On the Scientific Maturity of Digital Forensics Research

Martin Olivier and Stefan Gruner
Department of Computer Science
Universiteit van Pretoria
Republic of South Africa

Abstract. In this paper we transfer a well-known grade schema of scientific maturity from the domain of software engineering into the domain of digital forensics research. On the basis of this maturity schema and its grades we classify the current state of maturity in the research field of digital forensics, and we argue for more efforts towards higher levels of scientificness in this still new field of research.

1 Introduction

The digital age has both enabled and necessitated digital forensics as a means to maintaining law and order in society. Earlier forensic methods have occasionally failed those who were wrongfully convicted on the basis of low-quality evidence [22, 13]. Therefore digital forensic scientists and practitioners have a moral duty to to avoid repeating the mistakes of the past by scrutinizing the scientific maturity of their field, and by approaching and conveying information accordingly. In the past, the absence of strict scientific standards in some forensic practices has caused confusion about the reliability, validity, repeatability and accuracy of their outcomes, especially if those outcomes were presented in courtrooms where the intended audience does not have the technical knowledge to judge the reliability of the presented information.

In a developed scientific field, in contrast, one can place much more trust in the outcomes of processes, as 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. It is clear that scientific maturity is neither one dimensional, nor measurable in absolute terms. We will therefore use the somewhat informal term *scientificness* in this paper to acknowledge the fuzziness of the concept. This fuzziness, however, does not diminish the importance of being aware of the extent to which claims made in a field are supported by the underlying science.

As noted, digital forensics is still a developing field in its early days of establishment. Thus the question arises: *Where exactly* is digital forensics currently positioned in its early days of establishment'? Is it possible to assess the level of *scientificness* that has already been reached thus far? What is, by-and-large, the current level of *scientificness* in digital forensics?

In this paper — which has its focus on the question of scientificness as such, *not* on its external legal and ethical incentives and motivations — we present such a maturity assessment, based on a science maturity scale transferred from an earlier paper on the topic of software engineering, particularly software architecture. The transfer of that maturity scale, from software architecture to digital forensics, is justified by the similarity of the problems, including the shortage of scientificness, which were experienced in the domain of software architecture more than a decade ago and the impact of both fields in the physical world given that important decisions are based on claims from these fields.

In the remainder of this paper we recapitulate the scientificness scale from software architecture which we assert is useful in the filed of digital forensics. Thereafter we assess the short history of *this* (IFIP WG11.9) conference series — that is, its main outcomes over the past decade — against the template of the 'inherited' scientificness scale. Finally we conclude with some statements about the progress which has been made in the field of digital forensics in its brief history as an emerging scientific discipline.

2 A Similar Problem in Software Engineering

An early and well-argued lament about a shortage of scientificness in the field of software engineering, characterized by a flood of nice-idea-proposal kind of papers without any further implications, was published already in 1998 (first in German and then also in an English translation) by Snelting [47]. In that paper Snelting reminded the software engineering community about Popper's criterion of falsifiability, with a particular 'slant' against the post-modernist intellectual fashion of socio-constructivism, and demanded more efforts towards the empirical validation of speculative ideas and conjectures. However, Snelting's appeal for more scientificness did not take into account the typical gradual historic development of emerging academic subjects from pre-scientific via proto-scientific to fully scientific stages.

In a somewhat later paper on the problem of shortage of scientificness in software engineering (particularly: software architecture research), published in 2001 by Shaw [45], the spectrum from pre-scientific to scientific qualities in the historic development of an emerging academic subject has well been taken into account. With reference to older work by Redwine and Riddle, Shaw [45] broadly identified *six typical* stages in the historic development of an emerging subject of research particularly in the domain of the *technical* sciences (which are characterized by their drive towards practical applications and external usefulness):

- Early prospecting
- Concept formulation
- Development and extension
- Internal enhancement
- External 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?

- Popularization

For further details about those six typical historical phases, which need not be recapitulated for the purpose of our argument, please see Shaw [45]. Most important for the purpose of this paper is Shaw's three-dimensional maturity classification scheme, whereby the notion of maturation from early prospecting to popularization (as sketched above) re-appears *implicitly* in each of the three dimensions of her science-maturity classification scheme. These dimensions are, according to [45]:

- Research settings;
- Research approaches and methods; and
- Result validation techniques.

