Chapter 20

A SURVEY OF THE LEGAL ISSUES FACING DIGITAL FORENSIC EXPERTS

Sydney Liles, Marcus Rogers and Marianne Hoebich

Abstract This paper discusses the results of a survey focusing on the legal issues facing digital forensic experts in the United States. The survey attracted 71 respondents from law enforcement, academia, government, industry and the legal community. It extends the well-known Brungs-Jamieson research on attitudes and priorities of the Australian digital forensic community. The results are compared with those from the Brungs-Jamieson study to determine if digital forensic experts from different countries share priorities and concerns. Several differences are observed between stakeholder groups regarding the importance of specific legal issues. Nevertheless, the results indicate that, despite differing opinions, it is possible to find a common ground that can help craft public policy and set funding priorities.

Keywords: Legal issues, digital forensic experts, survey

1. Introduction

The primary purpose of digital forensics is to present digital evidence in legal proceedings. Therefore, the techniques employed to extract digital evidence from devices must comply with legal standards. However, due to the nature of the Internet, digital forensic investigations are not constrained by geographical boundaries and legal issues are complicated by the presence of multiple jurisdictions.

An electronic crime initiated in Australia can bring down a computer system in the United States (or vice versa). Consequently, it is important that there is a cohesive movement towards the acceptance of legal standards for digital evidence in international courts of law.

Jurisdictional issues are among the most common problems reported in the literature [2, 6, 10, 11]. Because cyber crime is not constrained

G. Peterson and S. Shenoi (Eds.): Advances in Digital Forensics V, IFIP AICT 306, pp. 267–276, 2009.

by territorial, state or national boundaries, there are often questions about the jurisdiction where the crime occurred and the agency with the authority to investigate and prosecute. International cooperation is a related issue – a cyber crime can occur anywhere in the world, have victims in different locations and leave trails of evidence that cross multiple national boundaries. The need to enact cyber crime laws on an international scale is an ongoing effort as is the need to improve cooperation among countries [10, 11]. Most researchers agree that new laws are probably not required as most nations and states have cyber crime laws. However, existing laws need improved definitions and clarification on several important points [2, 6, 10, 11].

Brungs and Jamieson [4] conducted research on the attitudes and priorities of the Australian digital forensic community. Their study, which identified seventeen legal issues in three categories (judicial, privacy and multi-jurisdictional), laid the groundwork for classifying legal issues related to digital forensics.

The Brungs-Jamieson study covered Australian telecommunications legislation, namely the Telecommunications Act of 1979 and its interpretation. The study identified the need to protect the privacy of individuals and businesses during investigations as a major challenge. Other researchers [7, 8, 11, 14] have also noted that this is a major issue in digital forensics.

The presentation of digital evidence in legal proceedings is another important issue. Because lawyers, judges and juries may have limited technical knowledge, the presentation of digital evidence must be done in a clear, easily understandable manner [3, 5, 8, 14]. Broucek and Turner [3] note that most legal professionals have a limited understanding of technology and tend to lack confidence in the ability of technical specialists to produce evidence that is admissible in a court of law.

Related work confirms the issues raised by Brungs and Jamieson concerning best practices, testing of digital forensic tools and expert witnesses. Numerous digital forensic techniques are used by investigators and examiners; however, no best practice guides are currently available. Also, there currently are no published error rates or testing results for digital forensic tools [5, 9, 12, 13]. The qualifications and skills of expert witnesses is also a serious issue. Meyers and Rogers [9] question whether one can be considered an expert based on the ability to use a tool or software package, but without the ability to clearly define how the tool works or without reviewing the source code. Attempts are underway to develop standards for expert qualifications [1, 12], but none exist at present.

Brungs and Jamieson identified many significant legal issues facing the discipline of digital forensics. However, while much has been written about the individual issues, little has been done to clarify the issues or to determine where the digital forensic community should focus its efforts. This study explores the same legal issues as Brungs and Jamieson, but in the context of the U.S. digital forensic community.

