THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 5 | Number 1 Article 1

2010

Identifying a Computer Forensics Expert: A Study to Measure the Characteristics of Forensic Computer Examiners

Gregory H. Carlton
California State Polytechnic University

Reginald Worthley
University of Hawaii

Recommended Citation

Carlton, Gregory H. and Worthley, Reginald (2010) "Identifying a Computer Forensics Expert: A Study to Measure the Characteristics of Forensic Computer Examiners," *Journal of Digital Forensics, Security and Law*: Vol. 5 : No. 1 , Article 1.
DOI: https://doi.org/10.15394/jdfsl.2010.1069
Available at: https://commons.erau.edu/jdfsl/vol5/iss1/1

Identifying a Computer Forensics Expert: A Study to Measure the Characteristics of Forensic Computer Examiners

Gregory H. Carlton
California State Polytechnic University
Computer Information Systems Department
College of Business Administration
USA
ghcarlton@csupomona.edu

Reginald Worthley
University of Hawaii
Shidler College of Business
USA
worthley@hawaii.edu>

ABSTRACT

The usage of digital evidence from electronic devices has been rapidly expanding within litigation, and along with this increased usage, the reliance upon forensic computer examiners to acquire, analyze, and report upon this evidence is also rapidly growing. This growing demand for forensic computer examiners raises questions concerning the selection of individuals qualified to perform this work. While courts have mechanisms for qualifying witnesses that provide testimony based on scientific data, such as digital data, the qualifying criteria covers a wide variety of characteristics including, education, experience, training, professional certifications, or other special skills. In this study, we compare task performance responses from forensic computer examiners with an expert review panel and measure the relationship with the characteristics of the examiners to their quality responses. The results of this analysis provide insight into identifying forensic computer examiners that provide high-quality responses.

1. INTRODUCTION

The relatively new field of Digital Forensics is rapidly expanding as courts recognize the ubiquitous nature of information technology and benefits it provides in the form of evidence in criminal and civil matters. Along with this rapid growth in the usage of digital forensics is a growth in the number of individuals that perform work as forensic computer examiners. As the number of forensic computer examiners increase, it is natural to consider issues regarding the qualifications and abilities of those that practice within this field. Data collected reveal that there is a wide variety of academic attainment, related work

experience, professional training, and levels of certification among forensic computer examiners (Carlton 2007a).

Given the variety of education, training, and experience among forensic computer examiners, it is useful to obtain a better understanding of the factors that contribute to a computer forensics expert. This study is the first in a line of research seeking to map the determinants of computer forensics experts. Given the limitations of current research methods, establishing causal elements will require the analysis of relevant experiments; however, we are able to measure the extent to which relationships exist within the primary data we have collected.

While this study stops short of identifying the causal elements for determining an expert, it does identify characteristics of forensic computer examiners and measures the extent to which these characteristics relate with preferred responses provided by a panel of recognized experts. These findings provide more insight into the qualifications of an expert than the Daubert criteria, which is currently utilized by the courts to evaluate the credentials of expert witnesses. Additionally, these findings provide a foundation for additional research aiming to validate the causal elements that contribute to determining a computer forensics expert.

Data were collected from a random sample of members of the High Technology Crime Investigation Association (HTCIA), and the responses from those that indicated that they performed forensic data acquisitions were compared against responses from an expert review panel consisting of five recognized computer forensics experts and five attorneys with experience in digital forensic matters. A prior article addressed issues regarding agreement and conflict among the experts (Carlton and Worthley 2009), whereas, this study measures the extent in which the responses of the forensic computer examiners correlate with those provided by the panel of experts. In addition to providing information regarding forensic data acquisition task performance, the respondents were asked to provide information concerning their education, training, certification, and experience, as well as, additional information, such as their age and gender. These measures allow us to evaluate the contribution these identified elements provide toward aligning the responses between the examiners and the panel of experts.