The ascending maturity values in each of these three dimensions of assessments are briefly recapitulated (including some interpretative modification and adaptation) from Shaw's paper in tables 1, 2 and 3.

In those table entries, where our classification criteria differ slightly from the ones in [45] for the sake of clarity, we have used Bunge's books [3, 4] as guide. Obviously the whole concept of tabulating levels of quality is also related to the well-known maturity assessment schemas in other domains of human practice, such as the CMMI for general organizational capabilities, or the TMMI for maturity assessment in the domain of systematic software testing.

Shaw concluded her often-cited literature survey and maturity assessment, carried out on the basis of the maturity scheme recapitulated above, with the following words: *"We see that software architecture is reaching the point of growing from its adolescence in research laboratories to the responsibilities of maturity. This brings with it additional responsibility to show not just that ideas are promising (...)"* —remember Snelting [47] as a frame of reference— *"but also that they are effective (a necessary grounds to move into practice). As*

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 generalisations from examples. Structure a problem area and formulate the right questions. Analyse 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 of engineering	Embody results in a systematic context. Use system development as source of insight and carrier or 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 which can do ... Here we see one example which has ...
3.c	Informal evaluation	Comparison of several objects against each other. Rule-of-thumb comparison against check-lists. Explorative 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

a result, software architects must not be content with simply doing more research in the style of the past decade. Certainly there are new ideas yet to be explored in that form, but we must attend to making existing results more robust, more rigorously understood, and more ready to move into application" [45]. 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*" [45].

It is not in the scope of our paper to delve into a deep and detailed science-philosophical critique of the maturity classification scheme itself which Shaw had presented and used in her paper —such would be a suitable topic for a journal in the philosophy of science— though we acknowledge up-front that such a critique might well be justified from several vantage points. Instead, we want to 'mimick' and transfer both Shaw's maturity schema and her method of analysis into the domain of digital forensics, with the aim of revealing explicitly and clearly how research in the field of digital forensics is now suffering by-and-large from the same illness which had been diagnosed in software engineering and software architecture a decade ago. Consequently we also argue that Shaw's conclusion and request for future work, as quoted and cited above, can also be transferred almost literally from the domain of software engineering in the year 2001 into the domain of digital forensics today. This is the topic of the following sections.

3 The State of the Art in Digital Forensics

This section's survey on the state of scientificness in digital forensics research is divided into two parts as follows. First, a large statistical overview of almost 50 IFIP papers (from this conference series) is given in terms of Mary Shaw's model of scientific maturity, adopted from software engineering research. Thereafter, some 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 IFIP WG 11.9 Papers from 2005 to 2010

For this subsection we checked some of the proceedings of this conference series, 'Advances in Digital Forensics', against the scientific maturity criteria from Section 2. For the purpose of our argument it is sufficient to look only at one proceedings book which we can classify as '*early*', namely Volume I [18] with 25 contributions, and one which we can classify as '*recent*', namely Volume VI [19] with 21 contributions. The tedious exercise of browsing through all papers of all volumes of this IFIP WG 11.9 series would be pointless, because you can easily convince yourself about the fact that the 'big picture' is more or less the same for Volumes II–V and VII as well as for most of the papers in the small number of related journals or similar workshops. Table 4 shows the 'raw data' of this survey, whereas

