On the Scientific Maturity of Digital Forensics Research

Martin Olivier, Stefan Gruner

Chapter 3

ON THE SCIENTIFIC MATURITY OF DIGITAL FORENSICS RESEARCH

Martin Olivier and Stefan Gruner

Abstract This paper applies a scientific maturity grade schema from the software engineering domain to research in the field of digital forensics. On the basis of this maturity schema and its grades, the paper classifies the current maturity of digital forensics research. The findings show that much more research conducted at higher levels of "scientificness" is necessary before the new field of digital forensics can be considered to be scientifically mature.

Keywords: Digital forensics, scientific maturity, software engineering

1. Introduction

The digital age has enabled and necessitated digital forensics as a means to maintain law and order in society. Forensic methods have occasionally failed those who were wrongfully convicted on the basis of low-quality evidence [14, 21]. In the past, the absence of strict scientific standards in some forensic practices has caused confusion about the reliability, validity, repeatability and accuracy of the outcomes, especially when the outcomes were presented in court, where the intended audience did not have the technical knowledge to judge the reliability of the presented evidence. Digital forensic scientists and practitioners have a duty to avoid repeating the mistakes of the past by scrutinizing the scientific maturity of their field, and by approaching and conveying evidence accordingly.

In a mature scientific field, the outcomes of processes can be trusted because they are constantly produced and reproduced in the course of "normal science." This trust is earned through the successful repeatability of processes, which render consistent, accurate, reliable and valid outcomes.

Digital forensics is still a developing field, and the question arises: Is it possible to assess the current level of "scientificness" in the field of digital forensics? We use the informal term "scientificness" to acknowledge the fuzziness of the concept of scientific maturity.

This paper presents a scientific maturity assessment of digital forensics using the Shaw [45] software architecture science maturity scale. The transfer of this maturity scale, from software architecture to digital forensics, is justified by the similarity of the problems, including the shortage of scientificness (which was experienced in the domain of software architecture more than a decade ago) and the impact claims that both fields have in the physical world.

The remainder of this paper presents the software architecture scientificness scale [45]. The scale is used to assess the scientificness of the digital forensics research presented at the first and sixth *IFIP WG 11.9 International Conferences on Digital Forensics* held in 2005 and 2010, respectively. From the assessment, statements about the progress that has been made in the field of digital forensics in its brief history are discussed.

2. Scientificness Software Engineering

In 1998, Snelting [47] published a lament about the shortage of scientificness in the field of software engineering. Snelting reminded the software engineering community about Popper's criterion of falsifiability, with a "slant" against the post-modernist intellectual fashion of socio-constructivism, and demanded more efforts towards the empirical validation of ideas and conjectures. However, Snelting's appeal for more scientificness did not take into account the gradual historic development of emerging academic subjects from the pre-scientific stage through the proto-scientific stage to the fully scientific stage.

In a later paper focusing on the software engineering sub-specialty of software architecture, Shaw [45] included the spectrum of pre-scientific to fully scientific stages. With reference to earlier work by Redwine and Riddle, Shaw [45] identified six typical stages in the historic development of an emerging subject of research, especially in technical science domains. These six stages are characterized by their drive towards practical applications and external usefulness:

- Early prospecting.
- Concept formulation.
- Development and extension.
- Internal enhancement.

Table 1. Dimension 1: Research setting [45].

Dimension	Setting Type	Typical Questions
1.a	Feasibility	Is there an X? Is X possible at all?
1.b	Characterization	What is X like? What do we mean by X? What are the important characteristics of X? What are the varieties of X, and how are they related?
1.c	Capability	How can I accomplish X? Is there a smarter way of accomplishing X?
1.d	Generalization	Is X always true of Y? Given X, what is Y?
1.e	Valuation	Is X more desirable than Y? How do I decide?

- External enhancement.
- Popularization.

Most relevant to this study is Shaw's three-dimensional maturity classification scheme. The three dimensions are:

- Research setting.
- Research product (approaches and methods).
- Result validation technique.

Tables 1, 2 and 3 show the ascending maturity values in each of these three dimensions of assessments (including some interpretative modification and adaptation).

Table entries where the classification criteria differ from Shaw [45] use Bunge's terminology [3, 4]. The concept of tabulating levels of quality is also related to maturity assessment schemas in other domains, such as CMMI for general organizational capabilities and TMMI for maturity assessment in the domain of systematic software testing.