2. DATA COLLECTION

The initial idea to perform this study came from observations during a doctoral dissertation. While collecting data to identify and measure forensic data acquisition task performance, the primary author realized that by collecting additional data at the time of the original study, a more thorough understanding of examiner qualifications might be achieved. Therefore, questions were added to the surveys to measure additional constructs beyond the scope of the initial dissertation (Carlton 2007b). These additional questions provide measures of forensic computer examiner characteristics and are used within this study to evaluate the extent to which they help explain traits of computer forensics experts. More specific information regarding the primary purpose for collecting the data,

the ancillary data collected, and questions derived from ancillary data analysis are presented in the following sections.

2.1 Primary purpose for collecting the data

The primary purpose for collecting the data was to identify and measure tasks forensic computer examiners perform during the forensic data acquisition of personal computer workstations, and this study was the focus of a doctoral dissertation (Carlton 2007b). To accomplish this, forensic computer examiners that were members of the HTCIA were surveyed to identify the tasks they perform when conducting a forensic data acquisition, and they indicated the extent to which they performed each of the identified tasks.

A series of five questionnaires evolved through Grounded Theory (Glaser and Strauss, 1967) that identified one hundred three (103) forensic data acquisition tasks performed by the respondents. The respondents indicated the extent to which they performed each task on a scale consisting of four choices. Those four choices were: always perform the task; typically perform the task, but may omit it; typically omit the task, but may perform it; and never perform the task. Additionally, respondents indicated conditions that lead them to perform a task they would otherwise omit or omit a task they would otherwise perform.

Data were also collected from two expert review panels concerning the set of 103 tasks identified by the forensic computer examiners. An expert review panel of attorneys with experience in computer forensics evaluated the set of 103 tasks from the legal perspective, and an expert review panel of recognized expert forensic computer examiners evaluated the set of 103 tasks from a technical perspective.

An analysis of this data was performed resulting in two primary results, one addressing the academic study of this field and the other addressing matter relevant to practitioners in the field of digital forensics. The first was a validation of Grounded Theory as a method to address the study of Computer Forensics where little or no theoretical research had occurred previously. The second result was a task performance guide that is of interest to practitioners and provided the first empirical study of forensic data acquisition task performance (Carlton 2006).

As the data were collected for the primary purpose stated above, additional questions were included in the surveys to measure constructs ancillary to the primary objective of the initial study. A discussion of these ancillary data is presented in the following section.

2.2 Ancillary data collected

While the initial focus for collecting data targeted constructs to identify tasks forensic computer examiners perform during data acquisitions and to obtain performance measurements of those tasks, we recognized that a richer understanding of examiner performance might be obtained by collecting ancillary

data through additional questions in the surveys provided to the forensic computer examiners. The constructs for these additional questions included examiner characteristics, including their professional credentials and personal attributes, such as age and gender. Additionally, a series of questions were included to identify and measure the factors that the respondents considered were indicators of forensic computer examiners' qualifications, and respondents were asked to provide a self-rating of their overall performance as a forensic computer examiner. Each of these ancillary constructs is described within this section.

Questions were included within the surveys to address constructs pertaining to the examiner characteristics associated with examiners' professional credentials, such as the highest level of educational attainment, levels of professional training, professional certifications, and industry relevant experience. Regarding relevant experience, respondents were asked to indicate the number of years they have worked as a forensic computer examiner, the number of times they have provided court testimony in matters regarding computer forensics, and the number of times they have provided depositions in matters regarding computer forensics. Respondents were asked to list their professional certifications and to indicate the number of professional training courses they have completed pertaining to computer forensics. Also, data were collected to determine the age and gender of the respondents and the type of organization in which they were employed.

As mentioned above, questions were included to identify and measure the factors that the respondents considered were indicators of forensic computer examiners' qualifications. Grounded Theory was again used during the iterations of the first four surveys to identify eleven factors, and the fifth survey then asked the respondents to measure the extent to which they thought each factor was a good indicator of a forensic computer examiner's qualifications based on a five-point scale ranging from "not important" to "essential." Nine of the eleven factors identified are qualities in which individuals can be measured as having a quantity of the factor based upon a scale, and these factors are: experience, training, certification, formal education, character, reputation, aptitude, methodology, and skill. The remaining two factors identified are attributes in which individuals either possess the attribute or not. The first of these attributes concerns whether the examiner has worked as a trainer in the field, and the second attribute indicates whether the examiner is a manger of other forensic computer examiners.

