A Grounded Theory Approach to Identifying and Measuring Forensic Data Acquisition Tasks

Gregory H. Carlton, Ph.D.
California State Polytechnic University
Pomona, California USA
ghcarlton@csupomona.edu

ABSTRACT

As a relatively new field of study, little empirical research has been conducted pertaining to computer forensics. This lack of empirical research contributes to problems for practitioners and academics alike.

For the community of practitioners, problems arise from the dilemma of applying scientific methods to legal matters based on anecdotal training methods, and the academic community is hampered by a lack of theory in this evolving field. A research study utilizing a multi-method approach to identify and measure tasks practitioners perform during forensic data acquisitions and lay a foundation for academic theory development was conducted in 2006 in conjunction with a doctoral dissertation.

An overview of the study's findings is presented within this article.

Keywords: computer forensics, digital forensics, forensic data acquisition, forensic protocol, grounded theory

1. INTRODUCTION

As a relatively new field of study, little empirical research has been conducted pertaining to computer forensics. (Fong *et al.*, 2005) This lack of empirical research contributes to problems for practitioners and academics alike. For practitioners, forensic examiners are expected to obtain training pertaining to this field; however, the existing procedural instruction is largely based on anecdotal contributions. Likewise, little theory has been developed by the academic community to aid in the development of this field.

Practitioners have a responsibility to apply scientific methodology, as the courts regard practitioners that examine computer data as forensic scientists, a classification of expert witnesses. (Nute, 1996) provides the following definition:

> Forensic Scientist - A person whose profession is applying scientific principles to produce information for purposes of the legal system. Examinations are based on the knowledge and skill of the expert when applying the scientific method to the tangible results, commonly termed evidence, produced by individuals interacting with the environment.

In addition to the problems presented pertaining to practitioners regarding the lack of empirical research, the academic community lacks theoretical tools for computer forensics.

From a theoretical perspective, no known model has been established as a basis for researchers desiring to develop forensic protocols for other areas of computer forensics or even other disciplines of forensic science. The lack of models to aid protocol development has been noted in academic literature, specifically, "The procedures and standards for developing an examination protocol have not been articulated, at least in forensic science literature."(Nute, 1996) The establishment of such a model should be a valuable tool that will make a significant contribution to the advancement of forensic science.

A doctoral dissertation was completed in 2006 utilizing a multi-method approach to identify and measure tasks practitioners perform during forensic data acquisitions and lay a foundation for academic theory development (Carlton, 2006a). The initial phase of this study was based largely on Grounded Theory (Glaser and Strauss, 1967) to identify tasks forensic examiners perform during forensic data acquisitions and to identify conditions which lead forensic examiners to perform or omit individual tasks. Upon achieving theoretical saturation in the study's initial, inductive phase, additional data were collected to empirically measure the extent to which examiners perform the set of identified tasks. Lastly, using a discursive analytic strategy, two expert review panels were interviewed to provide merit ratings for each of the identified tasks.

In addition to the perceived academic value associated with this study is an output primarily addressed to practitioners. A monograph titled "Forensic Data Acquisition Task Performance Guide – The Identification and Measurement of a Protocol for the Forensic Data Acquisition of Personal Computer Workstations – Introductory Edition" (Carlton, 2006b) presents the tasks and measures obtained from this study in a format designed to support expert testimony by forensic computer examiners.

2. METHODOLOGY

The research design method used in this research study was based on multiple methods performed in two research phases. The first phase utilized Grounded Theory (Glaser & Strauss, 1967) to identify tasks forensic examiners perform pertaining to the data acquisition of personal computer workstations through the use of a series of questionnaires.

The second phase of this study utilized review panels of experts, namely a panel of technical experts and a panel of legal experts, to evaluate the merit of each task identified in the first phase of this study. Based on Grounded Theory, the conceptual model of this research design is illustrated in Figure 1.

