Challenges to Digital Forensics:

A Survey of Researchers & Practitioners Attitudes and Opinions

M. Al Fahdi, N.L. Clarke & S.M. Furnell
Centre for Security, Communications & Network Research (CSCAN)
Plymouth University, Drake Circus, Plymouth, United Kingdom
info@cscan.org

Abstract **– Digital forensics have become increasingly important as an approach to investigate cyber- and computer-assisted crime. Whilst many tools exist and much research is being undertaken, many questions exist regarding the future of the domain. Indeed, prior literature has widely published the challenges that exist within the domain, from the increasing volume of data (e.g. SANs, hard drive capacities, databases) to the varying technology platforms and systems that exist (e.g. tablets, mobile phones, embedded systems, cloud computing). However, little effort has focused upon understanding the reality of these challenges. The paper presents research that seeks to identify, quantify and prioritise these challenges so that future efforts can be concentrated on the issues that actually affect the domain. The study undertook a survey of researchers and practitioners (both law enforcement and organisational) to examine the real-challenges from the perceived challenges and to understand what effect the future will have upon the digital forensic domain. A total of 42 participants undertook the study with 55% having 3 or more years of of experience. 45% were academic researchers, 16% law enforcement and 31% had a forensic role within an organisation. Overwhelmingly, 93% of participants felt that the number and complexity of investigations would increase in the future. Apart from the plethora of findings elaborated in the paper, the principal future challenge priorities included cloud computing, anti-forensics and encryption. Respondents also identified, improving communication between researchers and practitioners and the need to develop approaches to identify and extract "significant data" through techniques such as criminal profiling as essential. Interestingly, participants did not feel that the growth in privacy enhancing technologies nor legislation was a significant inhibitor to the future of digital forensics**.

Keywords – Digital Forensics, Forensic Tools, Cybercrime, Cybersecurity

I. INTRODUCTION

Digital forensics has become an important tool in the identification of computer-based and computer-assisted crime. They are ubiquitously utilised within law enforcement to investigate electronic media and increasingly within organisations as part of their incident response procedures. Whilst forensic tools, such as Guidance Software's Encase [1] and AccessData's FTK [2], have come a long way in the past 15 years to incorporate a good range of forensic functionality, well-documented challenges exist that tools have yet to be fulfil. Eric Holder, the then Deputy Attorney General of the United States Subcommittee on Criminal Oversight for the Senate classified the challenges into three categories [3]:

- Technical challenges – e.g. differing media formats, encryption, steganography, anti-forensics, live acquisition and analysis
- Legal challenges – e.g. jurisdictional issues and a lack of standardised international legislation.
- Resource challenges –e.g. volume of data, time taken to acquire and analyse forensic media

Whilst the challenges have been well documented, few studies have taken place to better understand the practical reality and relevance of those challenges [4-5]. Simply because a challenge exists, does not necessarily mean it is either relevant or important for investigators to focus upon. In 2004, [6] published a (limited) study investigating the top 5 issues facing the domain. From a population of 60 responses (including academics, students, researchers and practitioners) the research found education/training, technologies, encryption, data acquisition and tools as the top 5. There were no further questions asked to explore other aspects. Unfortunately, no further studies were found during the literature review stage that investigated end-user opinions and attitudes towards these challenges.

The purpose of this paper is to investigate from a stakeholder perspective what they feel are the current and future challenges within the digital forensic domain. Section 2 presents the survey methodology and explains the development of the quantitative-based approach and survey tool. Section 3 presents the survey results, including an analysis of researcher and practitioner perspectives. A discussion of the results in line with current literature is presented in Section 4, prior to the conclusions and future work.

II. THE SURVEY METHODOLOGY

A. Purpose Of The Survey

The aim of the survey was to establish and prioritize the key future challenges that are posed within digital forensics with an understanding of the differing perspectives of forensic practitioners and forensic researchers. It was felt the differing motivations of researchers, who typically look longer-term may differ from practitioners, who typically look near-term and thus this might have an impact upon what they consider to be the key challenges. To assist in achieving this, the following objectives were defined:

- For a baseline, understand the general forensic background of participants – in order to appreciate the relevancy of responses
- Understand what participants feel the role of digital forensics is and to what extent it is currently able to meet that requirement
- Understand what (if any) impact changes in future technology will have upon forensic investigations (from both a law enforcement and organizational perspective)
- Examine what effect the evolving nature of forensic capability and knowledge will have upon forensic practice – the evolution of anti-forensic techniques and technologies that are security aware and reduce the forensic opportunity (i.e. The operating systems that forensically wipe files upon deletion).

