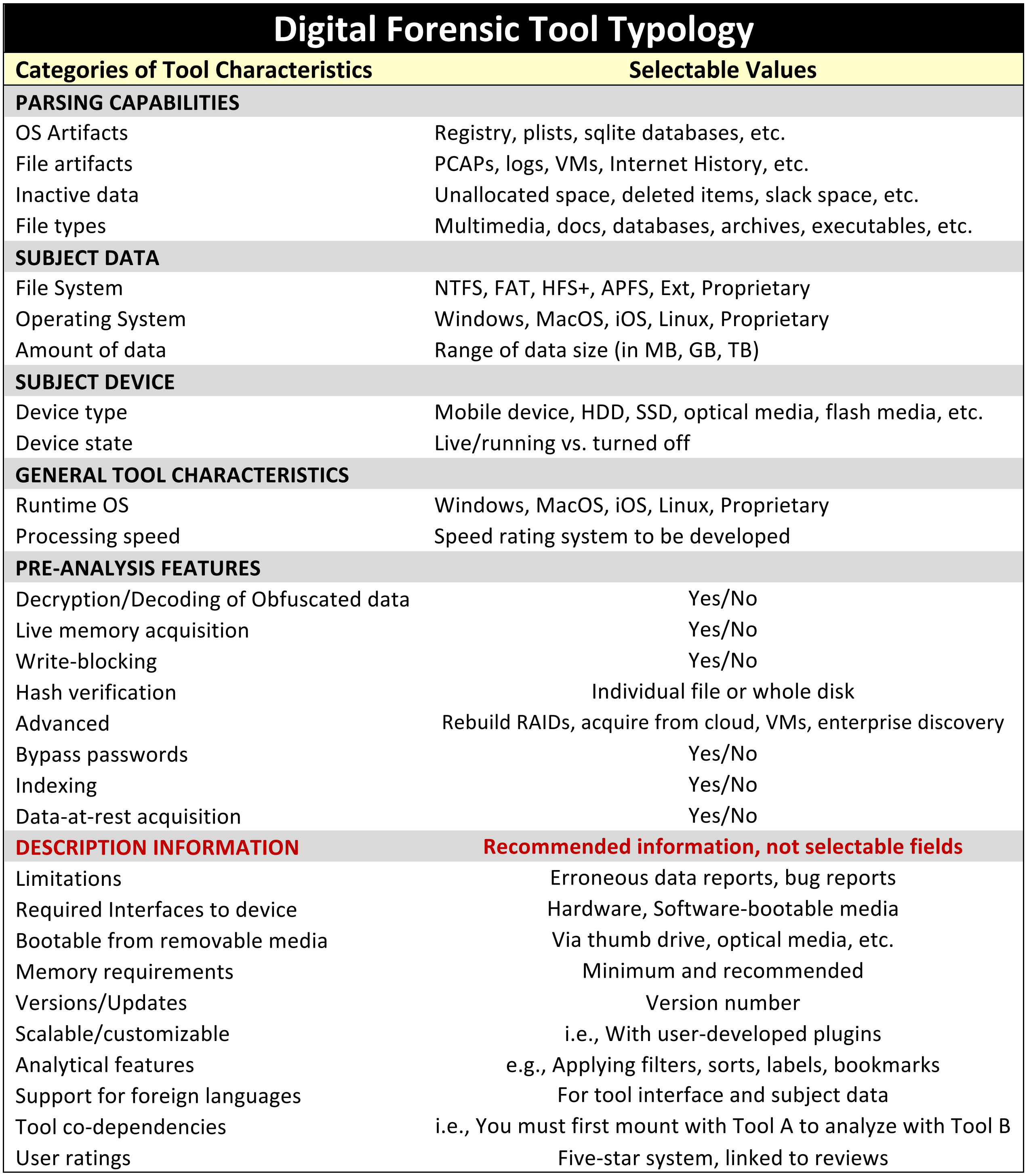
4.4. The typology

As stated previously, a tool typology identifies characteristics that are common across tools and helps organize them for research and use. For the digital forensic examiner, a typology may be used to build searchable criteria by which an appropriate tool may be selected for a particular task.

Typology of Digital Tool Characteristics

The results of the analysis of data from Phase One and Phase Two provided the basis of the proposed Digital Forensic Tool Typology depicted in Table 4. Specifically, the tool characteristics listed in Table 2 appear in the typology of Table 4, in roughly the same order, to preserve the priority level of the tool characteristics. This priority order may be used as guidance for building a database or application that may be limited by the number of searchable criteria. In addition, the lowest-rated characteristics from Table 2 were included as *description information* in the typology.

As discussed previously, *description information* includes characteristics that are useful to know about a tool but are not appropriate as selection criteria. In fact, users see descriptive information about a tool only AFTER they have located the tool using selection criteria. For example, after selecting a tool based on parsable file artifacts, subject data file system, and runtime operating system, a user would be presented with the versions, limitations, and analytical features of the tool.