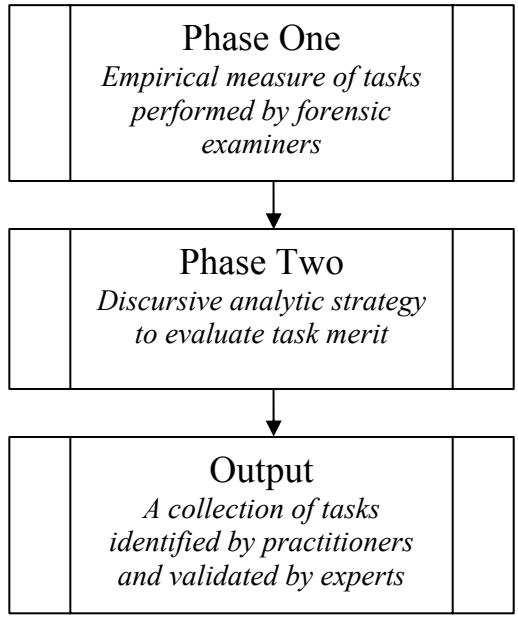

Figure 1 – Research design

2.1. Phase One

Without the benefit of preexisting literature on which to pose a hypothesis, Grounded Theory provided an approach to collect data in a series of surveys that eventually led to an emergence of tasks (Glaser, 1998). This design utilized a series of questionnaires distributed in an iterative approach, which began with open-ended questioning techniques and progressed to more narrowly focused questions with each iteration of the questionnaires (Dick, 2005). The data gathered in response to a questionnaire were used to define or refine categories presented in the subsequent questionnaire.

During the first phase of this study, the membership of the High Technology Crime Investigation Association (HTCIA) was surveyed through a series of five web-based questionnaires. The web-based instruments offered efficiency, and they have been shown to provide comparable results with other survey modes (Denscombe, 2006). Participants were randomly selected from the full, international membership of the HTCIA as of December, 2005. Selected members were sent e-mail invitations requesting their participation in the survey, access to the web-based questionnaires required user authentication, and controls within the website limited each authorized user to submit a single, complete response to the selected questionnaire.

The initial questionnaire, Questionnaire A, used open-ended questions to gather data from respondents without prejudice of established categories, conditions, or tasks, and a listing of the questions contained within it is presented in Appendix A (Borgatti, 2005). Respondents were requested to elaborate on their responses to the open-ended questions within free-from text fields. Also, the number of individuals selected for participation in Questionnaire A was not predetermined; instead, groups of twenty randomly selected HTCIA members were asked to participate in Questionnaire A, and the data were analyzed after each of fourteen groups of twenty members were collected. The fourteen iterations of data collection for Questionnaire A were necessary to reach a point of theoretical saturation whereby no additional task categories or constraint conditions were identified (Glaser, 1992). Overall, ten task categories and eight constraint conditions were identified from the data collected, and these categories and conditions formed the basis for the questions presented in Questionnaire B.

Questionnaire B presented the categories and constraint conditions identified above and within each category and constraint condition, this questionnaire asked respondents open-ended questions to encourage directed elaboration. Questionnaire B was organized to identify the conditions that lead forensic examiners to perform more tasks, perform tasks more rigorously, perform tasks less rigorously, and perform fewer tasks. Additionally, for each of these four conditions, Questionnaire B asked respondents to describe the tasks they add, perform more rigorously, perform less rigorously, or omit. An analysis of the data collected from responses to Questionnaire B resulted in the development of Questionnaire C, and similarly, an analysis of the data collected from responses to Questionnaire C led to the development of Questionnaire D.

The comprehensive analysis of data collected through the first four questionnaires, Questionnaire A through Questionnaire D, achieved theoretical saturation resulting in a set of 103 forensic data acquisition tasks and eight constraint conditions. These tasks and constraint conditions are discussed in more detail in section 3 of this article, and a complete listing of the tasks is located in Appendix B – Tasks. These 103 forensic data acquisition tasks and eight constraints were also presented in the final questionnaire of phase one of this study, Questionnaire E.

Questionnaire E consisted of closed-ended questions to identify two primary aspects of forensic data acquisition task performance. The first primary question measures the extent to which forensic examiners perform each task. For each of the 103 tasks respondents were asked to select from one of four choices concerning task performance. The choices were: (1) do not perform the task, (2) typically do not perform the task, but may perform it in some cases, (3) typically perform the task, but may omit it in some cases, and (4) always perform the task.

The second primary question measures the extent to which each of the eight identified constraining conditions affect forensic examiners' performance of each of the 103 tasks. To address this question, the Questionnaire D presented the listing of the eight constraining conditions after each task and asked respondents to identify each of the conditions that led them to add or omit the corresponding task. The response rates all of the questionnaires are presented in Table 1.