The format of the survey was kept simple yet effective so that there is an optimum balance between the time spent on the survey, the efforts required to complete it, while giving enough opportunity for the participants to express their views in the most succinct and reasonable manner possible. To achieve this, a number of trial runs of the survey were undertaken by local researchers in the domain acting as participants. From the feedback obtained, the survey was further refined and optimised. The use of a Likert-scale was utilised extensively in order to maximise the information provided through a quantitative approach. It was felt, whilst a qualitative-based research methodology would provide a richer set of results, fewer participants would be willing to take part. As such a quantitative approach was selected, with the option (in numerous places) for the participant to provide further information.

The survey was published online, and the researcher shortlisted potential participants from the identified stakeholder communities who were emailed directly. In total, 128 invitations were sent out for completion amongst the international community (a number of which were to groups rather than individuals). A total of 42 (split between 19 academic researchers and 23 practitioners) completed the survey and were subsequently analysed. Whilst this was not an overly large respondent level, given the highly targeted nature of the survey, it was considered not an unreasonable sample size from which to proceed to analyse.

III. SURVEY RESULTS

The survey was divided into four sections: demographics, the current forensic capabilities, the future challenges and legislative concerns. The results presented initially are based upon the response from the complete population; however, where appropriate, further analysis based upon the stakeholder perspectives of researchers and practitioners is presented.

A. Demographics

An analysis of the demographics illustrates the respondents are on the whole well educated with a significant level of experience – both in terms of years within the domain and holding relevant professional qualifications. Of the 19 researcher responses all have a postgraduate degree, as did 48% of the practitioners. Notably however, 65% of practitioners also had one or more relevant professional qualifications – as would be expected due to the nature of the role. Furthermore, as illustrated in **Figure 1**, 55% of the respondents have 3 or more years experience. This demonstrates the respondent population is a relevant and experienced mix of academic researchers and practitioners appropriate to provide informed opinions.

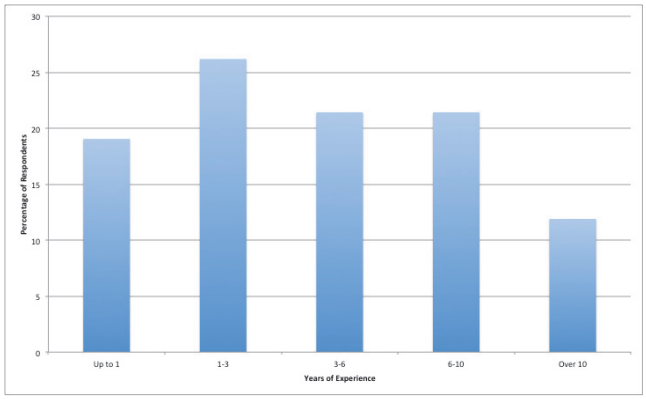

Figure 1. Respondent Experience within the Domain

B. The Role of Digital Forensics and Current Tool Capabilities

The purpose of this section was to explore how respondents currently felt about digital forensics and specifically with regards to what the current limitations were and how well tools are able to provide the necessary functionality. An initial question asked respondents how important they felt digital forensics was. Given their background and expertise, it was expected that the response would be favorable towards it being important; however, it was asked to explore their opinion within the wider context and to provide a comparison to later responses. The respondents overwhelming (98%) ranked it 4 or 5 out 5.