Shaw [45] concluded that researchers "must attend to making existing results more robust, more rigorously understood, and more ready to move into application." That is because, to date, "we don't recognize what our research strategies are and how they establish their results. Poor external understanding leads to lack of appreciation and respect. Poor internal understanding leads to poor execution, especially of validation, and poor appreciation of how much to expect from a project or result. There may also be secondary effects on the way we choose what problems to work on at all."

It is outside the scope of this paper to critique the maturity classification scheme. Instead, we transfer Shaw's maturity schema and method

Table 2. Dimension 2: Research product [45].

Dimension	Product Type	Typical Approach or Method
2.a	Qualitative or descriptive model	Organize and report interesting observations. Suggest and argue for generalizations from examples. Structure a problem area and formulate the right questions. Analyze a system or a project in an informal manner.
2.b	Technique	Invent new ways to do some tasks, including procedures and implementation techniques. Develop a procedure for choosing among alternatives.
2.c	System of knowledge or engineering	Embody results in a systematic context. Use system development as a source of insight and carrier of further results.
2.d	Empirical predictive model	Derive predictions from observed data.
2.e	Analytic model or theory	Develop structured quantitative and/or symbolic theories that permit formal analysis and deep explanations.

Table 3. Dimension 3: Validation technique [45].

Dimension	Technique Type	Style of Argument
3.a	Persuasion	We suggest... We believe...
3.b	Implementation	Here we made a prototype that can do... Here we see one example that has...
3.c	Informal evaluation	Comparison of several objects against each other. Rule-of-thumb comparison against check-lists. Exploratory measuring or counting without theoretical backup.
3.d	Formal analysis	Logical and/or mathematical proofs, including mathematical statistics.
3.e	Systematic experience	Theoretically motivated experiments. Reliable reproduction of previously hypothesized or predicted phenomena

of analysis to the domain of digital forensics, with the goal of revealing how research in the field of digital forensics is suffering from the same issue that software architecture research faced a decade ago. Consequently, we also argue that Shaw's conclusion and request for future work, as quoted above, can be transferred from the domain of software engineering to the domain of digital forensics today.

3. Scientific Maturity of Digital Forensics

The survey of the state of scientificness in digital forensics research is divided into two parts. First, a large statistical overview of 46 papers is given in terms of Shaw's model of scientific maturity [45]. Second, reviewer feedback for the early papers and some recent calls for developments in digital forensics are discussed in order to qualitatively deepen the findings from the statistical overview.

3.1 Classification of Conference Papers

This subsection analyzes the papers presented at two *IFIP WG 11.9 International Conferences on Digital Forensics* and subsequently published in the Springer book series, *Advances in Digital Forensics*. Shaw's model of scientific maturity [45] is used in the analysis.

For the purpose of discussion, it is sufficient to look at the first conference volume [39] from 2005 with 25 contributions, and one recent (sixth) conference volume, Volume VI [6] from 2010 with 21 contributions. The exercise of browsing through all the papers in the seven-volume series (at the time of conducting this research) would merely reinforce the argument because the results are similar for Volumes II–V and VII as well as for related journals and conference proceedings. Table 4 shows the raw data for this survey.

Table 4 and Figure 1 show that in both 2005 and 2010, the majority of papers do not reach Level **d** in any of the categories. However, a trend exists towards better evaluation efforts – with comparatively more work in Category 3.c – from 2005 to 2010. The large number of papers in Category 2.b in combination with Categories 1.a or 1.c indicates that many authors in the field of digital forensics are working in an engineering mode in which a useful solution is the goal, and not a theoretical explanation. Combinations of Categories 1.b and 2.c are rare in the table; this indicates a scientific research mode with an interest in knowledge for its own sake. Figure 1 shows the shrinking of the lowest value "—a—" in all three quality categories from 2005 to 2010. However, a high value "—d—" rarely appears in 2010.

The raw data in Table 1 is used to create the formal concept lattice visualization in Figure 2, which presents the mutual relationships existing between the papers in an intuitive manner. Figure 2 shows the diversity of attribute combinations (e.g., "1.a—2.b—3.b") extracted from Table 4, from all the papers in 2005 and 2010. The sixteen circles in the lattice in Figure 2 represent sixteen different attribute combinations. Small circles denote rare combinations while large circles denote frequently occurring combinations.