2. Brungs-Jamieson Survey

The Brungs-Jamieson study surveyed the attitudes and priorities of digital forensic experts in Australia. It identified seventeen key legal issues, which were divided into three categories: judicial, privacy and multi-jurisdictional. The study laid the groundwork for the classification of legal issues and the creation of a taxonomy. However, it appears that no follow-up research has been conducted related to the Brungs-Jamieson survey.

Brungs and Jamieson set out to accomplish two goals: (i) identify a set of legal issues facing digital forensics, and (ii) determine the importance of the identified issues to three stakeholder groups: police, regulators and consultants. A Delphi methodology was used to survey a panel of eleven Australian experts in order to identify the principal legal issues. After identifying seventeen issues, the experts were asked to rank them from 1 (highest priority) to 17 (lowest priority), and to rate each issue on a seven-point Likert scale from 1 (unimportant) to 7 (very important). All the issues were rated 3 or lower on an inverted scale from 1 (very important) to 7 (unimportant). The top five issues were "Jurisdictional," "Telecommunications Act covering data, "Interpretation of Telecommunications Act," "International cooperation in practice," and "Revision of mutual assistance." High concordance was observed between the importance ratings and average rankings, which was confirmed using a Kendall's W statistical test ($W = 0.974$, $p = 0.013$) [4].

The Brungs-Jamieson study also reported the average rankings of each issue by group. However, the method for determining this ranking was not reported. The average rankings were converted to ranks from 1 to 17 for comparison across groups.

3. Survey Methodology and Results

This study builds on the Brungs-Jamieson research by conducting a similar survey of digital forensic experts in the United States. The respondents included law enforcement, academics, government, industry and legal experts. The seventeen issues identified by Brungs and Jamieson were used to confirm and refine an initial taxonomy.

Our study involved a voluntary, anonymous, self-selecting web-based survey of digital forensic experts. The following issues were presented to the survey participants:

- **Issue 1:** Jurisdictional (state to state and federal to state)
- **Issue 2:** Computer evidence presentation difficulties
- **Issue 3:** Criminal prosecution vs. civil litigation
- **Issue 4:** International cooperation in legal practice
- **Issue 5:** Access and exchange of information
- **Issue 6:** Confidential records and business systems privacy
- **Issue 7:** Privacy protection for data transmission laws
- **Issue 8:** Privacy issues and workplace surveillance
- **Issue 9:** Interpretation of laws affecting digital evidence
- **Issue 10:** Preservation of privacy of clients during digital investigations
- **Issue 11:** Launching actions against persons unknown in civil litigation
- **Issue 12:** Requirement for best practices guides and standards
- **Issue 13:** Computer literacy in the legal sector
- **Issue 14:** Contrast of broadcast vs. communications
- **Issue 15:** Need to specify new offenses
- **Issue 16:** Testing of new tools and techniques
- **Issue 17:** Expert witness skills and qualifications

The respondents were asked to rank each of the seventeen issues using a five-point Likert Scale ranging from 1 (not important) to 5 (most important). The survey was accessed from a web page hosted by the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University from October 26, 2007 to November 20, 2007.

The survey was promoted by sending invitations to digital forensic professionals from around the United States. Emails were sent to authors of published research papers related to digital forensics and the law. A

link to the survey was also posted on technical forums on the Internet. Additionally, calls for participation were sent to companies, government agencies and universities with strong interests in information assurance and digital forensics.

A total of 71 respondents completed the online survey. The respondents were from law enforcement ($n = 13$), academia ($n = 26$), government ($n = 9$), legal/courts ($n = 3$) and commercial ($n = 20$).

Prior to analysis, the data was examined for accuracy, missing entries and the satisfaction of the assumptions for performing multivariate analysis. The data had no missing values. However, the answers provided by two respondents were found to be univariate outliers for six of the seventeen issues. Further examination revealed that all the answers provided by these two respondents had extreme values. The data provided by these two respondents was eliminated, leaving 69 responses for the final analysis.