Digital Forensic Tool Typology

Categories of Tool Characteristics	Selectable Values
PARSING CAPABILITIES	
OS Artifacts	Registry, plists, sqlite databases, etc.
File artifacts	PCAPs, logs, VMs, Internet History, etc.
Inactive data	Unallocated space, deleted items, slack space, etc.
File types	Multimedia, docs, databases, archives, executables, etc.
SUBJECT DATA	
File System	NTFS, FAT, HFS+, APFS, Ext, Proprietary
Operating System	Windows, MacOS, iOS, Linux, Proprietary
Amount of data	Range of data size (in MB, GB, TB)
SUBJECT DEVICE	
Device type	Mobile device, HDD, SSD, optical media, flash media, etc.
Device state	Live/running vs. turned off
GENERAL TOOL CHARACTERISTICS	
Runtime OS	Windows, MacOS, iOS, Linux, Proprietary
Processing speed	Speed rating system to be developed
PRE-ANALYSIS FEATURES	
Decryption/Decoding of Obfuscated data	Yes/No
Live memory acquisition	Yes/No
Write-blocking	Yes/No
Hash verification	Individual file or whole disk
Advanced	Rebuild RAIDs, acquire from cloud, VMs, enterprise discovery
Bypass passwords	Yes/No
Indexing	Yes/No
Data-at-rest acquisition	Yes/No
DESCRIPTION INFORMATION	**Recommended information, not selectable fields**
Limitations	Erroneous data reports, bug reports
Required Interfaces to device	Hardware, Software-bootable media
Bootable from removable media	Via thumb drive, optical media, etc.
Memory requirements	Minimum and recommended
Versions/Updates	Version number
Scalable/customizable	i.e., With user-developed plugins
Analytical features	e.g., Applying filters, sorts, labels, bookmarks
Support for foreign languages	For tool interface and subject data
Tool co-dependencies	i.e., You must first mount with Tool A to analyze with Tool B
User ratings	Five-star system, linked to reviews

Table 4. A Proposed Typology for Digital Forensic Tools.

Graphical Representation of Characteristics

To supplement the Digital Forensic Tool Typology and provide additional guidance for tool selection, the data from Table 3 was transformed into a graphical format. This approach was inspired by the research of Vaitkevičius, Merkys, and

Savanevičienė (2006), who used this method to visualize ratings for their strategic analysis tools typology. As explained in the survey introduction (see Appendix C), the chosen list of digital forensic tools was not intended to be a comprehensive list, but rather a representative list that could be used to test the effectiveness of representing attributes graphically.

Figure 1 graphs the *Required Skill* dimension against the *Output Quality* dimension for the selected tools, resulting in four quadrants. Using this graph, tools may be quickly characterized as either difficult or easy to use, while providing either a raw or refined output. For example, according to the graph Volatility may be characterized as a difficult tool that provides a relatively unrefined or raw output. On the other hand, IEF is an easy-to-use tool with a more sophisticated output, such as a full report.