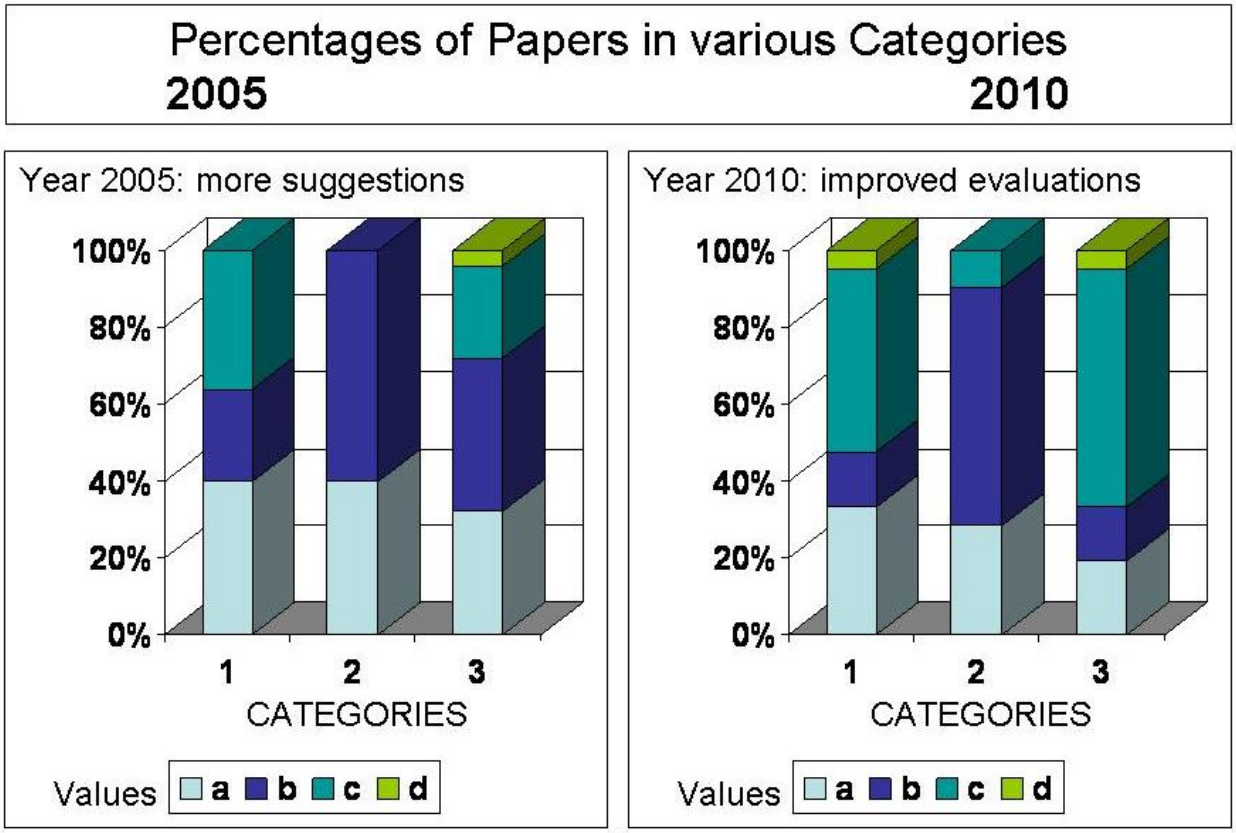

Figure 1: Shrinking of the lowest value —a— in all three quality categories from proceedings volume I (2005) to volume VI (2010). However a high value —d— was still achieved only rarely also in the year 2010.

the subsequent formal concept lattice visualizes the findings more intuitively in their mutual relations.

We can extract from this table that in most cases, both in 2005 and 2010, the large majority of papers does not reach level **d** in any of the categories. However we can see a trend towards better evaluation efforts, with comparatively more work in category 3.c, from the year 2005 to the year 2010. The large number of papers in category 2.b in combination with 1.a or 1.c indicates that many authors in the field of digital forensics are working in a typical '*engineering*' mode in which a useful skill is the goal — engineers are typically not highly interested in deep theoretical explanations, as long as 'it works OK' and does not 'bug us' with too many painful defects. Combinations of categories 1.b with 2.c, very rare in the table of above, would indicate more 'scientific' interests for knowledge of its own sake. The whole situation is depicted summarily in Figure 1.

Figure 2 depicts the diversity of attribute combinations (e.g., 1.a—2.b—3.b) extracted from the table of above, from all the papers (years 2005/2010) of our data set. The 16 'balls'

Table 4: Classification of IFIP WG 11.9 Papers

Year 2005 (early)		Year 2010 (recent)	
Paper	*Classification*	*Paper*	*Classification*
[2]	1.a—2.a—3.a	[39]	1.a—2.a—3.a
[34]	1.b—2.a—3.c	[6]	1.b—2.a—3.a
[9]	1.a—2.b—3.b	[51]	1.a—2.a—3.a
[28]	1.a—2.a—3.a	[26]	1.c—2.b—3.c
[27]	1.b—2.a—3.c	[7]	1.c—2.a—3.c
[16]	1.c—2.b—3.b	[54]	1.c—2.b—3.b
[36]	1.b—2.b—3.c	[1]	1.c—2.c—3.c
[10]	1.c—2.b—3.**d**	[32]	1.a—2.a—3.c
[24]	1.a—2.a—3.a	[23]	1.b—2.b—3.c
[11]	1.c—2.b—3.b	[14]	1.c—2.b—3.c
[44]	1.c—2.b—3.b	[17]	1.c—2.b—3.c
[40]	1.a—2.a—3.b	[42]	1.a—2.b—3.c
[20]	1.b—2.b—3.b	[25]	1.a—2.b—3.c
[21]	1.b—2.b—3.b	[33]	1.a—2.b—3.c
[29]	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**
[12]	1.c—2.b—3.b	[49]	1.c—2.b—3.c
[8]	1.c—2.b—3.a	[31]	1.a—2.b—3.c
[38]	1.a—2.a—3.a	[53]	1.c—2.b—3.b
[37]	1.c—2.b—3.c	[15]	1.b—2.a—3.a
[5]	1.c—2.b—3.c	-	-
[35]	1.c—2.b—3.b	-	-
[46]	1.a—2.a—3.a	-	-
[30]	1.a—2.a—3.a	-	-