While the data collected through the primary questions provided an empirical measure of the tasks examiners perform, the data collected through the combination of the primary questions and the ancillary questions provide an opportunity to develop a better understanding of the characteristics of the examiners whose task performance more closely aligns with the views of the members of the expert review panels. The following section describes questions that were derived from reflections upon this combined data set.

2.3 Questions derived from ancillary data analysis

Beginning with the assumption that the responses provided by the members of the expert review panels represent desired responses, it is relatively straightforward to deduce that those examiners whose responses more closely align with the responses provided by the expert review panels are better qualified than the examiners whose responses largely deviate from those of the expert review panels. Therefore, within this study, we will use the term "*quality response*" to indicate a response provided by the expert review panels. Given this assumption, we are drawn to consider the characteristics of the examiners to determine whether any relationship exist that would help identify highly qualified forensic computer examiners or unqualified forensic computer examiners.

First, we considered the characteristics that are consistent with the Daubert criteria, namely education, professional training, relevant work experience, and certifications. Several questions surface here, for example, do the examiners whose responses more closely align with the experts possess a higher level of formal education than the examiners whose responds largely deviate from the experts? Similar questions are presented for each of the data variables collected from the survey responses, and a listing of the questions are presented in Table 1 - Questions derived from an analysis of ancillary data.

Table 1 - Questions derived from an analysis of ancillary data

Questions
Does a relationship exist between formal education and quality responses?
Does a relationship exist between professional training and quality responses?
Does a relationship exist between relevant work experience and quality responses?
Does a relationship exist between professional certifications and quality responses?
Does a relationship exist between age and quality responses?
Does a relationship exist between gender and quality responses?

The data collected pertaining to the factors that examiners indicated were good measures of forensic computer examiners' qualifications also provided an opportunity to observe whether there were relationships between the attributes an examiner possesses and the factors he or she indicated to be important. For example, do forensic computer examiners with relatively low education and relatively high experience rate experience as a more desired factor than do those with the opposite characteristics? Similarly, do examiners without professional certifications rate certifications as a less desired factor than do those with numerous or prestigious certifications? Also, we consider the self-rating data collected to determine whether examiners accurately reflect their abilities compared to quality responses. The general questions that arise are presented in Table 2 – Questions derived from examiners' ratings of qualification measures.

Table 2 – Questions derived from examiners' ratings of qualification measures

Question
Does a relationship exist between the characteristics examiners possess and the qualities that they indicate are measures of a qualified examiner?
Does a relationship exist between examiners' self-rating and quality responses?

Answers to these questions should yield valuable contributions to the study and practice of the field of Digital Forensics. These contributions are presented in the following section.

3. CONTRIBUTIONS OF ANCILLARY DATA ANALYSIS

The ability to observe measureable characteristics to help distinguish qualified forensic computer examiners from those that are not is valuable from several perspectives. Immediately obvious is the value to those that are seeking to obtain the services of a forensic computer examiner, as this ability should make a contribution to the selection process. This should also lead to a corrective market adjustment within the forensic computer examiner community, as examiners will seek to obtain the characteristics that make them more valuable within their profession, thus a higher quality supply of forensic computer examiners will emerge.

A better understanding of the characteristics associated with qualified examiners will be of value to various government organizations as they address issues regarding licensing regulation. Currently, due to a lack of understanding of computer forensics, a few state governments within the United States have enacted laws requiring forensic computer examiners to obtain some type of private investigator license (Lonardo, et. al., 2008). Information concerning the correlation of examiner characteristics and quality responses is useful to lawmakers that seek to improve industry regulations.