Table 4. Classification of *IFIP WG 11.9 Conference* papers.

Year 2005 (Early)		Year 2010 (Recent)	
Paper	**Classification**	**Paper**	**Classification**
[2]	1.a—2.a—3.a	[38]	1.a—2.a—3.a
[33]	1.b—2.a—3.c	[7]	1.b—2.a—3.a
[10]	1.a—2.b—3.b	[51]	1.a—2.a—3.a
[27]	1.a—2.a—3.a	[25]	1.c—2.b—3.c
[26]	1.b—2.a—3.c	[8]	1.c—2.a—3.c
[17]	1.c—2.b—3.b	[54]	1.c—2.b—3.b
[35]	1.b—2.b—3.c	[1]	1.c—2.c—3.c
[11]	1.c—2.b—3.**d**	[31]	1.a—2.a—3.c
[23]	1.a—2.a—3.a	[22]	1.b—2.b—3.c
[12]	1.c—2.b—3.b	[15]	1.c—2.b—3.c
[44]	1.c—2.b—3.b	[18]	1.c—2.b—3.c
[40]	1.a—2.a—3.b	[42]	1.a—2.b—3.c
[19]	1.b—2.b—3.b	[24]	1.a—2.b—3.c
[20]	1.b—2.b—3.b	[32]	1.a—2.b—3.c
[28]	1.a—2.a—3.a	[41]	1.c—2.b—3.c
[52]	1.b—2.b—3.c	[43]	1.c—2.b—3.b
[48]	1.a—2.b—3.b	[50]	1.**d**—2.c—3.**d**
[13]	1.c—2.b—3.b	[49]	1.c—2.b—3.c
[9]	1.c—2.b—3.a	[30]	1.a—2.b—3.c
[37]	1.a—2.a—3.a	[53]	1.c—2.b—3.b
[36]	1.c—2.b—3.c	[16]	1.b—2.a—3.a
[5]	1.c—2.b—3.c	-	-
[34]	1.c—2.b—3.b	-	-
[46]	1.a—2.a—3.a	-	-
[29]	1.a—2.a—3.a	-	-

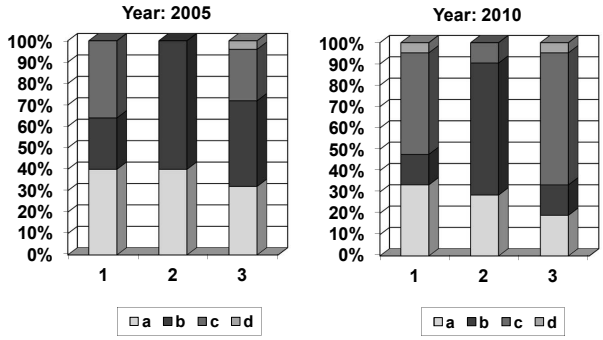

Figure 1. Shrinking of the lowest value in all three quality categories.

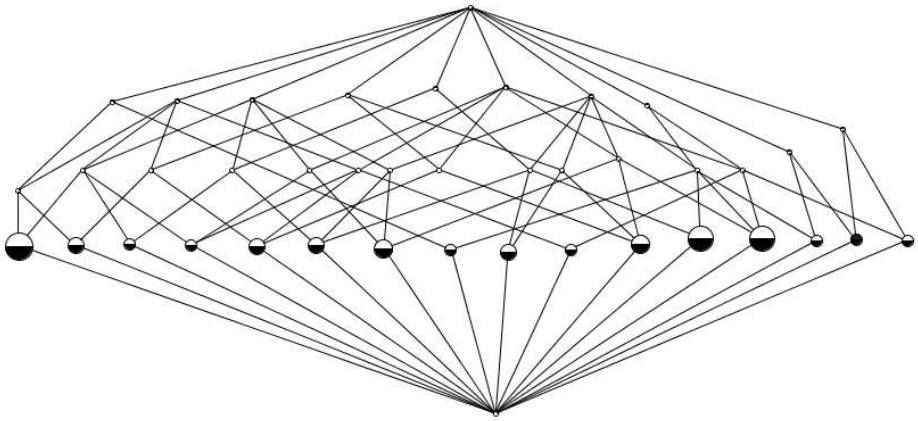

Figure 2. Method variety in the papers from 2005 and 2010.