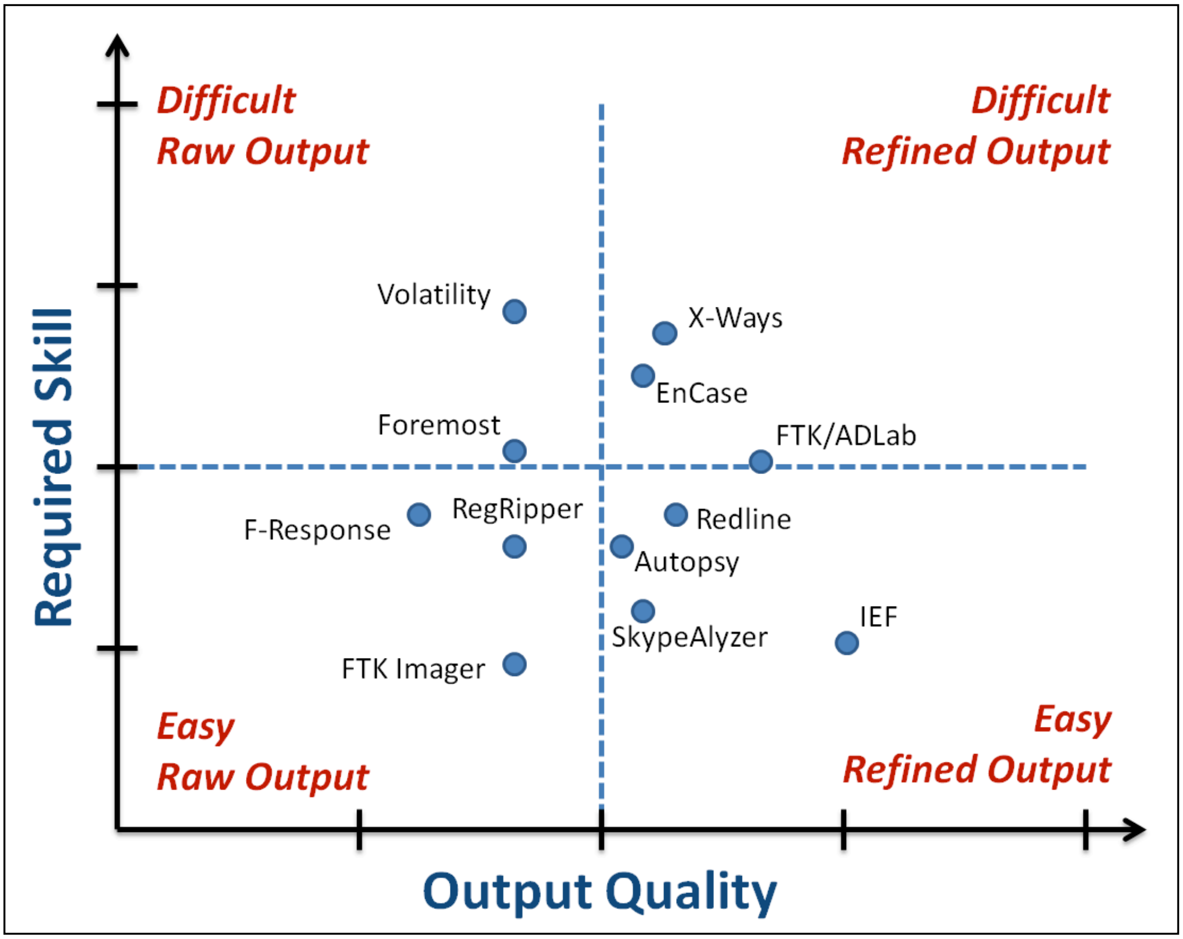


Figure 1. Graphing Required Skill versus Output Quality for Digital Forensic Tools.

While a tool's ease of use and output quality may be useful to know, other characteristics could determine whether an examiner selects a tool. Table 3 provided data to graph two other dimensions, which are graphed below in Figure 2: *Cost* and *Exam Focus*. In this figure, one may observe that free and open source tools are found clustered near the bottom of the graph, but they vary in their ability to examine a single artifact versus a variety of artifacts. More expensive, all-in-one tools are found in the top right quadrant.