Table 1 – Questionnaire response rate

Questionnaire	Sample Size	Number of Respondents	Non-Forensic Examiners	Invalid E-mail Addresses
Questionnaire A	280	46	14	22
Questionnaire B	200	19	4	21
Questionnaire C	200	25	2	20
Questionnaire D	100	11	0	10
Task Development Subtotal	780	101	20	73
Questionnaire E	1,700	195	46	237
Study Total	2,480	296	66	310

In summary, phase one of this study began with no preexisting tasks, categories, or constraints. Through a series of iterative questionnaires, beginning with open-ended questions and evolving into more narrowly focused and close-ended questions, a set of 103 tasks and eight constraining conditions emerged. Lastly, performance measures were obtained for each of the identified tasks and conditions.

2.2. Phase Two

Beginning with the set of tasks identified in the first phase of this study, the second phase evaluated the merit of each of the 103 tasks. Two review panels of experts were presented with the set of 103 tasks and asked to evaluate the merit of each task. One panel of experts was instructed to analyze the technical merits of each task, and the second panel of experts was instructed to analyze the legal merits of each task.

Both expert review panels were instructed to use the same scale when measuring each task. Each expert review panel member was provided with an electronic spreadsheet that presented the tasks and allowed them to select one of five choices for each task. Table 2 lists the choices available to the review panel of experts and the corresponding point value for each choice.

Table 2 – Review panel point ratings

Selection	Points
Absolutely Prohibited	0
Undesired	1
No contribution and no harm	2
Desired	3
Absolutely Essential	4

Each review panel of experts consisted of five members. The review panel of technical experts consisted of five HTCIA members that include a former President of the International HTCIA, the President of a local chapter of the HTCIA, an author of forensic application software and former officer with the HTCIA, an Associate Professor and Chair of the Computer and Digital Forensics major at a college, and a computer forensics manager with a major consulting firm.

The review panel of legal experts consisted of five attorneys with extensive experience in computer forensic cases. They include the Director of Office of Legal Counsel of a U.S. federal agency, a Managing Director for Discovery Services at a law firm and member of the American Bar Association's Digital Evidence Project Committee in 2005, a trial lawyer and certified computer forensic examiner that is also the author of a monthly column on computer forensics, a Senior Assistant District Attorney in Brooklyn, New York, and a Ph.D. and J.D. that is a member of the Office of Homeland Security Coordinating Council.

The results of the expert panel ratings were combined to provide three rating measurements for each task. A technical merit rating represents the average score assigned to each task by the review panel of technical experts. A legal merit rating represents the average score assigned to each task by the review panel of legal experts, and the overall merit rating represents the combined average score from both review panels of experts. The combined average score is analogous to an overall grade-point average (GPA) score assigned by academic institutions to measure performance in different subjects, and care was taken to ensure equal membership size among the different review panels to prevent skewing.

Overall, the methodology allowed a set of 103 tasks and eight constraining conditions to emerge from an empirical analysis and each task and condition was evaluated to determine relative performance measures and merit ratings.

3. FINDINGS

A review of the findings of this study reveals interesting observations within the data and positive contributions of immediate and potential future value for practitioners and academics. Among the interesting observations are two classifications of task measurements; those in agreement and those in conflict. As identified in section 2, different measurements were provided for each task, and it is interesting to note here that these different measurements were in conflict for some tasks. The contrary condition also occurred for some tasks, as the different measurements aligned in agreement. A collection of tasks with measurements in agreement and measurements in conflict is described below.

3.1. Task measurements in agreement

Numerous points of measurement are presented that represent the opinions of ten different experts and the combined performance measures from all of the survey respondents. Given the large number of input sources, it is interesting to identify the tasks that achieved widespread agreement pertaining to task performance measures. Three of the most notable tasks with high levels of agreement in their measurements are presented here.

The task with the highest level of alignment in its measurements was task number 39, and its description is, "document the system unit's manufacturer, model and serial number." Every member of the review panel of legal experts and four of the five members of technical experts indicated that this task is absolutely essential. The remaining member of the review panel of technical experts scored this task as being desired. Additionally, 91% of the forensic examiners that responded to the survey indicated that they always perform this task, and 3% indicated that they typically perform this task. None of the respondents indicated that they do not perform this task, and only 1% indicated that they typically do not perform this task.

The description for task number 20 is, "determine whether the computer workstation is powered on." This task received an expert technical merit rating of 3.6, an expert legal rating of 3.8, and an overall expert rating of 3.7. Three members of the review panel of technical experts indicated that this task is absolutely essential, as did four members of the review panel of legal experts. The remaining members of both expert review panels indicated that this task is desired. 83% of the forensic examiners that responded to the survey indicated that they always perform this task, and an additional 8% indicated that they typically perform this task. Only 2% of the forensic examiners that responded to this survey indicated that they do not perform this task.