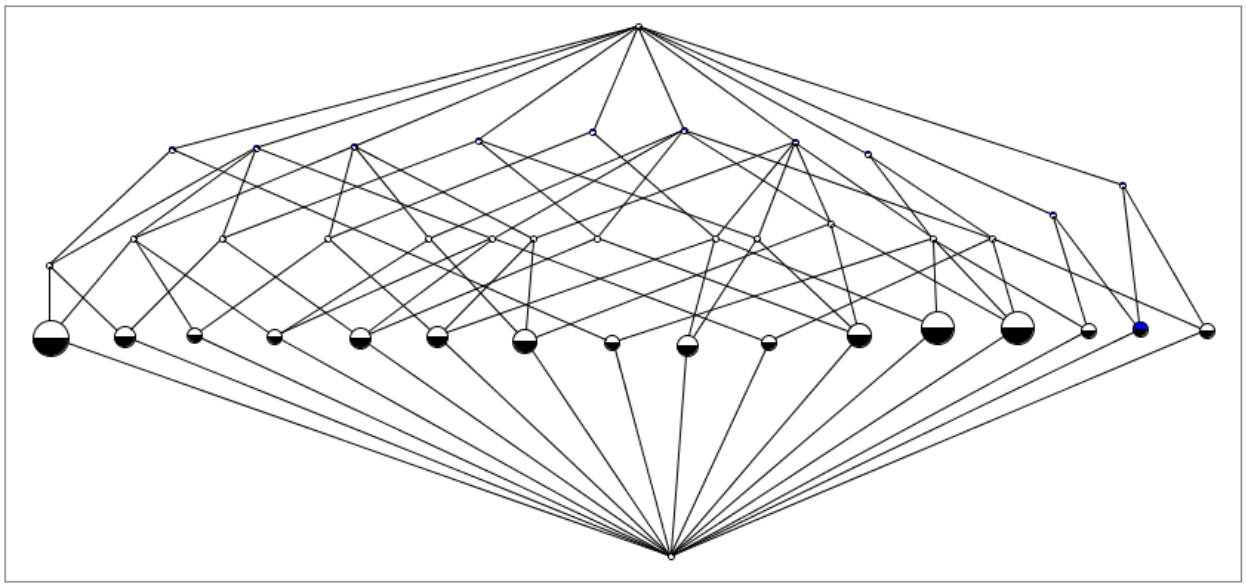

Figure 2: Method variety in the papers from volume I (2005) and volume VI (2010). The different balls represent different attribute combinations. Small balls represent rare combinations. Big balls represent larger sub-sets of papers sharing the same attribute combination.

in the lattice of Figure 2 indicate 16 different attribute combinations. This shows clearly a considerably large methodical variety as far as the 'flavour' and 'rigour' of those papers are concerned.

- Most often was the attribute combination '1.a—2.a—3.a', with 9 instance papers, represented by the biggest ball at the very left hand side of the lattice of Figure 2. Papers with this attribute combination are the suggestive informal new-idea-proposal papers.

- Second often, with 8 instance papers, was the attribute combination '1.c—2.b—3.b' represented by one of the two big balls in the right hand side of the lattice. Those are the typical 'engineering' papers which aim at a useful skill and prove ability by pointing to an implementation of a software prototype.

- Third often, with 7 instance papers, was the attribute combination '1.c—2.b—3.c' represented by the other one of the two big balls in the right hand side of the lattice. In those papers, which are also 'engineering-oriented' in principle, we can find additional efforts towards evaluating the properties of an implemented software prototype, instead of merely pointing out its very existence as a proof-of-concept.