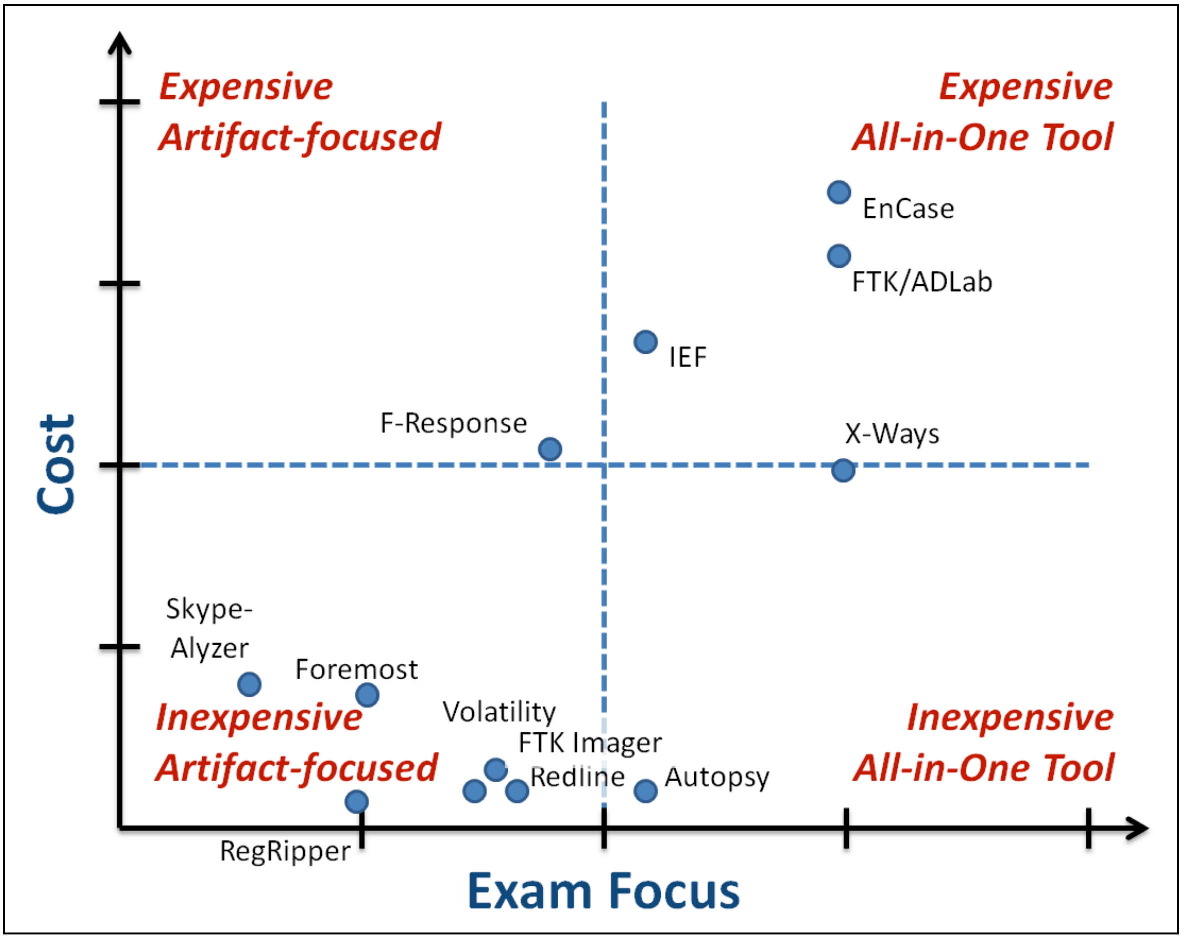


Figure 2. Graphing Cost verses Exam Focus for Digital Forensic Tools.

5. Implications and Recommendations

This paper makes two major contributions to the body of knowledge in the field of digital forensics. The first is a novel research-based topology for digital forensics tools. The second is a method for graphically representing quantifiable ratings for those tools. These contributions provide practical and educational value to digital forensics practitioners, instructors, and students, and could inspire future research in the field.

5.1. Implications

By relying on the expertise of digital forensic examiners, this study created a typology that identifies commonalities among the scores of commercial and open source digital forensics tools. The typology proposed in Table 4 is useful not only for thinking about digital forensics tools but also for developing a search strategy for tools suitable for a particular digital forensics task. In fact, by using the typology, one could develop an effective search utility that saves the examiner both time and frustration while looking for an appropriate tool. This possibility will be discussed in the next section.

The two-dimensional graphs of digital forensics tools (Figures 1 and 2) are an effective way of visualizing the four *quantifiable* characteristics that were identified in Phase One of this study. By referring to the graphs, an examiner can quickly locate a digital forensic tool on the spectra of *Required Skill*, *Output Quality*, *Cost*, and *Exam Focus*. The graphs would be especially useful in digital forensics training as a quick reference for students unfamiliar with the tools. For example, a classroom discussion could address the fact that Autopsy is considered an inexpensive all-in-one tool, but it may not be as comprehensive as EnCase, FTK/ADLab, or X-Ways. Even if instructors decide to modify the values of the graphs to suit their own opinions, this type of graphical representation still serves as a concise but effective way of conveying information about a variety of digital forensic tools.

5.2. Recommendations and future work

The next step in implementing the typology is to build a simple knowledge management system (KMS) – such as a database or spreadsheet – and populate its records with digital forensics tool characteristics and values. A KMS based on this typology has the advantage of having been developed and validated by several dozen experts in the field of digital forensics. The KMS designer could start with the characteristics at the top of the topology, and then could continue adding characteristics to the search criteria as design constraints permit. While there is no consensus in the literature about the *optimum* number of search criteria, some researchers recognize that having too many search criteria may be confusing to the user and could unnecessarily limit search results (see Jannach, Zanker, & Fuchs, 2009; Schwilch, Bachmann, & Liniger, 2008; Torge & Hying, 2003).

Further validation of the Digital Forensics Tool Typology could be accomplished by means of a usability study. For example, researchers could compare the search efficiency of the NIST Computer Forensics Tool Catalog (NIST, 2017) with a searchable KMS based on the typology developed in this study. Search efficiency could be measured by the time required to look up a tool that matches a given set of characteristics.

In addition, future research can refine the graphical representations of quantifiable tool characteristics as presented in this paper. Other popular tools, such as those suggested by the study participants, could be added to the existing graphs. Finally, researchers could develop other graphs, such as *Cost* versus *Output Quality* and *Required Skill* versus *Exam Focus*, which could likewise yield interesting results.

6. Conclusion

The primary aim of this study was to develop an efficient method for selecting digital forensic tools. The primary research question was addressed by the creation of the Digital Forensics Tool Typology, which provides attributes that enable the accurate characterization and selection of a digital forensic tool. Unlike other attempts to help examiners find forensic tools, the typology consists of a limited, but validated set of digital forensic tool selection criteria (and criteria categories) that may be used to build a simple search engine. In addition, the graphical approach presented in this paper offers a simple way of visualizing the quantifiable characteristics of digital forensics tools.

By reducing the effort needed to locate an effective digital forensics tool, examiners will have more time to perform the collection, preservation, analytical, and reporting functions associated with the digital forensics mission.