The respondents were also asked to check what they feel were key limitations. The list being derived from an examination of literature and with the additional option of permitting the respondent to add any missing limitations. Overall, the volume of data to be analyzed (74%) and the time taken (67%) are considered the key limitations, with the remaining factors obtaining less than 50% of the response. Further analysis based upon the stakeholders perspectives (i.e. researcher and practitioner), as illustrated in **Figure 2**, show that proportionally researchers feel there are a greater number of limitations than their practitioner counterparts. Whilst they agree with the volume of data, more researchers felt the time taken to undertake investigations was a limiting factor. Another significant difference of opinion appears with the automation of forensic analyses – with double the proportion of researchers (63%) identifying it as a key limitation over the practitioners (30%). The only category where a greater proportion of practitioners felt there was a limitation was the legal aspects. The reasons for this are unclear; however, it is likely practitioners have to contend with the legislative aspects in reality on a more regular basis than researchers and are thus subject to the difficulties.

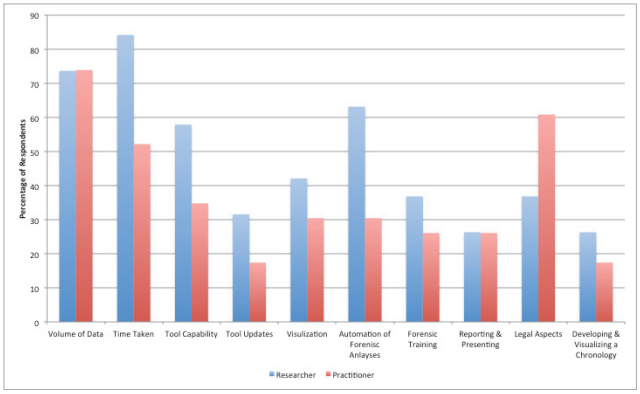

Figure 2. Principal Limitations to Investigations

Further examining the opinions of the stakeholders, participants were asked if restricting or limiting investigations to cases of high importance could be a viable approach as it would assist in releasing more investigative resources. Overall, only 9 of the 42 responses felt this would be a useful policy; interestingly, 7 of those responses were from practitioners. There are clear reasons why such a policy would be difficult to invoke in practice – how would one decide what was important until after the investigation? Furthermore, relying upon triage tools or automation alone could introduce an unacceptable level of error. However, it is clear that the volume of data and time taken results in investigations is becoming increasingly and prohibitively expensive. With the explosion of data and technologies, at what point does the traditional model of digital forensics become infeasible.

An analysis of current tool capabilities reveals an interesting perspective. Overall, the consensus is that tools reside in the middle of spectrum (neither too few or fit for purpose) with a slight skew towards being more capable than not (as illustrated in **Figure 3**). However, exploring capability based upon the forensic category (e.g. computer, network, embedded and mobile) suggests an order to the capability, with computer forensic tools being largely fit for purpose and subsequent categories declining in capability, in the order of mobile, network and finally embedded. This trend arguably matches the market maturity, with computer and mobile-based tools being far more widespread. It is notably that few feel any of the tools are completely fit for purpose. A further examination based upon stakeholder perspectives reveals the same trend. This is somewhat contradictory, as it might be expected that researchers (who are specifically tasked with developing solutions that current tools do not have the capability for and are therefore potentially more aware of the missing capabilities) would have resulted in the selection of poorer current capabilities. However, that was not the case.