All together, those $9 + 8 + 7 = 24$ papers make slightly more than 50% percent of our altogether $25 + 21 = 46$ papers analysed in this section.

3.2 Reviewers' perspectives

One of the authors of the current paper was program co-chair of the second conference. The reviews sent to the authors of accepted and rejected papers were still available. The feedback to authors was concatenated and scanned for comments that would help to confirm or refute the quantitative classification provided above. Many reports were positive, but few — if any — suggested that the reviewed paper was one that met the requirements of a mature discipline. Much of the positive feedback were based on the novelty of the idea in the paper, the way the paper extends the boundaries of digital forensics or selected a topic that is important in some way or another. One reviewer, for example, said about a specific paper *"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 development of new systems. It is a discipline finding its feet that is commending 'worthwhile' extensions, and critiquing those that seem unnecessary. Note that in quoting from the referee report above (as well as below) we intentionally try to redact the comment such that it does not identify the paper it relates to, because we consider communication between reviewers and authors to be private (albeit facilitated by program chairs and program committees).

We new proceed to look at some critical comments from reviewer feedback using Shaw's three dimensions; again note that the critical bias is used to highlight reviewer expectations.

3.2.1 Research setting

As can be expected for a new discipline, many of the research setting dimension feedback focusses on the boundaries of the field, as well as some initial exploration of which directions show promise.

One positive comment, for example, 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 *Moreover, despite the title, the paper does not address forensic issues."* are two addition comments dealing with the boundaries of the discipline. Referring to Table 1, it is clear that these questions are indeed at the low end of the scale.

It should be noted that a good number of papers explored question of the form "What is X?" or, even more often "Is X possible at all?". (See Table 1 again These papers papers typically elicited the factual statement from the reviewer that the paper shows that X has potential. As such they seemed to meet reviewer's expectations, although reviewers often wanted such tools to shift boundaries somewhat. Stated differently, proposing a system to achieve X was acceptable; however, with X as the research product some additional functionality was expected — rather than an increase on the research setting scale.

3.3 Research product

The rubric *Research product* arguably was the one under which most critical feedback can be classified. The community consists of people who often have one foot in academia and the other in practice. The practitioners are want tools that will give them the competitive advantage. However, even from a pure scientific standpoint, research products (new tools, techniques and even theories) are likely to push the research setting scale to higher levels.

Examples of comments we classified as dealing with research product are listed below. They tell their own story.

- *"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 suppress the field for alternative new ideas too soon Solutions that venture beyond the beaten track may be the ones that eventually strike gold.

On the other had, a number of solutions attracted critique that indicated that the mere fact that they could have been novel was no longer sufficient. The following examples illustrate such comments. However, gain, many of the comments seem to call for a greater

emphasis in dimension 3, rather than a deepening of dimension 2. Consider the following feedback extracts:

1. *"Also, the paper should have included experimental results to make it more convincing and solid."*
2. *"My question is who do you arrive at 30% and 15%?"*
3. *"At a minimum the authors should convince the reader that there are many things mentioned in the paper that are technology invariant."*
4. *"We should have a good start on wireless network forensics research, but are not working on it from the scratch."*

3.4 Validation technique

The reviewers' feedback reflect a number of the issues regarding validation listed in Table 3.

One recurring theme is reviewers' doubts that a solution is correct.. About one paper a reviewer says *"the analytical results in the paper heavily rely on this 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 some specific 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 scepticism, 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 it has not been proven to work as advertised."* In another case the reviewer's lament is *"Currently the paper does not provide any evidence that such relationship exists."* In one case the absence of validation is noted: *"One thing that the paper is lacking is a validation of the model"*

As a final illustration, consider some of the remarks about missing details (primarily affecting repeatability).

- *"My main problem with this paper is that some very important details are missing. The authors talk about quantifying the confidence of a forensics 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 on the frequencies and other results?"*

4 Stability vs. Fluctuation of the Community

Maturation of an emerging field of research is also related to the stability versus fluctuation of the 'community' of researchers who are active in this field.