References

Alinier, G. (2007). A typology of educationally focused medical simulation tools. Medical teacher, 29(8), e243-e250.

Bolger, F. and Wright, G. (2011). Improving the Delphi process: Lessons from social psychological research. Technological Forecasting & Social Change, 78, 1500-1513.

Brinson, A., Robinson, A., & Rogers, M. (2006). A cyber forensics ontology: Creating a new approach to studying cyber forensics. Digital Investigation, 3, 37-43.

Carrier, B. (2003). Defining digital forensic examination and analysis tools using abstraction layers. International Journal of digital evidence, 1(4), 1-12.

Garfinkel, S. (2012). Digital forensics XML and the DFXML toolset. Digital Investigation, 8(3), 161-174.

Grigaliunas, S., Toldinas, J., & Venckauskas, A. (2017). An Ontology-Based Transformation Model for the Digital Forensics Domain. Elektronika ir Elektrotechnika, 23(3), 78-82.

Hines, P., & Rich, N. (1997). The seven value stream mapping tools. International journal of operations & production management, 17(1), 46-64.

Jannach, D., Zanker, M., & Fuchs, M. (2009). Constraint-based recommendation in tourism: A multiperspective case study. *Information Technology & Tourism*, *11*(2), 139-155.

Kiper, J. R. (2016, January). Needs to Know: Validating User Needs for a Proposed FBI Academy Knowledge Management System. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4334-4343). IEEE.

Landeta, J., Barrutia, J., and Lertxundi, A. (2011). Hybrid Delphi: A methodology to facilitate contribution from experts in professional contexts. Technological Forecasting & Social Change, 78, 1629-1641.

Lee, R. (2014). SANS SIFT 3.0 Virtual Machine Released. SANS Digital Forensics and Incident Response Blog, March 24, 2014. Downloaded on August 25, 2017 from SANS: https://digital-forensics.sans.org/blog/2014/03/23/sans-sift-3-0-virtual-machine-released.

National Initiative for Cybersecurity Careers and Studies (2017). Cybersecurity Workforce Framework: Digital Forensics. Retrieved August 21, 2017 from NICCS: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/digital-forensics.

National Institute of Standards and Technology (2017). Computer Forensics Tool Catalog. Last modified March 6, 2017. Retrieved August 21, 2017 from https://toolcatalog.nist.gov/index.php.

Pagella, T. F., & Sinclair, F. L. (2014). Development and use of a typology of mapping tools to assess their fitness for supporting management of ecosystem service provision. Landscape ecology, 29(3), 383-399.

Quick, D., & Choo, K. K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation, 11(4), 273-294.

Schwilch, G., Bachmann, F., & Liniger, H. (2008). Guidelines for WB3 Part III: Stakeholder workshop 2: Selection and decision on prevention and mitigation strategies to be implemented.

Seele, P., & Lock, I. (2015). Instrumental and/or deliberative? A typology of CSR communication tools. Journal of Business Ethics, 131(2), 401-414.

Torge, S., & Hying, C. (2003). *U.S. Patent No. 20050234872A1*. Washington, DC: U.S. Patent and Trademark Office.

Vaitkevičius, S., Merkys, G., & Savanevičienė, A. (2006). Model of strategic analysis tools typology. Engineering Economics, 47(2), 99-109.

Weil, P. A., Schleiter, M. K., & Tarlov, A. R. (1978). National study of internal medicine manpower: II. A typology of residency training programs in internal medicine. Ann Intern Med, 89(5 Pt 1), 702-715.

Wright, K. (1992). A classification system for ground stone tools from the prehistoric Levant. Paléorient, 53-81.Strunk, W., & White, E. B. (1999). *The elements of style*. Boston: Allyn and Bacon.