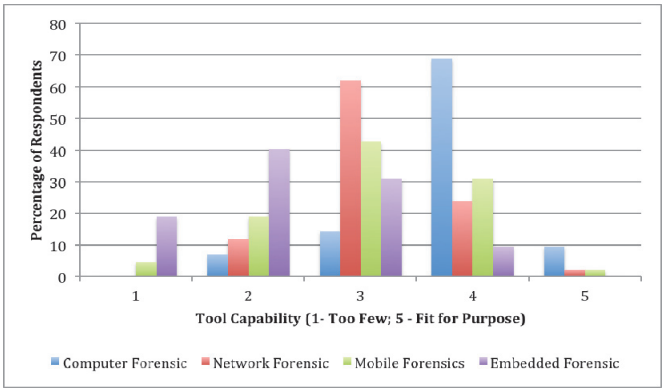

Figure 3. Current Tool Capability

Participants were asked a series of questions regarding how concerned they were with respect to a range of technologies that can have an impact upon forensic investigations. As illustrated in **Figure 4**, on average all of the technologies were skewed towards being concerned, with over 60% of respondents selecting 4 or 5 out of 5 in 5 out of the 7 categories. The two categories that that respondents appeared less concerned with were malicious software and steganography. It is unclear as to the reasons for this but perhaps they are at opposite sides of the same spectrum – investigators have been working with malicious software since the inception of cybercrime, and therefore are comfortable with the technology. Conversely, given the nature of steganography, its rather undetectable nature, it is not perceived to a problem because it (appears) not to exist. Arguably both encryption and steganography are a form of anti-forensics; however, given their significance, it was deemed important to extract them and have them considered in their own right.

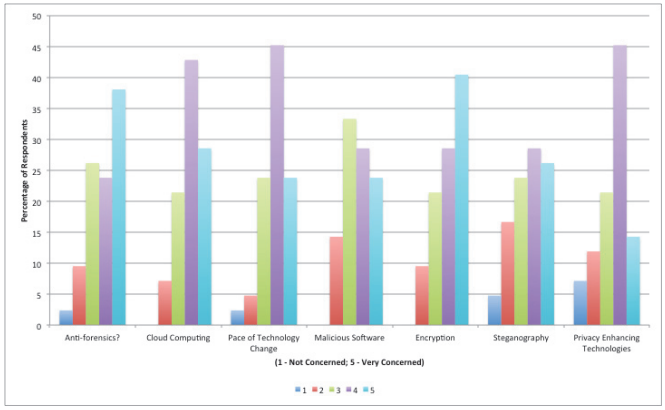

Figure 4. Technologies that Cause Concern

Upon asking respondents to rank the technologies, a slight difference results within the stakeholder perspectives. As illustrated in **Table 1**, researchers feel that cloud computing is the single highest priority, whereas researchers feel it is third after anti-forensics and encryption. Whilst both stakeholders agree encryption is a key issue, they differ on the remaining priority – with researchers suggesting the pace of technological change.

Table 1. Ranked Technologies that Cause Concern

	Priority		
	1	*2*	*3*
Researchers	Cloud Computing	Encryption = Pace of Technology	
Practitioners	Anti-Forensics	Encryption	Cloud Computing
Overall	**Anti-Forensics**	**Cloud Computing**	**Encryption**

To provide a better insight into the experiences of the respondent population (as this will likely impact upon their responses), participants were asked on how frequently they had undertaken investigations involving more advanced data hiding techniques. Of those to whom the question was applicable (i.e. had undertaken investigations) 66% responded that they had infrequently, with only 24% stating frequently. None had undertaken them on a very frequent basis. Whilst digital forensic challenges are well understood and documented, this finding suggests the impact of many of them has not yet manifested itself practically. This would suggest that whilst literature highlights the many technological issues that exist and the possible opportunities open to criminals, they are not currently utilizing them. Furthermore, the resultant issues that investigators focus upon are therefore those that have an immediate impact upon them.

Finally, respondents were asked how they felt towards the use of open source utilities and tools. Significantly, 69% of respondents consider open source tools as an important or very important aspect of tool development. Given the rapid pace of technology, it will become increasingly difficult to rely upon commercial vendors to provide all the necessary solutions, particularly in a timely manner.

C. The Future Challenges

A key aspect of the survey was to focus upon the (perceived) future challenges to digital forensics, with a view of enabling researchers to priorities them. Respondents were asked a couple of preliminary questions in this regard – whether they felt the field of forensics would be more or less challenging, whether investigations would take more or less time and whether investigations would be more sophisticated. Overwhelmingly, 93% of participants felt investigations would be more challenging in the future and more sophisticated, with 67% also of the mind it would take more time. Given the current challenges identified in the previous section, this presents a rather bleak outlook. Interestingly, 19% of participants did feel investigations in the future would take less time. Unfortunately, a subsequent question did not follow this up to understand why they felt this. Arguably however, given the increases in cases, increases in technology, increases in the volume of data and increases in the sophistication of analysis required, given current technology capabilities this will have to result in an increase in the resources required.