- On the one hand, serious researchers, who have confidence in the worthiness of their own work, should not tend to abandon their field of work prematurely.
- On the other hand, 'fresh blood' should flow into an emerging research field (see above: 'popularization' in Section 2) if and as soon as others begin to recognize the relevance of this field of research, too.
- In the long run, some fluctuation is to be expected by the natural retirement of the pioneers and 'founding fathers'.
- Some short-term fluctuation is to be expected due to the co-authorship of student-researchers who often vanish from the public research scene into some private business after having obtained their postgraduate degrees.
- The long-term existence of a small set of always the same 'Gurus', together with a high fluctuation rate of student co-authors, is likely a symptom of esoteric stagnation and lack of external popularisation of the field.

To this end we have also computed a formal concept lattice which represents the 'community' in the years 2005 and 2010, based on the authorship of all the papers of IFIP WG 11.9 Volume I and Volume VI which we have classified above in Section 3. The lattice graph of Figure 3 intuitively shows rapid fluctuation in the community of co-authors during the short period of time between the years 2005 and 2010, with only a small number of co-authors present both in 2005 and in 2010. Some clusters of researchers can clearly be recognized, but on the other hand there were also considerable numbers of contributions from outside of those clusters. In other words: The research community depicted by Figure 3 does surely not suffer from unhealthy 'esoteric inbreeding', but the rather small area of personal continuity during such a short time span (of only five years) might perhaps also raise some concern.

5 Conclusion and Outlook

This paper gauged the scientific maturity of digital forensics. Both the statistical review, as well as the qualitative remarks illustrated that the same lack of scientificness that characterized software engineering a decade ago are currently present in digital research. Like Shaw, for software engineering, we note the necessity for digital forensics to become more scientific and urge our colleagues to redouble their efforts to increase the scientificness of digital forensics research. We contend that Shaw's model provides a useful strategy to incrementally improve the scientificness of digital forensic research up to a point where the discipline may be considered mature.

Last but not least we may remark that we have also demonstrated with this paper the fertility of inter-sub-disciplinary dialogues between different sub-disciplines of and within the over-arching discipline of informatics.

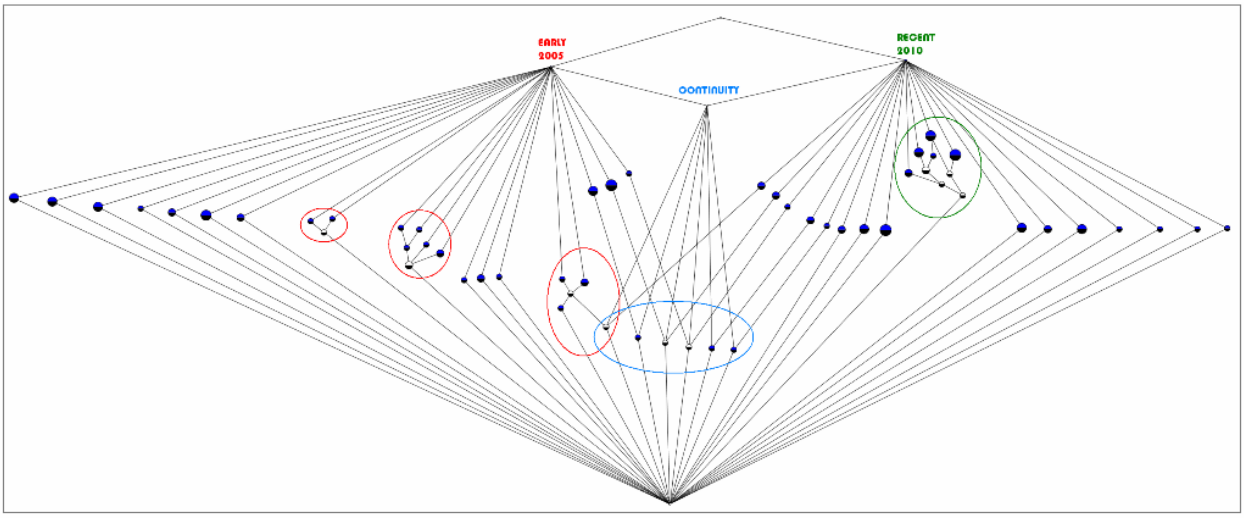

Figure 3: Lattice depicting the early community of authors (2005) on the left-hand-side and the recent community (2010) on the right-hand-side. Research clusters are circled in. The middle-ground represents a continuity of researchers who co-authored papers both in 2005 and in 2010.

Acknowledgements

Parts of the introduction were written by *Candice le Sueur* (on behalf of Martin Olivier).