Task 75 has the description, "generate a MD5 hash value of the forensic image." Four members of the review panel of technical experts and three members of the review panel of legal experts indicated that this task is absolutely essential. The remaining panel members of both panels indicated

that this task is desired. Additionally 87% of the forensic examiners that responded to the survey indicated that they always perform this task, and an additional 2% indicated that they typically perform this task. 4% of the respondents indicated that they do not perform this task, and 2% indicated that they typically do not perform this task.

3.2 Task Measurements in Conflict

It is interesting to compare the measurements associated with task 75 to those of task 76, described as, "generate a SHA-1 hash value of the forensic image." The SHA-1 hashing algorithm is arguably more reliable than the MD5 hashing algorithm; however, this task received significantly lower measures in each category. Three members of each expert review panel indicated that this task is absolutely essential. One member on each panel indicated that this task is desired and one member on each panel indicated that this task makes no contribution. Additionally, 33% of the forensic examiners that responded to the survey indicated that they do not perform this task, and 27% indicated that they typically do not perform this task. Another 27% indicated that they always perform this task, and 8% indicated that they typically perform this task. The conditional performance measure of this task with the highest measure is the type of case, as it was identified by 15% of the respondents. Table 3 lists the measurements for tasks 75 and 76 for comparison.

Table 3 – MD5 and SHA-1 task measurement comparison

Measurement	MD5	SHA-1
Overall Merit Rating	3.7	3.4
Technical Merit Rating	3.8	3.4
Legal Merit Rating	3.6	3.4
Do Not Perform	4%	33%
Typically No	2%	27%
Typically Yes	2%	8%
Always Perform	87%	27%
Legal Limitations	9%	3%
Temporal Limitations	1%	3%
Financial Limitations	0%	1%
Corroborating Information	4%	4%
Technical Ability of Suspect	0%	2%
Physical Condition of Computer	1%	3%
Type of Case	6%	15%
High/Low Profile	1%	2%

Another task that received conflicting measurements is task 28, and it has the following description, "if the computer workstation is powered on, determine the type of operating system in use prior to selecting the power off method." Two members of the review panel of technical experts indicated conflicting opinions regarding this task, as one indicated that this task is absolutely essential while the other indicated that it is absolutely prohibited. Continuing this controversy, two other members of this panel indicated that this task is undesired while the remaining member indicated that it is desired. The review panel of legal experts contributed to the conflict surrounding this task, as two members of the legal panel indicated that this task is undesired, two members indicated that this task is desired, and the remaining panel member indicated that the task provides no contribution and no harm. The forensic examiners that responded to the survey further contributed to this conflict, as 33% of them indicated that they do not perform this task while 35% indicated that they always perform it. 17% of the responding forensic examiners indicated that they typically perform the task while 10% indicated that they typically do not perform the task.

Task 79 received conflicting opinions from expert panel members within and between the panels. One member in each expert review panel indicated that this task, described as, "perform a visual comparison of the directory structure of the image and the suspect disk to verify that the image is readable," is absolutely essential. In contrast, one member of the review panel of technical experts indicated that this task is absolutely prohibited. Three members of the review panel of legal experts and two members of the review panel of technical experts indicated that this task is desired while one member on each panel indicated that it makes no contribution or harm. The responding forensic examiners were fairly balanced on this issue, as 31% indicated that they always perform this task and 31% indicated that they do not perform this task. 20% indicated that they typically do not perform this task and 13% indicated that they typically perform it.

3.3 Summary of Findings

An analysis of the data collected during the first phase of this study resulted in the emergence of a set of 103 forensic data acquisition tasks. Additionally, a set of eight constraints were identified whereby forensic examiners may choose to add tasks, omit tasks, perform tasks more rigorously, or perform tasks less rigorously. The data collected during the second phase of the study yielded three sets of merit ratings for each task, namely a technical merit rating, a legal merit rating, and an overall merit rating.