Figure 2 shows a considerably large methodical variety in the rigor of the papers:

- The most frequent attribute combination is "1.a—2.a—3.a" (nine instance papers) represented by the large circle on the far left of the lattice in Figure 2. Papers with this attribute combination are suggestive, informal and new idea or proposal papers.
- The second most frequent combination is "1.c—2.b—3.b" (eight instance papers) represented by one of the two big circles on the right side of the lattice. These are typical engineering papers that focus on a useful skill and prove ability by pointing to a software implementation.
- The third most frequent combination is "1.c—2.b—3.c" (seven instance papers) represented by the other large circle on the right side of the lattice. These papers are also engineering-oriented, but they include additional efforts towards evaluating the properties of a software implementation, instead of merely presenting its existence as a proof-of-concept.

All together, these $9 + 8 + 7 = 24$ papers correspond to slightly more than 50% percent of the 46 papers analyzed in the two conferences.

3.2 Reviewer Perspectives

One of the authors of this paper served as the program co-chair of the second conference (in 2006). The reviews sent to the authors of accepted and rejected papers were still available. The feedback to the authors was

concatenated and scanned for comments that would confirm or refute the quantitative classification. Many reviews were positive, but only a few reviews suggested that the corresponding papers met the requirements of a mature discipline. Much of the positive feedback was based on the novelty of the idea in the paper, the way the paper extended the boundaries of digital forensics, or the fact that the paper covered a topic that was important in some way or another.

One reviewer, for example, stated that "despite its shortcomings, I believe the work is interesting for two reasons: it provides an opportunity for digital forensics people to take a look beyond the hard drive; and raises the important issue of" considering a specific facet of forensics during the development of new systems. It is a discipline finding its feet that commends worthwhile extensions and critiques those that seem unnecessary. Note that in quoting from a review, verbiage that may identify the paper is redacted.

As can be expected for a new discipline, most of the research feedback focuses on the boundaries of the field as well as initial explorations that show promise.

One positive comment was "This paper looks at a relevant problem and gives a simple solution for it." More critical are the comments that draw the boundaries closer than authors have hoped: "This is not a digital forensics topic. It is a computer security topic" or "The motivation for this work is not obvious." "The connection made to forensics, albeit not deniable, is quite tenuous" and "Despite the title, the paper does not address forensic issues" are two additional comments dealing with the boundaries of the discipline. Referring to Table 1, it is clear that these comments are at the low end of the scale.

It should be noted that a good number of papers explore questions of the form "What is X?" and more often "Is X possible?" (Table 1). Each of these papers typically elicited a statement from a reviewer that the paper shows that X has potential. As such, the papers met reviewer expectations, although the reviewers often wanted tools that could shift the boundaries. In other words, proposing a system to achieve X was acceptable. However, with X as the research product, some additional functionality was expected, which is indicative of an increase in the research setting scale.

3.3 Research Product

The research product dimension included the most critical feedback. The community mainly comprises individuals who often have one foot in academia and the other in practice. The practitioners want tools that

provide a competitive advantage. However, even from a pure scientific standpoint, research products (new tools, techniques and theories) are likely to push the research setting scale to higher levels.

Examples of comments dealing with the research product dimension are:

- "The primary flaw with the paper is that the work is not presented in enough detail for the underlying technology to be used or replicated."
- "This is not really a research paper. It is more of a hands-on lab manual."
- "Instead of discussing how this tool could benefit the area of digital forensics, the author focused on how the tool is built and functions."
- "It would have been nice to see an analysis of an implementation, what were the end requirements of the investigator for initializing and using the system on a compromised network. As well as a study on the amount and type of logging that is necessary."
- "The paper is definitely one I would like to see developed, but as the document is I found it hard to find significant value."
- "This paper presents a sketch of an architecture for recording and retrieving TCP/IP network data in a ... system."
- "No new material is contributed and some vital current methods/techniques for establishing location during a network event are missing."
- "There is no mention of how these things will be done other than stating that they are future work, which really should have been done."
- "It is more like a position paper."
- "In terms of pure computer science, this is yet another file format and I find the basic design reasonable."