A thorough understanding of the correlation of examiner characteristics and quality responses will also be of value to further research in this field. The current set of characteristics and their associated correlation data offer a solid foundation for additional testing that should help identify a more comprehensive set of characteristics and eventually lead to the development of a theory or a model that demonstrates causality and identifies the determinates of a qualified, forensic computer examiner. While there are several steps yet to be completed to achieve this goal, this study does provide the first step in this direction.

As listed above, several valuable contributions are obtained from a better understanding of the correlations of examiner characteristics and quality responses. To achieve this understanding, we analyzed the data collected and tested a series of hypotheses based on the questions presented in section 2.3. Our analysis and findings are described in the following section.

4. ANALYSIS AND FINDINGS

Data used in this study were collected from forensic computer examiners and two expert review panels as described in section 2 above. Data collected from the expert review panels addressed task performance, whereas, the examiner response data addressed three areas: task performance, examiner characteristics, and examiners' ratings of qualification measures. Our approach to systematically analyze the data consisted of first determining a rating procedure for the forensic computer examiners, then applying this rating to each examiner. Next we looked for correlations between characteristics of forensic computer examiners and examiner performance. Details of our analysis and findings are described below:

4.1 Procedure to rate forensic computer examiners

Our first step in the analysis of this data was to compare the expert review panel members' task performance measures with the task performance measures provided by the forensic computer examiners. This comparison required several data conditioning steps to be taken before we undertook a direct comparison.

First, the responses from the expert review panel members and the forensic computer examiners for each of the 103 forensic data acquisition tasks included on the questionnaire, as described in section 2.1, were coded with numeric values. We coded the task response data from the expert review panel members into ordinal variables as shown in Table 3 - Expert task performance measures. Similarly, we coded the task response data from the forensic computer examiners as shown in Table 4 - Examiner task performance measures.

Table 3 - Expert task performance measures

Value	Expert task performance
0	Absolutely prohibited
1	Undesired
2	No contribution & no harm
3	Desired
4	Absolutely essential

Table 4 - Examiner task performance measures

Value	Forensic computer examiner task performance
0	I do not perform this task
1	I typically do not perform this task, but I perform it in some cases
2	I typically perform this task, but I omit it in some cases
3	I always perform this task

We examined the responses from the expert review panels and selected a subset of 29 tasks in which the experts were mostly in agreement. This analysis of the expert review panel data resulted in several interesting observations, including some serious potential consequences in legal matters involving expert testimony of computer forensics experts, and we have documented our findings in a previous article (Carlton and Worthley 2009). Substantial agreement among the experts was found in 18 tasks where they indicated "absolutely essential" (i.e., 4) was the correct response. For another nine tasks, they indicated that "desired" (i.e., 3) was the proper response. Our method eliminated the highest and lowest expert ratings, and then we checked whether at least 75% of the remaining eight agreed. Each examiner was assigned an agreement match with the experts' collective response if they responded with a response of "typically perform this task" (i.e., 2) or "always perform this task" (i.e., 3). The number of agreements for the totality of examiners in the study ranged from six (6) to twenty-seven (27), and the distribution is shown in Table 5 - Examiner rating scores.

4.2 Rating the forensic computer examiners

We determined performance ratings using letter grades from A to F for each examiner based on their alignment with the experts' ratings, as shown in Table 5 - Examiner rating scores. We then assigned a letter grade to each examiner, as summarized in Table 6 - Examiner rating grades. The letter grade of A was assigned to examiners that agreed with the experts on 25 or more of the 27 tasks. The examiners that agreed with the experts on 22, 23, or 24 of the 27 tasks received a grade of B, those that agreed with the experts on 19, 20, or 21 of the tasks received a grade of C, those that agreed on 17 or 18 tasks received a grade of D, and those that only agreed with the experts on 16 or fewer of the 27 tasks received a grade of F.