In the preceding sections, three tasks with highly aligned measurements were discussed and three tasks with conflicting measurements were discussed. It is interesting to note that the complete analysis of the study identified more than twice as many tasks with conflicting measurements as were identified with

aligning measurements. Of particular interest are the differences between the indicated performance of practitioners and the opinions of experts within this field. Likewise differences in opinions between expert panels and/or difference among experts within panels were observed in over ten percent of all of the tasks identified. Forensic examiners practice their trade by delivering expert opinions within the legal system, and the differences in opinions observed in this study raise questions concerning the consistency of tasks performed by forensic computer examiners. This suggests the need for additional research to identify potential problems and to discover solutions to those problems.

This study achieved its objectives of providing a practical application for forensic computer examiners, demonstrating the applicability of the Grounded Theory Method in theory development of protocols in computer forensics and establishing a foundation for future research. As a result of the successful identification and measurement of the forensic data acquisition tasks, the research model is suggested as a model for advancement by future researchers.

4. LIMITATIONS

Although significant practical and theoretical value may be realized from the results of this study, there are numerous limitations concerning potential bias in the data collected, output derived from a limited sample size, the scope of usefulness in the application of the protocol, and theoretical limitations. These limitations are discussed below.

First, this study limited its survey population to the HTCIA. Although the HTCIA is the largest known international organization of forensic examiners, it represents only a portion of the entire population of forensic examiners. Furthermore, members of the HTCIA must accept the organization's policy of not working for the defense in criminal cases. This condition places bias in the study population that may impact the data collected.

Additional concerns were realized from the survey of HTCIA members in the area of respondent bias. Foremost is the limitation derived from generating the output of this study based on responses from 11.5% of those randomly selected. After the survey responses were collected from the study's website, an e-mail message was sent to the non-responders requesting them to provide reasons for not responding. Table 4 contains a listing of the reasons non-respondents provided for not participating in the study. Based on self-rated responses, no identified differences were observed in respondents and non-respondents regarding experience, training, or education.

Another limitation of this study concerns the size of the expert review panels. The relatively small size of these panels presents an opportunity for an individual panel member to skew the merit ratings on any task. Additionally, an individual continued to agree to participate through every follow-up contact,

but failed to submit his or her response worksheet prior to the deadline for completion of this study. This resulted in the inclusion of an alternate panel member's responses. The alternate panel member was identified within the list of potential panel members provided by the Chair of the ABA's Digital Forensics Project, the same list that other panel members were selected from. The credentials of the alternate panel member are comparable with the other experts.

Table 4 – Reasons provided by non-respondents

Description	Quantity
Responses received	160
Do not perform data acquisitions	56
Auto-reply out-of-office	33
Invalid e-mail addresses	17
Time constraints (too busy)	17
Vacation/travel/training	10
Could not find HTCIA member number	8
Did not trust	5
Spam blocker	3
Could not get past the survey login screen	2
Did not see e-mail	2
No longer a member of the HTCIA	1
Too much e-mail	1
Did not check e-mail within time period	1
Did not attempt to participate	1
Intended to participate and forgot	1

The tasks identified within the protocol are not implied to represent a comprehensive set of tasks forensic examiners perform pertaining to the forensic data acquisition of personal computer workstations. This set of tasks is limited to those that were identified by respondents of this study. Additionally, no conditional logic regarding the performance of tasks is suggested nor is the sequence of the performance of tasks.

Regarding theoretical limitations, this study used a multi-method approach based on the Grounded Theory Method and based largely on constructs defined by (Nute, 1996). This approach is bound by the constructs of legal and technical (i.e. computer science) merit. Further refinement of this approach may yield a more comprehensive protocol, as described in the following section on future research directions.

Lastly, although this study gathered data from international forensic examiner members of the HTCIA, all of the expert panel members were from the United

States of America. This limitation raises two concerns, one of internal validity within this study, and the second pertaining to the influence of a U.S. legal perspective in the merit ratings.

5. DIRECTIONS FOR FUTURE RESEARCH

Upon the completion of this study, numerous research questions are observed. First, to address some of the limitations described in the preceding section, it may be beneficial to repeat this study with a larger sample size and larger review panels; however, care must be taken regarding the use of larger panel sizes to ensure that the quality of expertise is not diluted. Additionally, a more complete understanding of the tasks and task conditions is likely to emerge if these larger sample sizes and larger review panels include the perspective of legal defense, as well as legal prosecution.

The author is currently considering repeating this study on an annual basis to provide revised versions of the protocol. Hopefully, as practitioners recognize useful characteristics of this protocol and familiarity with it increases, a larger number of forensic examiners will participate in future studies. Furthermore, a longitudinal study is also possible if a stream of annual editions of this study is performed.