The (explicit or implied) critique above is of the form that this is "yet another" solution to a known problem. The fact that "yet another" tool or technique has been developed is not necessarily bad. In an emerging field, it may be fatal to prematurely suppress alternative new ideas. Solutions that venture beyond the beaten track may be the ones that eventually have broad impact.

However, a number of solutions were critiqued in that the mere fact that they were novel was no longer sufficient. Many of the comments called for a greater emphasis in the validation technique dimension rather than a deepening of the research product dimension:

- "Also, the paper should have included experimental results to make it more convincing and solid."
- "My question is how do you arrive at 30% and 15%?"
- "At a minimum, the authors should convince the reader that there are many things mentioned in the paper that are technology invariant."
- "We should have a good start on [some specific forensic issue] but are not working on it from the scratch."

3.4 Validation Technique

The reviewer feedback reflects a number of issues regarding the validation dimension described in Table 3.

One recurring theme was doubt that a solution was correct. One reviewer stated "the analytical results in the paper heavily rely on [some] assumption. Without this assumption, the analytical results would not be valid. But in most real-world scenarios, this assumption is invalid." A related remark about a different paper questions the data used, rather than an assumption: "I would like to be convinced that this is not a toy or contrived problem. The authors could do this by validating their algorithm on actual data, rather than on generated data."

Some other attempts at validation were not met with the same skepticism, but pointed out that the validation was incomplete in some respect. For example: "One of the key aspects of this paper is the new ... protocol, which even the author says has not been proven to work as advertised." In another instance, a reviewer laments "Currently the paper does not provide any evidence that such a relationship exists." In one case, the absence of validation is noted: "One thing lacking is a validation of the model."

As a final illustration, consider the following remarks about missing details, which primarily affect repeatability:

- "My main problem with this paper is that some very important details are missing. The authors talk about quantifying the confidence of a forensic examination, but give no information whatsoever how this quantification is done."

- "The main problem with the paper is its relative vagueness."
- "What is the standard deviation of the frequencies and other results?"

4. Stability and Fluctuation of the Community

The maturation of an emerging field of research is also related to the stability and fluctuation of the community of researchers who are active in a field. The arguments encouraging these aspects are:

- Serious researchers, who have confidence in the worthiness of their own work, do not tend to abandon their field of work prematurely.
- New researchers tend to flow into an emerging research field as others begin to recognize the relevance of the field.
- Some fluctuation is to be expected by the natural retirement of the pioneers and "founding fathers."
- Short-term fluctuation is to be expected due to the co-authorship of student-researchers, who often depart the research scene after having obtained their postgraduate degrees.
- The long-term existence of a small set of "gurus" and the high fluctuation rate of student co-authors are likely symptoms of esoteric stagnation and lack of external popularization of the field.

To this end, we have computed a formal concept lattice that represents the "community" during the years 2005 and 2010, based on the authorship of all the papers from the two conferences. Figure 3 shows a lattice graph of the overall author community, with the 2005 community on the left-hand side and the 2010 on the right-hand side. Research clusters are marked using circles, and the middle-ground represents a continuity of researchers who co-authored papers in 2005 and 2010.

The lattice graph shows rapid fluctuation in the community of co-authors during the relatively short period of time between 2005 and 2010, with only a small number of co-authors present in both 2005 and 2010. Some clusters of researchers are recognizable, but on the other hand, there are also a considerable number of contributions from outside the clusters. In other words, the research community depicted in Figure 3 does not suffer from unhealthy inbreeding. On the other hand, the rather small area of personal continuity during a short time span of only five years might be a cause for concern.

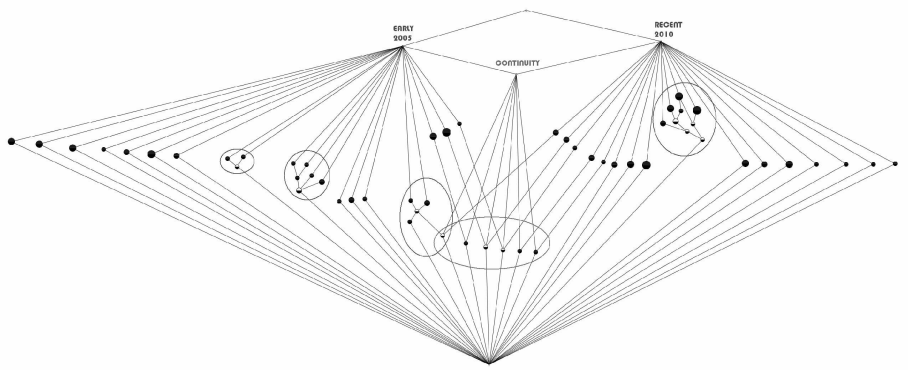

Figure 3. Lattice showing the early (2005) and recent (2010) author communities.