Table 5 - Examiner rating scores

Score	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6
Number	9	7	14	8	12	7	4	8	4	4	2	1	0	1	1	0	1	0	0	0	0	1

Table 6 - Examiner rating grades

Examiner grades	Percent	Score to get grade	Scores	Number of Examiners
A	90%	24.3	25-27	30
B	80%	21.6	22-24	27
C	70%	18.9	19-21	16
D	60%	16.2	17-18	6
F	<60%	<16.2	6-16	5

Once examiners were assigned grades based on their agreement with the expert review panel members, we then focused on determining characteristics associated with high or low grades.

4.3 Relationship between examiner characteristics and examiner performance

After obtaining an examiner performance ranking, as described in sections 4.1 and 4.2 above, we next sought to identify characteristics possessed by forensic computer examiners that were related to their quality of performance. In other words, we wanted to identify the extent to which attributes of forensic computer examiners related to their performance ratings. A logical starting point for this analysis is based on the factors of the Daubert criteria, such as, education, training, certification, and experience.

Using the data collected, attributes for employer and education were easily available for analysis; however, additional filtering of the data was necessary to extract appropriate attributes for professional certification. Respondents were asked to indicate the names of the certifications they held, and we determined that many of the certifications listed were of general computer knowledge (e.g., A+ Certification), and not specifically for the practice of Computer Forensics. We then identified a subset of the certifications listed by the respondents that specifically addressed the practice of Computer Forensics, or closely aligned with the practice, and assigned an attribute name of "CF certification" to this subset. The professional certifications that were included in the CF certification set include, in alphabetical order: CCCI, CCE, CCFT, CFCE, CIFI, CISSP, and EnCE. In addition to attributes for employer, education, and CF certifications, we included gender as an attribute of forensic computer examiners in our analysis.

The results of our initial analyses are summarized in Table 7 - Nonparametric tests for differences in examiner agreement with experts, and based on the attributes of employer, education, gender, and CF certification, only CF certification yielded a significant correlation with examiner performance.

Table 7 - Nonparametric tests for differences in examiner agreement with experts

Characteristic	Test	Statistic	P-value
Employer	Kruskal-Wallis	H = 1.39	0.498
Education	Kruskal-Wallis	H = 1.70	0.637
Gender	Mann-Whitney	U = 146.5	0.213
CF certification	Mann-Whitney	U = 2212	0.014

The dependent variable is the number of agreements with the experts (i.e., the examiner rating scores shown in Table 5 - Examiner rating scores). The test results shown in Table 7 - Nonparametric tests for differences in examiner agreement with experts test the null hypotheses of no differences between the specific characteristic categories with respect to examiner rating scores. All null hypotheses are accepted except for the condition where an examiner has at least one of the computer forensics professional certifications (i.e., CF certifications). Examiners with CF certifications have a higher agreement with the experts. Therefore, the data indicate that the type of employment, education, and gender have no significant bearing on an individual's agreement with the experts, whereas, forensic computer examiners that possess one or more CF certifications provided responses that align more closely with the expert review panel.

As shown in Table 8 - Percent of factor in each grade group, we use the grading system as a mechanism for trying to differentiate between examiners that did well in agreeing with the experts and those that did not. For example, within the groupings of forensic computer examiners for each grade, 47% of the A group had one of more of the CF certifications, while 26%, 19% and 18% of the B, C, and D/F groups had the CF certification characteristic respectively. It is interesting that the trend indicates a direct relationship between CF certification and agreement with the experts.

Other noteworthy observations include the characteristic of expert testimony. There is a direct relationship between providing expert testimony ten or more times and achieving a good grade (i.e., high alignment with the expert review panel), and there is an inverse relationship between providing expert testimony zero times and achieving a good grade. It also is interesting to notice the characteristics for those that received grades of D or F when comparing those employed by a law enforcement agency and those employed by private industry. Similarly, notice the comparison between those that have taken twenty of more courses with those that have taken eight or fewer courses for the same grade, This interesting observation of D or F grades occurs again between those examiners that provided a self-rating of excellent compared with those that provide a self-rating of below average. While interesting, these observations occur only at the D or F grade, and not across the range of grades from A to F, whereas, the CF certification and expert testimony observations occur across the range of grades.