It would also be useful to test this methodology on other aspects of forensic data acquisition protocols, such as servers. On a more generalized level, testing the methodology on other aspects of computer forensics protocols, such as analysis should also prove to be interesting.

On interest concerning a general theory perspective, testing the methodology on other aspects of forensic protocol development, not computer related may prove interesting, as well.

On a smaller scale, much information remains to be analyzed from the data collected within this study. Several interesting questions remain unanswered. These unanswered questions pertain to determining correlations between examiner status and task performance. Finally, this study acknowledges numerous task measurements in agreement and task measurements in conflict, and it would be worthwhile to examine these further to develop a better understanding within this area.

APPENDIX A – QUESTIONNAIRES

Questionnaire A:

1. Do you perform forensic data acquisitions?
2. Please describe the information you request about a new computer forensic case before beginning work on the case.
3. Please describe the tasks you typically perform pertaining to the forensic data acquisition of a personal computer workstation.

4.. Considering forensic data acquisition cases with exactly the same technical configuration, are there circumstances regarding a particular case that lead you to perform more tasks than you typically perform?

4A. If yes, please list the conditions that would lead you to perform more tasks than you typically perform.

4B. If yes, Considering those cases where you perform more tasks than you typically perform, please describe the additional tasks you perform beyond those tasks you typically perform.

5. Considering forensic data acquisition cases with exactly the same technical configuration, are there circumstances regarding a particular case that lead you to perform some tasks more rigorously than you typically perform?

5A. If yes, please list the conditions that would lead you to perform tasks more rigorously than you typically perform.

5B. If yes, Considering those cases where you perform tasks more rigorously than you typically perform, please describe the tasks you perform more rigorously than those tasks you typically perform

6. Considering forensic data acquisition cases with exactly the same technical configuration, are there circumstances regarding a particular case that lead you to perform some tasks less rigorously than you typically perform?

6A. If yes, please list the conditions that would lead you to perform tasks less rigorously than you typically perform.

6B. If yes, Considering those cases where you perform tasks less rigorously than you typically perform, please describe the tasks you perform less rigorously than those tasks you typically perform.

7. Considering forensic data acquisition cases with exactly the same technical configuration, are there circumstances regarding a particular case that lead you to perform fewer tasks than you typically perform?

7A. If yes, please list the conditions that would lead you to perform fewer tasks than you typically perform.

7B. If yes, Considering those cases where you perform fewer tasks than you typically perform, please describe the tasks you eliminate from those tasks you typically perform.

8. Please describe the type of organization in which you are employed.

9. Please describe your qualifications to perform computer forensic work.

10. How would you rate your ability to perform compute forensic work compared to other computer forensic examiners?

11. What factors do you consider to be good measures of a forensic examiner's qualifications?

Questionnaires B, C, and D utilized similar questioning techniques.

1. Do you perform forensic data acquisitions?

2. Considering information you request about a new computer forensic case prior to beginning work on the case please describe the information, if any, you request regarding:

   Authorization to conduct the forensic data acquisition:

   The location or locations involved:

   The purpose of the investigation:

   The issues pertaining to time:

   The technical issues:

   Any additional issues not listed above:

3. Please describe the tasks you typically perform, if any, concerning the forensics data acquisition of a personal computer workstation pertaining…

   To preparation:

   To the running state (i.e., the power on/off) of the computer:

   To the date and time:

   To the physical examination (i.e., inspection) of the computer:

   To documenting and/or photographing:

   To imaging storage media:

To the verification (i.e., hash) that the image was acquired successfully:

To the treatment of suspect media after an image is created:

To concluding tasks:

To any differences between a field acquisition and a lab acquisition:

Please describe any other tasks you typically perform that were not listed above:

Questions 4, 5, 6, and 7 repeat the following suite of questions based on the following respective conditions: more tasks, tasks more rigorously, tasks less rigorously, and fewer tasks.

4. Considering forensic data acquisition cases with exactly the same configuration, do you perform more tasks than you typically perform …

   If the case involves a specific purpose?

   Based on corroborating information?

   If the case involves legal limitaions?

   If the case involves time limitations?

   Based on the technical ability of the suspect?

   Based on the type of case?

   If the case involves a high profile situation?

   Based on the physical condition of the computer?

   Please describe any other conditions that lead you to perform more tasks than you typically perform:

   Considering those cases where you perform more tasks than you typically perform, please describe the additional tasks you perform beyond those tasks you typically perform.