5. Conclusions

This paper has attempted to evaluate the scientific maturity of digital forensics. The statistical review and the qualitative remarks demonstrate that the lack of scientificness that characterized software engineering a decade ago is currently present in digital forensics research. Like Shaw [45] did in the case of software engineering, we emphasize that digital forensics must become more scientific and we urge our colleagues to redouble their efforts to increase the level of scientificness. We also believe that Shaw's model provides a strategy for incrementally improving the scientificness of digital forensics research to the point where the discipline can be considered to be scientifically mature.

Acknowledgements

The authors thank Candice le Sueur for her assistance with writing the introductory remarks. The authors also thank the anonymous reviewers and workshop participants for their constructive comments.

References

[1] S. Al-Kuwari and S. Wolthusen, Forensic tracking and mobility prediction in vehicular networks, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 91–105, 2010.

[2] N. Beebe and J. Clark, Dealing with terabyte data sets in digital investigations, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 3–16, 2005.

[3] M. Bunge, *Philosophy of Science (Volume One): From Problem to Theory*, Transaction Publishers, New Brunswick, New Jersey, 1998.

[4] M. Bunge, *Philosophy of Science (Volume Two): From Explanation to Justification*, Transaction Publishers, New Brunswick, New Jersey, 1998.

[5] Y. Chen, V. Roussev, G. Richard and Y. Gao, Content-based image retrieval for digital forensics, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 271–282, 2005.

[6] K. Chow and S. Shenoi, *Advances in Digital Forensics VI*, Springer, Heidelberg, Germany, 2010.

[7] F. Cohen, Toward a science of digital forensic evidence examination, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 17–35, 2010.

[8] S. Conrad, G. Dorn and P. Craiger, Forensic analysis of a Playstation-3 console, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 65–76, 2010.

[9] P. Craiger, Recovering digital evidence from Linux systems, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 233–244, 2005.

[10] M. Davis, G. Manes and S. Shenoi, A network-based architecture for storing digital evidence, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 33–42, 2005.

[11] T. Duval, B. Jouga and L. Roger, The Mitnick case: How Bayes could have helped, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 91–104, 2005.

[12] B. Fei, J. Eloff, H. Venter and M. Olivier, Exploring forensic data with self-organizing maps, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 113–123, 2005.

[13] P. Gershteyn, M. Davis, G. Manes and S. Shenoi, Extracting concealed data from BIOS chips, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 217–230, 2005

[14] P. Giannelli, Wrongful Convictions and Forensic Science: The Need to Regulate Crime Labs, Working Paper 08-02, School of Law, Case Western Reserve University, Cleveland, Ohio, 2008.

[15] M. Gunestas, M. Mehmet and D. Wijsekera, Detecting Ponzi and pyramid business schemes in choreographed web services, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 133–150, 2010.

[16] Y. Guo and J. Slay, Data recovery function testing for digital forensic tools, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 297–311, 2010.

[17] M. Hoeschele and M. Rogers, Detecting social engineering, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 67–77, 2005.

[18] R. Ieong, P. Lai, K. Chow, M. Kwan and F. Law, Identifying first seeders in Foxy peer-to-peer networks, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 151–168, 2010.

[19] P. Kahai, M. Srinivasan, K. Namuduri and R. Pendse, Forensic profiling system, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 153–164, 2005.

[20] E. Kim, D. Massey and I. Ray, Global Internet routing forensics, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 165–176, 2005.

[21] R. Koppl and M. Ferraro, Digital devices and miscarriages of justice, *Daily Caller* (`dailycaller.com/2012/06/15/digital-devices-and-miscarriages-of-justice`), June 15, 2012.