As shown in Table 9 - Spearman rank correlations of agreement with experts, we use the actual agreement score (6 to 27) and report a rank correlation with all the characteristics that can be ranked. Four of the characteristics show significant association with agreement with experts. All of the correlations are interpreted in a similar manner, where positive correlations indicate that higher values of a given characteristic are associated with higher values on the agreement index (i.e., more agreement with the experts).

Table 8 - Percent of factor in each grade group

Characteristic	**A**	**B**	**C**	**D or F**	**Total**
Sample size	***30***	***27***	***16***	***11***	***84***
Employed by law enforcement agency	50.0%	66.7%	68.8%	0.0%	52.4%
Employed by private industry	36.7%	33.3%	31.3%	72.7%	39.3%
Highest education is Graduate degree	23.3%	29.6%	6.3%	18.2%	21.4%
Highest education is Bachelor's degree	46.7%	29.6%	62.5%	63.6%	46.4%
Gender (Male)	100%	88.9%	93.8%	90.9%	94.0%
Has certifications (two or more)	36.7%	29.6%	12.5%	18.2%	27.4%
Has at least one CF certification	46.7%	25.9%	18.8%	18.2%	31.0%
Testified as expert (ten times or more)	23.3%	14.8%	6.3%	0.0%	14.3%
Testified as expert (zero times)	30.0%	29.6%	43.8%	54.5%	35.7%
Provided depositions (ten times or more)	33.3%	18.5%	25.0%	18.2%	25.0%
Provided depositions (zero times)	36.7%	44.4%	50.0%	36.4%	41.7%
Taken courses (twenty courses or more)	40.0%	29.6%	31.3%	18.2%	32.1%
Taken courses (eight courses or less)	23.3%	33.3%	37.5%	72.7%	35.7%
Self-rating of excellent	33.3%	11.1%	18.8%	0.0%	19.0%
Self-rating of below average	3.3%	0.0%	6.3%	27.3%	6.0%
Age (years)	46.8	43	44.8	44.3	44.9
Experience (years)	8.9	6.9	6.1	7	7.5

Table 9 - Spearman rank correlations of agreement with experts

Characteristic	**Coefficient**	**P-Value**
Age	0.096	0.387
Experience (Years)	0.082	0.458
Testify	0.246	0.024
Depositions	0.170	0.123
Courses	0.219	0.046
Total number of certifications	0.263	0.016
Self-Rating	0.297	0.006

4.4 Analysis of examiner self-ratings of qualifications and actual characteristics

We initially hypothesized that examiners would tend to rate qualities they possess as being more important than qualities they do not possess. The results shown in Table 10 - Spearman rank correlations between forensic computer examiners' ratings of qualifications and actual characteristics confirm that the reason examiners rate certain qualifications highly is that the examiners, themselves, posses the characteristic or related characteristic. The few that do not have significant results do not really have a related measure to check, for example, character, reputation, methodology and skill. Indicated in bold are the measures

with the largest values, representing, for example, that those that claim to have taken the most courses think training, certification, and education are good measures of an examiner, while those that indicated that they have higher levels of education think education is a good measure of a forensic computer examiner, and those that have the most certifications think that experience and certifications are good measures of a forensic computer examiner. Those that provided self-rating scores indicating that they consider themselves among the best examiners think that being a trainer is a good measure of a forensic computer examiner. Similarly, years on the job tracks with trainers, number of times expert testimony is provided tracks with trainers, the number of depositions provided and number of courses taken. Those that claim to have provided the largest number of depositions think that being a manager is an important measure of a forensic computer examiner. Notice that gender is coded as a dummy variable (i.e., males coded as one and females coded as zero); therefore, the negative 0.218 indicates that as gender is higher (i.e. male) the reputation rating is lower. In other words, reputation is considered to be a more important measure by females than males.