Exploring exactly where respondents felt increases would result gave rise to a set of interesting results – as illustrated in **Figure 5**. All participants, independent of their role, felt that investigators would experience an increase in mobile-based cases. However, with the remaining categories, a greater proportion of researchers than practitioners felt there would be increases. The largest difference between stakeholders opinions was with regards to the role embedded forensics will have – with 59% of researchers envisaging an increase in demand but this is accompanied with only 30% of practitioners.

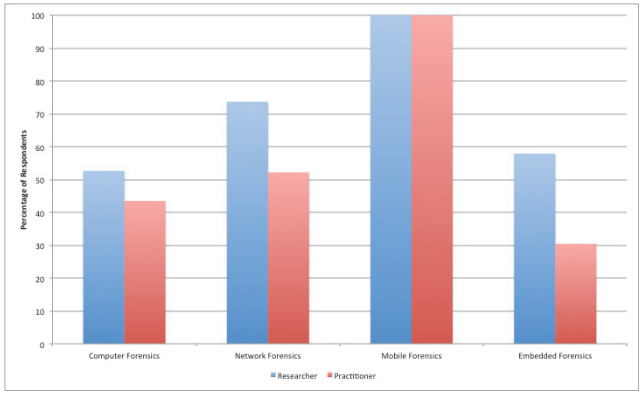

Figure 5. Increase in Forensic Investigations

Participants were also asked to rank the future challenges. Many of the categories were a duplicate from the current challenges, in addition to a number of broader categories such as tool capability, visualization and social networks. An analysis of **Figure 6** reveals a similar result to the earlier challenge question – with cloud computing, anti-forensics and encryption remaining high priorities. This is interesting from the perspective that participants not only feel these are current issues but that no tools or solutions exist (or arguably are on the horizon) to solve them in the future. This raises further questions are to why this is the case? In reality a mix of technological barriers and legislative impediments are likely reasons. Further down the list and challenges such as social networks, forensic analyses and network forensics come through as key priorities.

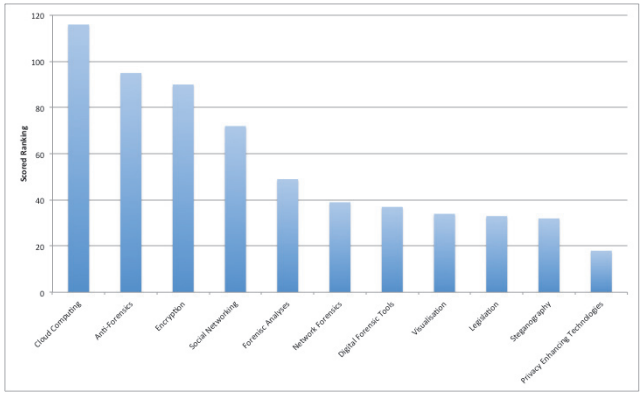

Figure 6.The Relative Ranking of Future Challenges

An analysis based upon stakeholder perspectives (as illustrated in **Figure 7**) show a similar outlook with respect to the key priorities such as cloud computing and encryption. However, they do differ with respect to a number of other priorities. Researchers feel anti-forensics, steganography and visualization to be less significant than practitioners. Instead,

they feel social networking, digital forensic tools, forensic analyses and legislation as more significant priorities.

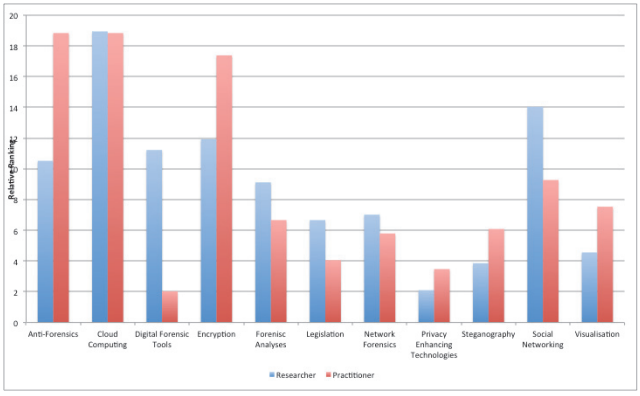

Figure 7. The Relative Stakeholder Ranking of Future Challenges

Given the challenges that exist, a number of questions were posed to participants with a view of examining their opinion towards approaches or technologies that could have an impact upon the challenges. Initially, they were asked if having the ability to identify and extract relevant evidence/artifacts was important. Overwhelming (83%), respondents felt this was a essential (with an average Likert score of 4.2).