[22] M. Kwan, R. Overill, K. Chow, J. Silomon, H. Tse, F. Law and P. Lai, Evaluation of evidence in Internet auction fraud investigations, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 121–132, 2010.

[23] R. Laubscher, D. Rabe, M. Olivier, J. Eloff and H. Venter, Applying forensic principles to computer-based assessment, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 105–112, 2005.

[24] F. Law, P. Chan, S. Yiu, B. Tang, P. Lai, K. Chow, R. Ieong, M. Kwan, W. Hon and L. Hui, Identifying volatile data from multiple memory dumps in live forensics, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 185–194, 2010.

[25] F. Li, H. Chan, K. Chow and P. Lai, An analysis of the Green Dam Youth Escort Software, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 49–62, 2010.

[26] M. Losavio, Non-technical manipulation of digital data, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 51–63, 2005.

[27] M. Meyers and M. Rogers, Digital forensics: Meeting the challenges of scientific evidence, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 43–50, 2005.

[28] T. Moore, A. Meehan, G. Manes and S. Shenoi, Using signaling information in telecom network forensics, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 177–188, 2005.

[29] Y. Motora and B. Irwin, In-kernel cryptographic executable verification, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 303–313, 2005.

[30] Y. Nakayama, S. Shibaguchi and K. Okada, A visualization system for analyzing information leakage, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 269–282, 2010.

[31] S. Ngobeni, H. Venter and I. Burke, A forensic readiness model for wireless networks, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 107–117, 2010.

[32] J. Okolica and G. Peterson, A compiled memory analysis tool, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 195–204, 2010.

[33] M. Olivier, Forensics and privacy-enhancing technologies, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 17–31, 2005.

[34] L. Peng, T. Wingfield, D. Wijsekera, E. Frye, R. Jackson and J. Michael, Making decisions about legal responses to cyber attacks, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 283–294, 2005.

[35] A. Persaud and Y. Guan, A framework for email investigations, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 79–90, 2005.

[36] G. Peterson, Forensic analysis of digital image tampering, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 259–270, 2005.

[37] S. Piper, M. Davis, G. Manes and S. Shenoi, Detecting hidden data in ext2/ext3 file systems, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 245–256, 2005.

[38] M. Pollitt, A history of digital forensics, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 3–15, 2010.

[39] M. Pollitt and S. Shenoi, *Advances in Digital Forensics*, Springer, Boston, Massachusetts, 2005.

[40] S. Redding, Using peer-to-peer technology for network forensics, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 141–152, 2005.

[41] V. Roussev, Data fingerprinting with similarity digests, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 207–226, 2010.

[42] A. Savoldi, P. Gubian and I. Echizen, Uncertainty in live forensics, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 171–184, 2010.

[43] B. Schatz and M. Cohen, Redefining evidence containers for provenance and accurate data representation, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 227–242, 2010.

[44] K. Shanmugasundaram, H. Bronnimann and N. Memon, Integrating digital forensics in network infrastructures, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 127–140, 2005.

[45] M. Shaw, The coming-of-age of software architecture research, *Proceedings of the Twenty-Third International Conference on Software Engineering*, pp. 656–664, 2001.

[46] J. Slay and K. Jorgensen, Applying filter clusters to reduce search state space, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 295–301, 2005.

[47] G. Snelting, Paul Feyerabend und die Softwaretechnologie, *Informatik Spektrum*, vol. 21(5), pp. 273–276, 1998.

[48] C. Swenson, G. Manes and S. Shenoi, Imaging and analysis of GSM SIM cards, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 205–216, 2005.

[49] K. Tadano, M. Kawato, R. Furukawa, F. Machida and Y. Maeno, Digital watermarking of virtual machine images, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 257–268, 2010.

[50] V. Thing, Virtual expansion of rainbow tables, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 243–256, 2010.

[51] K. Wang, Using a local search warrant to acquire evidence stored overseas via the Internet, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 37–48, 2010.

[52] S. Willassen, Forensic analysis of mobile phone internal memory, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 191–204, 2005.

[53] Y. Yang, K. Chow, L. Hui, C. Wang, L. Chen, Z. Chen and J. Chen, Forensic analysis of popular Chinese Internet applications, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 285–295, 2010.

[54] Y. Zhu, J. James and P. Gladyshev, A consistency study of the Windows registry, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 77–90, 2010.