In addition, Issue 11 (Launching actions against persons unknown in civil litigation) showed numerous outliers, which indicated considerable confusion among respondents about this issue. Issue 11 was therefore eliminated from further analysis.

Each of the remaining sixteen issues was treated as a variable of interest in the data analysis. Examination of skewness and kurtosis, the application of the Kolmogorov-Smirnov and Shapiro-Wilk tests, and visual inspection of histograms, box plots and Q-Q plots verified that the data was not normally distributed for any of the sixteen issues. Therefore, the data was analyzed using non-parametric statistical tests.

3.1 Survey Results

The Pearson and the Spearman correlation tests showed a significant correlation between Issue 4 (International cooperation in legal practice) and Issue 5 (Access and exchange of information) by group. In particular, Issue 4 had $r(67) = -0.320$, $p < 0.01$ (two-tailed) and $rs(67) = -0.334$, $p < 0.01$ (two-tailed). Issue 5 had $r(67) = 0.320$, $p < 0.01$ (two-tailed) and $rs(67) = 0.299$, $p < 0.05$ (two-tailed) by group.

A Kruskal-Wallis test was performed to determine the mean ranking of each issue by group. The results of the test (mean rankings) are shown in Table 1. A higher number indicates a higher ranking or greater importance as identified by the group. Note that Group 2 denotes law enforcement ($n = 13$), Group 3 denotes academia ($n = 25$), Group 4 denotes government ($n = 9$), Group 5 denotes legal/courts ($n = 3$) and Group 6 denotes commercial entities ($n = 19$).

Table 1. Kruskal-Wallis test results.

Issue		Group				
		2	**3**	**4**	**5**	**6**
1	Jurisdictional	41.15	31.64	43.83	21.83	33.11
2	Presentation Difficulties	32.88	40.30	41.39	12.00	20.08
3	Criminal vs. Civil	31.15	38.00	32.28	28.67	35.97
4	International Cooperation	42.04	39.24	33.11	39.33	24.82
5	Access and Exchange Information	29.46	32.66	24.61	34.00	46.95
6	Confidential Records	31.31	32.88	33.67	48.33	38.84
7	Data Transmission Privacy	41.46	33.50	32.72	41.00	32.68
8	Work Surveillance	32.92	38.80	40.67	40.67	27.84
9	Interpretation of Laws	33.54	33.12	40.67	60.00	31.84
10	Client Privacy	27.31	40.60	26.83	37.50	36.37
12	Best Practices	43.08	34.94	25.11	41.67	33.18
13	Literacy in Legal Sector	32.31	37.40	27.28	57.50	33.79
14	Broadcast vs. Communications	33.85	41.24	34.67	7.00	32.16
15	New Offenses	38.15	33.72	34.44	19.33	27.36
16	Testing of New Tools	31.19	35.86	37.94	22.33	37.08
17	Expert Witness	27.04	38.66	34.33	38.17	35.45

3.2 Analysis of Results

In order to permit a comparison with the Brungs-Jamieson results, the data was converted into a separated data set with scores ranging from 1 (very important) to 5 (unimportant). Kendall's W test was performed for the three groups (law enforcement, government and commercial) that were comparable to the Brungs-Jamieson groups. A one-to-one comparison of results was not possible because our study included two additional groups (academia and legal/courts), which are also legitimate stakeholders. Results corresponding to these additional groups will be included in future reports.

Table 2 compares the results of Kendall's W tests for our survey and the Brungs-Jamieson survey for the three common groups (law enforcement, government and commercial). Note that the non-parenthesized values in the table represent mean rankings while the values in parentheses correspond to issue rankings.

The results indicate that differences exist in the Kendall's W rankings for the two surveys. Both the actual values and the rankings show differences between groups. However, it is interesting to note that in both studies the law enforcement group ranked the need to specify new offenses fairly low (Rank 14 in our study and Rank 12 in the Brungs-Jamieson study). Also, the need for international cooperation

Table 2. Comparison of Kendall's W test results.