References

[1] Al-Kuwari, S. & Wolthusen, S.: *Forensic Tracking and Mobility Prediction in Vehicular Networks*, pp. 91-106 in [19].

[2] Beebe, N. & Clark, J.: *Dealing with Terabyte Data Sets in Digital Investigations*, pp. 3-16 in [18].

[3] Bunge, M.: *Philosophy of Science — From Problem to Theory.* Transaction Publ., revised ed., 1998.

[4] Bunge, M.: *Philosophy of Science — From Explanation to Justification.* Transaction Publ., revised ed., 1998.

[5] Chen, Y. & Roussev, V. & Richard, G. & Gao, Y.: *Content-based Image Retrieval for Digital Forensics*, pp. 271-282 in [18].

[6] Cohen, F.: *Toward a Science of Digital Forensic Evidence Examination*, pp. 17-36 in [19].

[7] Conrad, S. & Dorn, G. & Craiger, P.: *Forensic Analysis of a Playstation-3 Console*, pp. 65-76 in [19].

[8] Craiger, P.: *Recovering Digital Evidence from Linux Systems*, pp. 233-244 in [18].

[9] Davis, M. & Manes, G. & Shenoi, S.: *A Network-based Architecture for Storing Digital Evidence*, pp. 33-42 in [18].

[10] Duval, T. & Jouga, B. & Roger, L.: *The Mitnick Case — how Bayes could have helped*, pp. 91-104 in [18].

[11] Fei, B. & Eloff, J. & Venter, H. & Olivier, M.: *Exploring Forensic Data with Self-organizing Maps*, pp. 113-126 in [18].

[12] Gershteyn, P. & Davis, M. & Manes, G. & Shenoi, S.: *Extracting Concealed Data from BIOS Chips*, pp. 217-232 in [18].

[13] Giannelli, P.C.: Wrongful convictions and forensic science: The need to regulate crime labs. Working Paper 08-02, Case Western Reserve University, 2007.

[14] Gunestas, M. & Mehmet, M. & Wijsekera, D.: *Detecting Ponzi and Pyramid Business Schemes in choreographed Web Services*, pp. 133-150 in [19].

[15] Guo, Y. & Slay, J.: *Data Recovery Function Testing for Digital Forensic Tools*, pp. 297-311 in [19].

[16] Hoeschele, M. & Rogers, M.: *Detecting Social Engineering*, pp. 67-78 in [18].

[17] Ieong, R. & Lai, P. & Chow, K.-P. & Kwan, M. & Law, F.: *Identifying First Seeders in Foxy Peer-to-Peer Networks*, pp. 151-169 in [19].

[18] IFIP WG 11.9: *Advances in Digital Forensics* Vol. I, ed. by M. Pollitt & S. Shenoi. Revised Post-Proc. of the 1st Internat. Conf. on Digital Forensics 2005, Springer-Verlag, 2006.

[19] IFIP WG 11.9: *Advances in Digital Forensics* Vol. VI, ed. by K.-P. Chow & S. Shenoi. Revised Post-Proc. of the 6th Internat. Conf. on Digital Forensics 2010, Springer-Verlag, 2010.

[20] Kahai, P. & Srinivasan, M. & Namuduri, K. & Pendse, R.: *Forensic Profiling System*, pp. 153-164 in [18].

[21] Kim, E. & Massey, D. & Ray, I.: *Global Internet Routing Forensics*, pp. 165-176 in [18].

[22] Koppl, R. & Ferraro, M.M.: Digital devices and miscarriages of justice. *The Daily Caller*, 2012. Online,
http://dailycaller.com/2012/06/15/digital-devices-and-miscarriages-of-justice/

[23] Kwan, M. & Overkill, R. & Chow, K.-P., & Silomon, J. & Tse, H. & Law, F. & Lai, P.: *Evaluation of Evidence in Internet Auction Fraud Investigations*, pp. 121-132 in [19].

[24] Laubscher, R. & Rabe, D. & Olivier, M. & Eloff, J. & Venter, H.: *Applying Forensic Principles to Computer-based Assessment*, pp. 105-112 in [18].

[25] Law, F. & Chan, P. & Yiu, S.-M. & Tang, B. & Lai, P. & Chow, K.-P. & Ieong, R. & Kwan, M. & Hon, W.-K. & Hui, L.: *Identifying volatile Data from multiple Memory Dumps in live Forensics*, pp. 185-194 in [19].