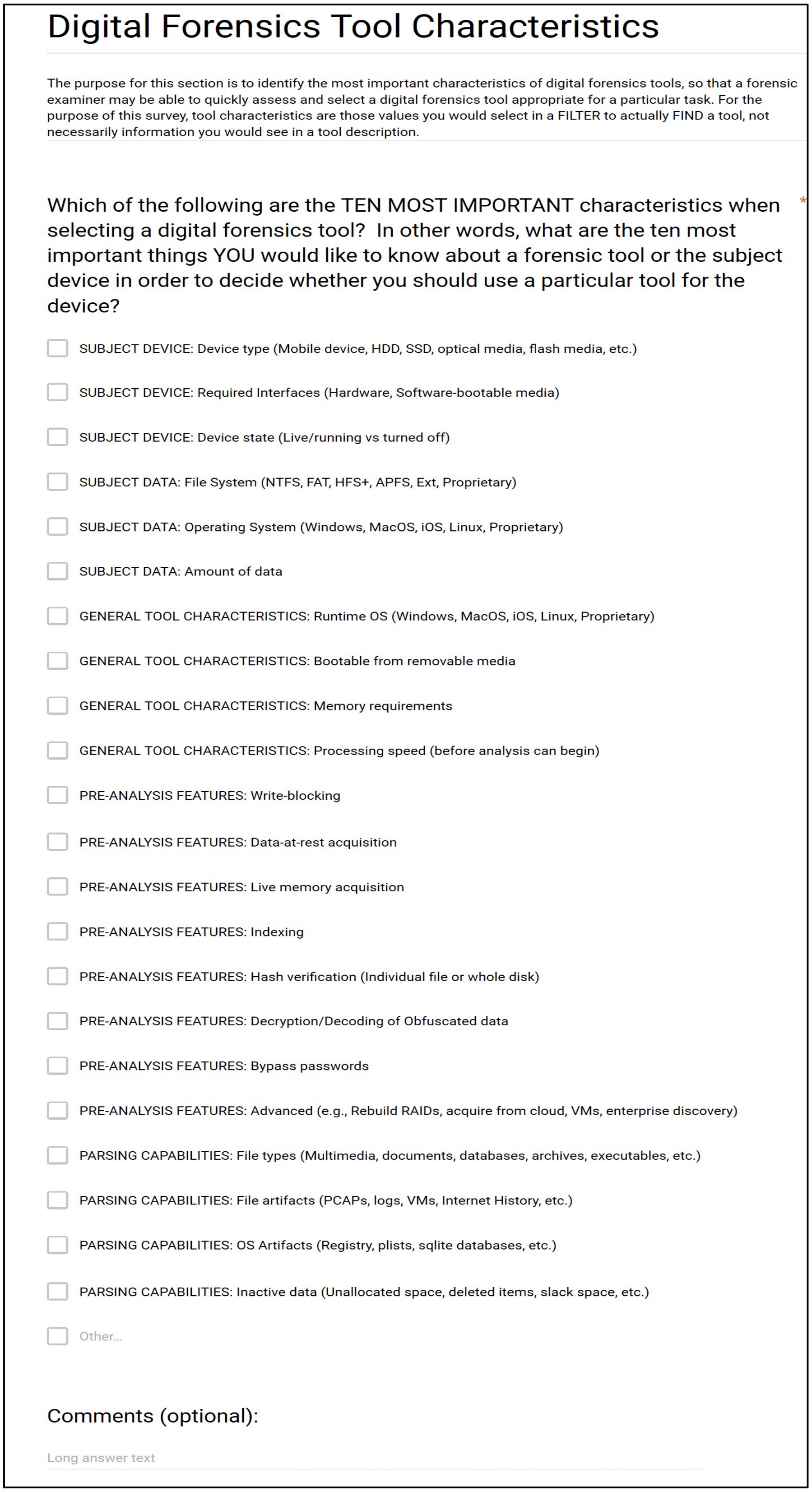
Appendix A

Phase One Results

		PARTICIPANTS												
CATEGORY and Proposed VALUES	**Totals**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
The Subject Device														
Device type (Mobile device, HDD, SSD, optical media, flash media, unknown)	12	1	1	1	1	1	1	1	1	1		1	1	1
Required Interfaces (Hardware, Software-bootable media)	1		1											
Device state (Live/running vs turned off)	2				1						1			
The Subject Data														
File System (NTFS, FAT, HFS+, APFS, Ext, Proprietary)	11		1	1		1	1	1	1	1	1	1	1	1
Operating System (Windows, MacOS, iOS, Linux, Proprietary)	11			1	1	1	1	1	1	1	1	1	1	1
Amount of data	3		1	1							1			
General Tool Characteristics														
Runtime OS (Windows, MacOS, iOS, Linux, Proprietary)	2								1		1			
Bootable from removable media	1									1				
Memory requirements	2								1		1			
Processing speed (before analysis can begin)	8			1	1		1	1	1	1	1	1		
Output format (Raw data, tech report, runtime/reader tool, etc.)	10	1	1				1	1	1	1	1	1	1	1
Required skill for use (Simple GUI, difficult GUI, command line)	8			1	1			1	1	1		1	1	1
Cost (Open source, individual/group licensing)	4			1				1			1	1		
Exam Focus (All-in-one vs artifact-focused only tool)	7			1			1	1	1	1		1		1
Pre-analytical Features - Ability to perform:														
Write-blocking	2		1									1		
Data-at-rest acquisition	5					1	1	1		1			1	
Live memory acquisition	1					1								
Indexing	1										1			
Hash verification	2								1					1
Decryption/Decoding of Obfuscated data	6	1	1				1		1			1	1	
Bypass passwords	1											1		
Advanced features (e.g., Rebuild RAIDs, acquire from cloud, VMs, enterprise discovery)	4			1				1			1	1		
Processing Features - Ability to parse/extract:														
File types (Multimedia, documents, databases, archives, executables)	10	1	1			1	1	1	1		1	1	1	1
File artifacts (PCAPs, logs, VMs, Internet History)	8	1	1			1	1	1	1	1				1
OS Artifacts (Registry, plists, sqlite databases)	8	1	1			1	1	1	1	1				1
Inactive data (Unallocated space, deleted items, slack space)	7	1	1		1	1	1	1					1	
Descriptive information														
Versions/Updates	2							1			1			
Supported formats	2							1	1					
Analytical features (e.g., Applying filters, sorts, labels, bookmarks)	1												1	
Scalable/customizable (i.e., with user-developed plugins)	2							1			1			
Support for foreign languages (Tool interface and subject data)	1										1			
Limitations/erroneous data reports/bug reports	6							1		1	1	1	1	1
Tool co-dependencies (i.e., you must first mount with Tool A to analyze with Tool B)	1													1
User ratings	1												1	
Validity as judged by the forensic community	3			1	1									1
Admissibility in court	2			1	1									