Table 10 - Spearman rank correlations between forensic computer examiners' ratings of qualifications and actual characteristics

Characteristic	Q-Exper	Q-TC	Q-Cert	Q-Ed	Q-Char	Q-Rep	Q-Apt	Q-Meth	Q-Skill	Q-Train	Q-Mgr
Years	0.142	0.053	-0.061	0.133	-0.167	0.093	-0.121	-0.072	-0.054	**0.290**	0.130
Testify	0.132	-0.008	0.036	0.080	-0.116	-0.054	-0.040	-0.049	-0.051	**0.227**	0.117
Depositions	0.120	-0.130	-0.066	0.056	-0.099	0.028	-0.061	0.025	0.016	**0.219**	0.330
Courses	0.137	**0.309**	**0.226**	**0.220**	-0.045	0.126	-0.162	0.079	0.008	**0.257**	0.143
Education	-0.084	-0.003	0.114	**0.409**	-0.182	0.001	-0.075	0.039	-0.052	0.051	-0.001
Age	-0.021	0.095	-0.064	0.068	-0.131	0.130	-0.078	-0.104	-0.144	0.023	-0.038
Gender	0.008	-0.081	0.060	-0.006	-0.137	**-0.218**	0.094	-0.112	-0.024	-0.121	-0.083
Total Certs	**0.252**	0.116	**0.455**	0.151	0.016	0.021	-0.135	0.015	-0.068	-0.053	-0.065
Self-Rate	-0.011	-0.052	0.053	0.198	0.175	0.089	0.126	0.036	0.036	**0.279**	0.112

Characteristic	Q-Exper	Q-TC	Q-Cert	Q-Ed	Q-Char	Q-Rep	Q-Apt	Q-Meth	Q-Skill	Q-Train	Q-Mgr
Years	0.021	0.637	0.585	0.232	0.130	0.404	0.277	0.516	0.627	**0.008**	0.242
Testify	0.233	0.941	0.745	0.471	0.296	0.629	0.720	0.661	0.646	**0.039**	0.291
Depositions	0.281	0.241	0.554	0.615	0.372	0.801	0.584	0.824	0.884	**0.046**	**0.002**
Courses	0.216	**0.004**	**0.040**	**0.045**	0.684	0.257	0.143	0.478	0.946	**0.019**	0.199
Education	0.451	0.977	0.305	**0.000**	0.100	0.996	0.501	0.723	0.643	0.646	0.990
Age	0.850	0.395	0.563	0.544	0.781	0.240	0.483	0.352	0.195	0.836	0.731
Gender	0.942	0.467	0.587	0.960	0.219	**0.047**	0.399	0.312	0.827	0.275	0.457
Total Certs	**0.022**	0.298	**0.000**	0.172	0.887	0.847	0.223	0.893	0.539	0.632	0.561
Self-Rate	0.925	0.638	0.635	0.072	0.114	0.422	0.256	0.743	0.744	**0.011**	0.312

5. CONCLUSIONS

Upon completing our analysis we are able to identify several factors regarding the correlation of characteristics of forensic computer examiners and their quality responses. Along with our observations are several significant limitations that

must be recognized concerning our study, and details of these observations and limitations are presented below along with our view concerning the need for continuing research on this topic.

5.1 Summary of observations

Our overall goal was to identify characteristics that contribute to the identification of a forensic computer examiner of high quality. To achieve this goal, we performed an extensive analysis on data collected from forensic computer examiners and an expert review panel. We compared the responses of the forensic computer examiners with those from the expert review panel on each of 103 different forensic data acquisition tasks to determine a quality performance ranking among the forensic computer examiners, and once we achieved this performance ranking, we then measured the correlation between characteristics of the forensic computer examiners with their quality performance rankings.

The results of our analysis show that the possession of a professional certification specifically within the field of Computer Forensics is the characteristic that best correlates with quality responses among the characteristics we measured. We also found that, to a lesser degree, the number of times expert testimony has been provided by the forensic computer examiner may also help identify quality responses. However, we did not observe any significant relationship between quality responses and professional computer certifications not specifically addressing the field of Computer Forensics. Likewise, we did not observe any significant relationship between quality responses and formal education, years of experience, number of professional training courses taken, type of employment, self-rating, age, or gender.