Issue	**Law Enforcement**		**Government**		**Commercial**	
	Liles	**B-J**	**Liles**	**B-J**	**Liles**	**B-J**
Jurisdictional	7.88(8)	7.00(5)	7.00(5)	4.75(3)	9.53(11)	8.67(7)
Presentation Difficulties	8.50(9)	5.67(3)	6.33(3)	5.50(4)	9.03(10)	9.00(9)
Criminal vs. Civil	11.50(15)	10.67(14)	11.78(15)	13.00(16)	10.34(12)	7.00(5)
International Cooperation	6.85(4)	5.33(2)	7.72(9)	3.25(1)	10.55(14)	9.67(10)
Access and Exchange Information	9.27(11)	6.00(4)	10.94(13)	6.75(7)	5.26(1)	12.33(14)
Confidential Records	7.08(5)	10.33(12)	6.67(4)	8.00(8)	5.68(2)	13.00(17)
Data Transmission Privacy	5.23(2)	10.00(10)	7.56(7)	6.50(6)	7.08(5)	6.00(3)
Work Surveillance	9.23(10)	7.33(7)	7.50(6)	10.25(11)	10.53(13)	4.00(1)
Interpretation of Laws	6.73(3)	4.33(1)	4.89(1)	4.25(2)	7.34(6)	5.00(2)
Client Privacy	9.96(12)	10.00(10)	10.06(12)	6.00(5)	7.92(8)	8.67(7)
Best Practices	5.08(1)	11.00(15)	9.33(11)	11.50(13)	7.42(7)	12.67(15)
Literacy in Legal Sector	7.42(7)	9.33(9)	8.94(10)	12.25(14)	7.03(4)	10.00(11)
Broadcast vs. Communications	12.50(16)	7.00(5)	12.33(16)	10.50(12)	12.92(16)	10.67(13)
New Offenses	11.46(14)	10.33(12)	11.33(14)	8.50(9)	11.11(15)	12.67(15)
Testing of New Tools	7.35(6)	8.67(8)	6.00(2)	10.00(10)	6.26(3)	6.67(4)
Expert Witness	9.96(13)	3.33(16)	7.61(8)	12.75(15)	8.00(9)	7.00(5)

was ranked fairly high (Rank 4 in our study and Rank 2 in the Brungs-Jamieson study).

The government groups in both studies gave high rankings to the interpretation of laws, presentation difficulties and jurisdictional issues. However, there was no agreement between the government groups regarding the issues that received low rankings.

On the other hand, the commercial groups in the two studies found some common agreement on the need to test new tools and to protect client privacy; they also agreed on low rankings for new offenses. Nevertheless, it is interesting to note that there is little, if any, agreement across groups regarding the importance of the sixteen issues.

4. Discussion

The results of the current study do indeed differ from those of the Brungs-Jamieson study. Unfortunately, the Brungs-Jamieson data set is not available (and it may not be detailed enough), so it is not possible to determine the factors responsible for the differences. Two possible reasons are the differing sizes of the data sets ($N = 69$ for the current data set while $N = 11$ for the Brungs-Jamieson data set) and the fact that the surveys were conducted in different countries. But these are mere speculation and additional research is required to fully explore this question.

The current study indicates marked differences between stakeholder groups regarding the rankings and, therefore, the importance of the sixteen legal issues. Based on the Kruskal-Wallis test results, the law enforcement group ranked best practices as the most important issue while the government group rated jurisdictional issues and the commercial group ranked access and exchange of information as the most important. This trend holds for the second and third ranked issues for each group. Law enforcement ranked international cooperation as the second most important issue while the government group ranked presentation difficulties and the commercial group ranked confidential records and business systems privacy as the second most important issue. The third ranked issues are privacy protection for data transmission laws in the case of the law enforcement group, privacy issues and workplace surveillance for the government group and the need to specify new offenses for the commercial group.