[26] Li, F. & Chan, H. & Chow, K.-P. & Lai, P.: *An Analysis of the Green Dam Youth Escort Software*, pp. 49-63 in [19].

[27] Losavio, M.: *Non-Technical Manipulation of Digital Data*, pp. 51-66 in [18].

[28] Meyers, M. & Rogers, M.: *Digital Forensics — Meeting the Challenges of Scientific Evidence*, pp. 43-50 in [18].

[29] Moore, T. & Meehan, A. & Manes, G. & Shenoi, S.: *Using Signalling Information in Telecom Network Forensics*, pp. 177-190 in [18].

[30] Motorad, Y. & Irwin, B.: *In-Kernel Cryptographic Executable Verification*, pp. 303-313 in [18].

[31] Nakayama, Y. & Shibaguchi, S. & Okada, K.: *A Visualization System for Analyzing Information Leakage*, pp. 269-283 in [19].

[32] Ngobeni, S. & Venter, H. & Burke, I.: *A Forensic Readiness Model for Wireless Networks*, pp. 107-119 in [19].

[33] Okolica, J. & Peterson, G.: *A copiled Memory Analysis Tool*, pp. 195-205 in [19].

[34] Olivier, M.: *Forensics and Privacy-Enhancing Technologies*, pp. 17-32 in [18].

[35] Peng, L. & Wingfield, T. & Wijsekera, D. & Frye, E. & Jackson, R. & Michael, J.: *Making Decisions about Legal Responses to Cyber Attacks*, pp. 283-294 in [18].

[36] Persaud, A. & Guang, Y.: *A Framework for EMail Investigations*, pp. 79-90 in [18].

[37] Peterson, G.: *Forensic Analysis of Digital Image Tampering*, pp. 259-270 in [18].

[38] Piper, S. & Davis, M. & Manes, G. & Shenoi, S.: *Detecting Hidden Data in Ext2/Ext3 File Systems*, pp. 245-258 in [18].

[39] Pollitt, M.: *A History of Digital Forensics*, pp. 3-16 in [19].

[40] Redding, S.: *Using Peer-to-Peer Technology for Network Forensics*, pp. 141-152 in [18].

[41] Roussev, V.: *Data Fingerprinting with Similarity Digests*, pp. 207-226 in [19].

[42] Sawoldi, A. & Gubian, P. & Echizen, I.: *Uncertainty in live Forensics*, pp. 171-184 in [19].

[43] Schatz, B. & Cohen, M.: *Redefining Evidence Containers for Provenance and accurate Data Representation*, pp. 227-242 in [19].

[44] Shanmugasundaram, K. & Brönnimann, H. & Memon, N.: *Integrating Digital Forensics in Network Infrastructures*, pp. 127-140 in [18].

[45] Shaw, M.: *The Coming-of-Age of Software Architecture Research.* Proceedings ICSE'01, pp. 656-664, IEEE, 2001.

[46] Slay, J. & Jorgensen, K.: *Applying Filter Clusters to Reduce Search State Space*, pp. 295-302 in [18].

[47] Snelting, G.: *Paul Feyerabend und die Softwaretechnologie.* Informatik Spektrum 21/5, pp. 273-376, Springer-Verlag, 1998.

[48] Swenson, C. & Manes, G. & Shenoi, S.: *Imaging and Analysis of GSM SIM Cards*, pp. 205-216 in [18].

[49] Tadano, K. & Kawato, M. & Furukawa, R. & Machida, F. & Maeno, Y.: *Digital Watermarking of Virtual Machine Images*, pp. 257-268 in [19].

[50] Thing, V.: *Virtual Expansion of Rainbow Tables*, pp. 243-256 in [19].

[51] Wang, K.: *Using a local Search Warrant to acquire Evidence stored Overseas via the Internet*, pp. 37-48 in [19].

[52] Willassen, S.: *Forensic Analysis of Mobile Phone Internal Memory*, pp. 191-204 in [18].

[53] Yang, Y. & Chow, K.-P. & Hui, L. & Wang, C. & Chen, L. & Chen, Z. & Chen, J.: *Forensic Analysis of popular Chinese Internet Applications*, pp. 285-296 in [19].

[54] Zhu, Y. & James, J. & Gladyshew, P.: *A Consistency Study of the Windows Registry*, pp. 77-90 in [19].