5.2 Limitations

Several limitations regarding the scope and methodology of this study must be recognized to ensure that the findings and conclusions are viewed in the proper context. As with many studies utilizing statistical methods, we must recognize the limits of a relatively small sample size of forensic computer examiner respondents and the weight associated with the panel of experts consisting of ten members. Another limitation is our premise that the alignment between the responses from examiners with those from the expert review panel is desired. Additional, significant limitations are discussed below.

The most significant limitation of this study concerns the scope of the computer forensic tasks measured. While this study performed an extensive analysis concerning the relationship between tasks forensic computer examiners perform compared with the responses provided by an expert review panel, it is important to recognize that only tasks pertaining to the forensic data acquisition of personal computer workstations were measured. Although the forensic data acquisition of personal computer workstations represents a significant subset of tasks performed by forensic computer examiners, it does not include any of the numerous and

potentially more significant data analysis tasks, nor does it include tasks concerning forensic reporting or the forensic data acquisition of digital devices other than personal computer workstations (i.e., servers, cell phones, etc.).

Similar to the methodological limitations concerning the tasks analyzed within this study are the categories for examiner characteristics. These characteristics, such as types of certifications and employment, evolved from the data collected using Grounded Theory. While other certifications exist, or have been introduced to the marketplace since the data were collected, only those certifications and employment categories that were contained with our data were analyzed.

A limitation concerning the methodology of this study surfaces regarding the association of a quality response and a forensic computer examiner that performs high quality work. It is reasonable to deduce that a forensic computer examiner whose responses to questions align more closely with the responses provided by the expert review panel has a better understanding of the procedures than does a forensic computer examiner whose responses deviate significantly from those provided by the expert review panel; however, selection of a correct task response does not indicate that the forensic computer examiner performs the task correctly. Therefore, care must be taken when drawing conclusions that those forensic computer examiners that agree with the panel of experts are of high quality.

An additional significant limitation of this study is found with the constraints of the methodology used. While our goal of achieving a better understanding of identifying forensic computer examiners of high quality was achieved as we sought to identify relationships between characteristics of forensic computer examiners and their quality responses, it must be recognized that this study does not indicate causality. We are not attempting to determine the factors that yield a high-quality forensic computer examiner within this study, as we are merely identifying characteristics associated with high-quality, forensic computer examiners within the limitations described above.

5.3 Call for additional research

As identified within the limitations presented in section 5.2, this study focuses on identifying a high-quality forensic computer examiner based on observed relationships in the survey data, not causal factors. The study of Computer Forensics would benefit from additional research that would yield the identification of the determinants for a high-quality, forensic computer examiner. We think that this study will serve as a foundation for additional research, as we have analyzed characteristics identified through Grounded Theory that relate with quality responses. Future experiments utilizing these characteristics may determine whether these characteristics are causal factors or artifacts.

REFERENCES

Carlton, Gregory H., Forensic Data Acquisition Task Performance Guide – The Identification and Measurement of a Protocol for the Forensic Data Acquisition of Personal Computer Workstations, http://www.htcia.org, 2006.

Carlton, Gregory H., A Grounded Theory Approach to Identifying and Measuring Forensic Data Acquisition Tasks. Journal of Digital Forensics, Security and Law; Volume 2, Number 1, 35-56, 2007.

Carlton, Gregory H., A Protocol for the Forensic Data Acquisition of Personal Computer Workstations, ProQuest, Ann Arbor, Michigan, UMI 3251043, 2007.

Carlton, Gregory H., and Worthley, Reginald, An Evaluation of Agreement and Conflict Among Computer Forensics Experts, Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, p. 277, 2009.

Glaser, B.G., and Strauss, A.L., The Discovery of Grounded Theory: Strategies for Qualitative Research, Aldine Publishing Co., New York, 1967.

Lonardo, T., White, D., and Rea, A., To License or Not to License: An Examination of State Statutes Regarding Private Investigators and Digital Examiners. Journal of Digital Forensics, Security and Law; Volume 3, Number 3, 61-80, 2008.