APPENDIX B - TASKS

Task	Task Description
1	Purchase new target drives.
2	Wipe target disk drives.
3	Verify target disk drives are wiped.
4	Initialize and format target disk drives.
5	Prepare and verify toolkit – ensure equipment is fully functional.
6	Prepare and verify toolkit – ensure that all necessary hardware connectors and adapters are fully stocked.
7	Prepare and verify toolkit – ensure that all consumable items are fully stocked (bags, tags, forms, and log books).
8	Add additional items to forensic toolkit based on pre-acquisition intelligence from requestor.
9	Obtain latest versions, releases, or updates for forensic software tools.
10	Test forensic software tools.
11	Create a write-blocking forensic boot floppy disk and/or CD.
12	Refer to checklist to ensure that all equipment is available prior to beginning the data acquisition.
13	Receive written authorization to proceed with the case.
14	Assign an identification code to the case.
15	Obtain instructions from requestor concerning covert or overt data acquisition.
16	Document preparation tasks in log book prior to beginning the data acquisition.
17	Follow procedures identified in the acquisition checklist.
18	View location of equipment prior to acquisition.
19	Document all items connected to the computer workstation.
20	Determine whether the computer workstation is powered on.
21	If the computer workstation is powered on, then reboot it.
22	If the computer workstation is powered on and the workstation's monitor is powered on and blank, move the mouse to terminate the screen saver.
23	If the computer workstation is powered on and the workstation's monitor is powered on and blank, press the space bar to terminate the screen saver.
24	If the computer workstation is powered on, examine it prior to powering it down to determine whether encryption may be in use.
25	If the computer workstation is powered on, perform a RAM dump.
26	If the computer workstation is powered on, collect volatile data.

Task	Task Description
27	If the computer workstation is powered on, perform a live acquisition.
28	If the computer workstation is powered on, determine the type of operating system in use prior to selecting the power off method.
29	If computer workstation is powered on, photograph the displayed image shown on the workstation's monitor.
30	If computer workstation is powered on, determine the programs currently running.
31	If the computer workstation is powered on, power off the unit by using the operating system shutdown method.
32	If the computer workstation is powered on, power off the unit by pulling the electrical cord from the rear of the system unit.
33	If the computer workstation is powered on, power off the unit by pressing and holding the power-on button until the system unit is powered off.
34	If the computer workstation is powered off, leave it off until storage media is removed.
35	If the computer workstation is powered off, power it on.
36	Determine the current date and time from a reliable source.
37	Document the current date and time in log book.
38	Look for any potential devices detrimental to individual or evidence safety.
39	Document the system unit's manufacturer, model and serial number.
40	Photograph the system unit, including identifying information regarding manufacturer, model, and serial number.
41	Photograph the inside of the system unit.
42	Photograph all sides of the computer system.
43	Photograph the entire area surrounding the seized computer systems.
44	Sketch a diagram of the computer system with reference to its location and connections in log book.
45	Document the identity of individuals present at the scene of data acquisition.
46	Document the system components in the log book.
47	Document the manufacturer, model, and serial number of all storage media in the log book.
48	Document any irregularities, modifications or damage to the computer equipment.
49	Remove the hard disk drive(s) from the system unit.

Task	Task Description
50	Photograph the hard disk drive(s) taken from the system unit including identifying information regarding manufacturer, model, and serial number(s).
51	Document the pin settings of hard disk drive(s) in log book.
52	Photograph the pin settings of hard disk(s).
53	Remove diskettes from the system unit.
54	Remove CDs from the system unit.
55	Remove thumb drives from the system unit.
56	Disconnect all USB devices from the system unit.
57	Identify any network connections, and document findings.
58	Identify any telephone modem connections, and document findings.
59	Identify and document all peripherals attached to system unit.
60	Identify and document all peripherals available to the system unit through wired or wireless network connections.
61	Assign lab inventory numbers to each item seized and document in log book.
62	Document number of hard drives, size and disk geometry.
63	Using a write-protected method, preview contents of the suspect computer to determine whether an image of the suspect computer is necessary.
64	Filter data based on attorney-client privilege prior to imaging.
65	Seize external storage devices.
66	Seize documentation, manuals, and miscellaneous notes found in the proximity of the suspect computer system.
67	Connect the suspect hard disk to a hardware, write-blocking device, and obtain an image onto the target media using a forensic computer system.
68	Ensure that the suspect computer will boot from a software, write-blocking forensic diskette or CD, replace the hard disk in the system unit, and obtain an image using a network crossover cable method to a target disk attached to a forensic computer.
69	Install a known disk controller card in the suspect computer, connect the target disk drive to the disk controller card, boot the suspect computer with software write-protection forensic tools, and create an image to the target drive using the suspect computer.
70	Use EnCase to obtain an image of suspect media.
71	Use AccessData's FTK to obtain an image of suspect media.
72	Use Safeback to obtain an image of suspect media.