The rankings of two issues showed agreement across groups. The law enforcement and government groups ranked Issue 14 (Contrast of broadcast vs. communications) as the sixth most important issue; the commercial group ranked this issue twelfth. Issue 7 (Privacy protection

for data transmission laws) was ranked eleventh by the government and commercial groups, and third by the law enforcement group.

While some of the results differ from those of the Brungs-Jamieson study, the two studies share a common finding – stakeholder groups disagree on the importance of specific legal issues. This is expected because digital forensics is an interdisciplinary field with multiple stakeholder groups, each with different priorities regarding the legal issues.

5. Conclusions

Despite the exploratory nature of the survey and limitations in research design, the finding that law enforcement, government and commercial experts disagree on the importance of specific legal issues that face digital forensics is significant. In order to have effective governance and allocate limited resources, it is important to understand the priorities of all the principal stakeholders in the discipline of digital forensics. The study also suggests that, while the stakeholders disagree about the individual issues, it may be possible to find common ground if the issues are examined more broadly. For example, the top issues in this study (international cooperation, jurisdiction and access and exchange of information) should be examined for areas of overlap rather than just the differences. Identifying the common areas can assist in crafting public policy and in setting funding priorities.

References

[1] V. Baryamureeba and F. Tushabe, The enhanced digital investigation process model, *Proceedings of the Fourth Digital Forensic Research Workshop*, 2004.

[2] R. Broadhurst, Developments in the global law enforcement of cyber-crime, *Policing: International Journal of Police Strategies and Management*, vol. 29(3), pp. 408–433, 2006.

[3] V. Broucek and P. Turner, Bridging the divide: Rising awareness of forensic issues amongst systems administrators, presented at the *Third International System Administration and Networking Conference*, 2002.

[4] A. Brungs and R. Jamieson, Identification of legal issues for computer forensics, *Information Systems Management*, vol. 22(2), pp. 57–66, 2005.

[5] M. Carney and M. Rogers, The Trojan made me do it: A first step in statistical based computer forensics event reconstruction, *International Journal of Digital Evidence*, vol. 2(4), 2004.

[6] J. Conley and R. Bryan, A survey of computer crime legislation in the United States, *Information and Communications Technology Law*, vol. 8(1), pp. 35–58, 1999.

[7] N. King, Electronic monitoring to promote national security impacts workplace privacy, *Employee Responsibilities and Rights Journal*, vol. 15(3), pp. 127–147, 2003.

[8] R. Laubscher, D. Rabe, M. Olivier, J. Eloff and H. Venter, Computer forensics for a computer-based assessment: The preparation phase, *Proceedings of the Fifth Annual Information Security South Africa Conference*, 2005.

[9] M. Meyers and M. Rogers, Computer forensics: The need for standardization and certification, *International Journal of Digital Evidence*, vol. 3(2), 2004.

[10] F. Pocar, New challenges for international rules against cyber-crime, *European Journal on Criminal Policy and Research*, vol. 10(1), pp. 27–37, 2004.

[11] L. Reid, Expert opinion: Interview with Amanda M. Hubbard, J.D., Fulbright Scholar, former trial attorney, Computer Crime and Intellectual Property Section, U.S. Department of Justice, *Journal of Information Privacy and Security*, vol. 2(1), pp. 47–56, 2006.

[12] M. Reith, C. Carr and G. Gunsch, An examination of digital forensic models, *International Journal of Digital Evidence*, vol. 1(3), 2002.

[13] M. Saudi, An Overview of Disk Imaging Tools in Computer Forensics, InfoSec Reading Room, SANS Institute, Bethesda, Maryland, 2001.

[14] F. Witter, Legal Aspects of Collecting and Preserving Computer Forensic Evidence, InfoSec Reading Room, SANS Institute, Bethesda, Maryland, 2001.