Appendix B

Phase Two Survey Form



Digital Forensics Tool Characteristics

The purpose for this section is to identify the most important characteristics of digital forensics tools, so that a forensic examiner may be able to quickly assess and select a digital forensics tool appropriate for a particular task. For the purpose of this survey, tool characteristics are those values you would select in a FILTER to actually FIND a tool, not necessarily information you would see in a tool description.

Which of the following are the TEN MOST IMPORTANT characteristics when selecting a digital forensics tool? In other words, what are the ten most important things YOU would like to know about a forensic tool or the subject device in order to decide whether you should use a particular tool for the device? *

□ SUBJECT DEVICE: Device type (Mobile device, HDD, SSD, optical media, flash media, etc.)

□ SUBJECT DEVICE: Required Interfaces (Hardware, Software-bootable media)

□ SUBJECT DEVICE: Device state (Live/running vs turned off)

□ SUBJECT DATA: File System (NTFS, FAT, HFS+, APFS, Ext, Proprietary)

□ SUBJECT DATA: Operating System (Windows, MacOS, iOS, Linux, Proprietary)

□ SUBJECT DATA: Amount of data

□ GENERAL TOOL CHARACTERISTICS: Runtime OS (Windows, MacOS, iOS, Linux, Proprietary)

□ GENERAL TOOL CHARACTERISTICS: Bootable from removable media

□ GENERAL TOOL CHARACTERISTICS: Memory requirements

□ GENERAL TOOL CHARACTERISTICS: Processing speed (before analysis can begin)

□ PRE-ANALYSIS FEATURES: Write-blocking

□ PRE-ANALYSIS FEATURES: Data-at-rest acquisition

□ PRE-ANALYSIS FEATURES: Live memory acquisition

□ PRE-ANALYSIS FEATURES: Indexing

□ PRE-ANALYSIS FEATURES: Hash verification (Individual file or whole disk)

□ PRE-ANALYSIS FEATURES: Decryption/Decoding of Obfuscated data

□ PRE-ANALYSIS FEATURES: Bypass passwords

□ PRE-ANALYSIS FEATURES: Advanced (e.g., Rebuild RAIDs, acquire from cloud, VMs, enterprise discovery)

□ PARSING CAPABILITIES: File types (Multimedia, documents, databases, archives, executables, etc.)

□ PARSING CAPABILITIES: File artifacts (PCAPs, logs, VMs, Internet History, etc.)

□ PARSING CAPABILITIES: OS Artifacts (Registry, plists, sqlite databases, etc.)

□ PARSING CAPABILITIES: Inactive data (Unallocated space, deleted items, slack space, etc.)