Task	Task Description
73	Use SPADA 3 to obtain an image of suspect media.
74	Use UNIX/Linux dd command to obtain an image of suspect media.
75	Generate a MD5 hash value of the forensic image.
76	Generate a SHA-1 hash value of the forensic image.
77	Allow the forensic software used for imaging to automatically calculate a MD5 hash value and then verify the MD5 hash value.
78	Perform a visual comparison using a hex editor to ensure that byte swapping or sector rotation did not occur during imaging.
79	Perform a visual comparison of the directory structure of the image and the suspect disk to verify that the image is readable.
80	With storage media removed, power on suspect computer system and document the date and time settings from BIOS.
81	With storage media removed, power on suspect computer system and determine the boot sequence settings from BIOS.
82	Media is reinstalled in suspect computer system.
83	Suspect media is preserved in its original condition and sealed.
84	PCs are returned to original condition and tested for functionality if on-site.
85	Suspect computer system is returned to the submitting agency.
86	Suspect media is placed in a secure storage area or evidence vault.
87	Image sets are placed in a secure storage area or evidence vault.
88	Suspect media is tagged with chain-of-custody labels.
89	Suspect media is replaced in suspect computer system, but data and power cables are not attached to suspect media.
90	A label is placed on the suspect computer system to prevent powering on unit.
91	Suspect media is placed in an anti-static bag and stored inside a manila envelope in the lab.
92	Suspect media is stored in an offsite, confidential storage facility.
93	If instructed to do so, the equipment is returned as close as possible to the original condition after imaging is complete.
94	Create a restore image of the suspect media onto a new disk to be returned to the owner.
95	Create a clone copy of suspect media for analysis.
96	Write handwritten reports to document all activity performed during the data acquisition.
97	Print computer generated reports to document all activity performed during the data acquisition.

Task	Task Description
98	Issue a receipt for the items seized.
99	Make sure all items are identifiable by serial number or applied number/tag.
100	Archive image to DVDs.
101	Make additional copies of images for attorneys.
102	Request a written data destruction form to be sent to suspect if drive contains objectionable material.
103	During a field acquisition, obtain signed waiver from owner indicating that forensic image is now the “best evidence.”

REFERENCES

Borgatti, S. (2005). Introduction to grounded theory. Retrieved 9/19/05, 2005, from http://ww.analytictech.com/mb870/introtoGT.htm

Carlton, G H (2006a). *A protocol for the forensic data acquisition of personal computer workstations*. Unpublished doctoral dissertation. University of Hawaii.

Carlton, G.H. (2006b). *Forensic data acquisition task performance guide: The identification and measurement of a protocol for the forensic data acquisition of personal computer workstations*. Unpublished manuscript.

Denscombe, M. (2006). Web-based questionnaires and the mode effect: An evaluation based on completion rates and data contents of near-identical questionnaires delivered in different modes. *Social Science Computer Review*, 24(2), 246-254.

Dick, B. (2005). Grounded theory: A thumbnail sketch. Retrieved 9/19/05, 2005 from http://www.scu.edu.au/schools/gcm/ar/arp/grounded.html

Fong, I. K., Paul, G., Prounis, M., Faraci, M., Ford, G.T., & Herman, L. (2005), *ABA digital evidence project survey on electronic discovery trends and proposed amendments to the federal rules of civil procedure – preliminary report*: ABA.

Glaser, B.G. (1992). *Basics of grounded theory analysis: Emergence vs forcing*. Mill Valley, CA: Sociology Press.

Glaser, B.G. (1998). *Doing grounded theory analysis: Issues & discussion*. Mill Valley, CA: Sociology Press.

Glaser, B.G., & Strauss, A.L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. New York: Aldine Publishing Co.

Nute, H.D. (1996). *A scientific basis for forensic science.* Unpublished doctoral dissertation, The Florida State University.