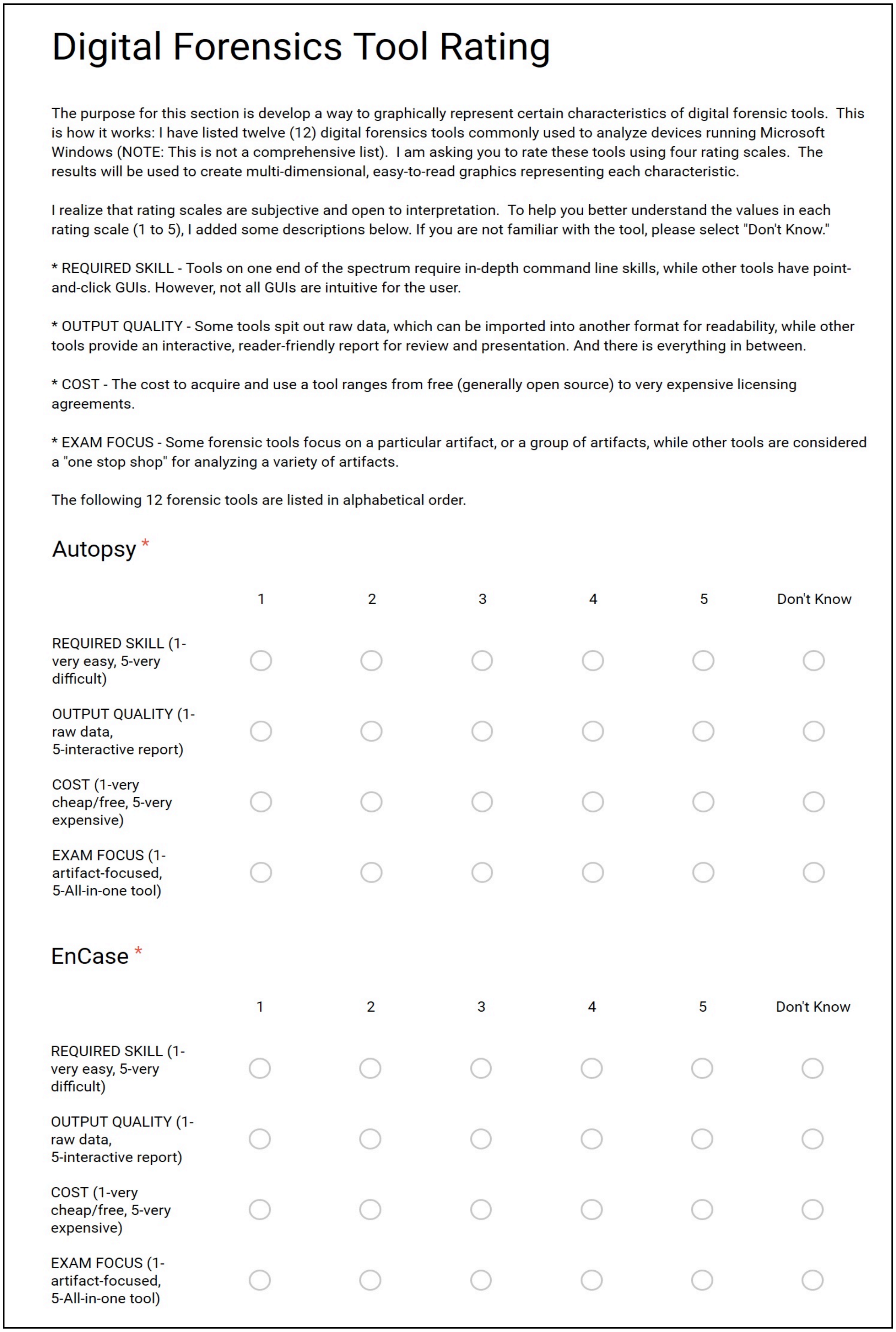
□ Other...

Comments (optional):

Long answer text

Appendix C

Phase Three Survey Form (excerpt)



Digital Forensics Tool Rating

The purpose for this section is develop a way to graphically represent certain characteristics of digital forensic tools. This is how it works: I have listed twelve (12) digital forensics tools commonly used to analyze devices running Microsoft Windows (NOTE: This is not a comprehensive list). I am asking you to rate these tools using four rating scales. The results will be used to create multi-dimensional, easy-to-read graphics representing each characteristic.

I realize that rating scales are subjective and open to interpretation. To help you better understand the values in each rating scale (1 to 5), I added some descriptions below. If you are not familiar with the tool, please select "Don't Know."

* REQUIRED SKILL - Tools on one end of the spectrum require in-depth command line skills, while other tools have point-and-click GUIs. However, not all GUIs are intuitive for the user.

* OUTPUT QUALITY - Some tools spit out raw data, which can be imported into another format for readability, while other tools provide an interactive, reader-friendly report for review and presentation. And there is everything in between.

* COST - The cost to acquire and use a tool ranges from free (generally open source) to very expensive licensing agreements.

* EXAM FOCUS - Some forensic tools focus on a particular artifact, or a group of artifacts, while other tools are considered a "one stop shop" for analyzing a variety of artifacts.

The following 12 forensic tools are listed in alphabetical order.

Autopsy *

	1	2	3	4	5	Don't Know
REQUIRED SKILL (1-very easy, 5-very difficult)	○	○	○	○	○	○
OUTPUT QUALITY (1-raw data, 5-interactive report)	○	○	○	○	○	○
COST (1-very cheap/free, 5-very expensive)	○	○	○	○	○	○
EXAM FOCUS (1-artifact-focused, 5-All-in-one tool)	○	○	○	○	○	○

EnCase *

	1	2	3	4	5	Don't Know
REQUIRED SKILL (1-very easy, 5-very difficult)	○	○	○	○	○	○
OUTPUT QUALITY (1-raw data, 5-interactive report)	○	○	○	○	○	○
COST (1-very cheap/free, 5-very expensive)	○	○	○	○	○	○
EXAM FOCUS (1-artifact-focused, 5-All-in-one tool)	○	○	○	○	○	○