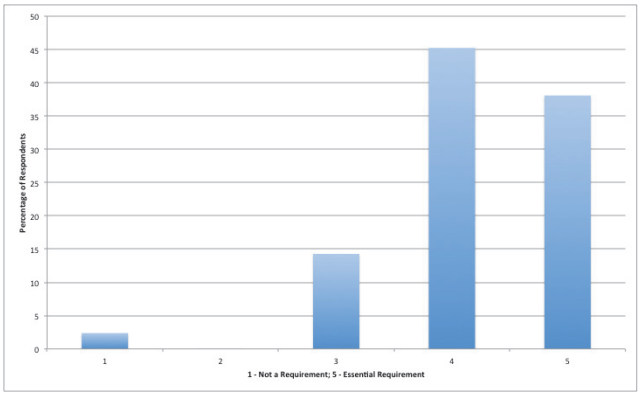

Figure 8. Importance of Identify Relevant Artifacts

A further question then asked whether criminal profiling could be an approach to identifying relevant artifacts. Theoretically, profiling offers the investigator the opportunity to more easily identify and extract relevant evidence. As illustrated in **Figure 9**, 85% of participants thought this was an important (or very important) area (average Likert score of 4).

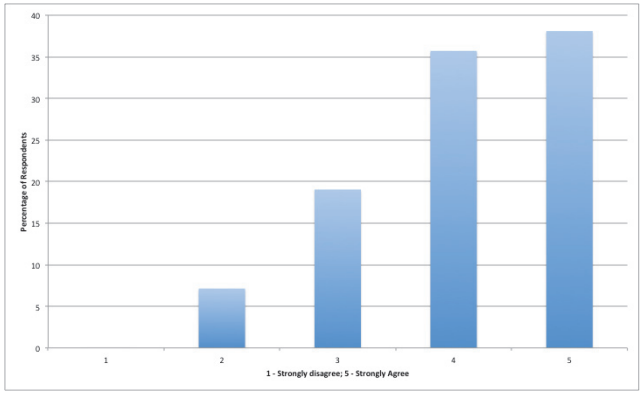

Figure 9. The Role/Application of Criminal Profiling in Digital Forensics

Two questions were then focused upon approaches that aid the aforementioned approaches. Overall, participants were very positive towards the use of such technologies. They were asked if they felt automation was an important factor in the future. Automation has the potential to remove a considerable volume of manual tasks. As illustrated in **Figure 10**, 58% of respondents felt it was important.

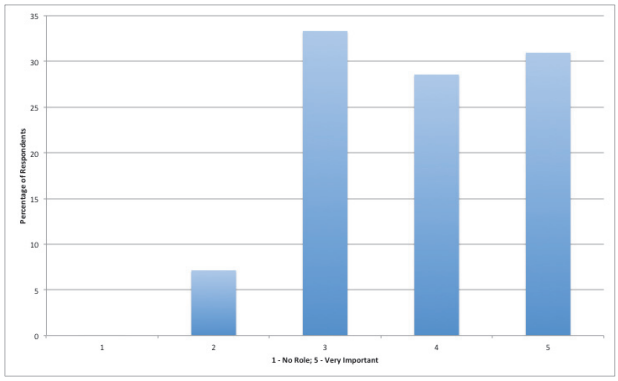

Figure 10. The Role and Importance Automation can have within Digital Forensics

The second question, specifically asked them whether artificial intelligence (AI) approaches could have a role in assisting investigators. Overall, the response was more mixed with an average Likert score of 3.7 - suggesting a slight skew towards using the approach. Whilst the use of AI has been successfully applied in a range of fields, including aspects of forensics, it will inevitably introduce errors which themselves would require verification by an investigator.

Finally, respondents were asked about the relationship between the researcher and practitioner communities – specifically whether it would benefit from improved communication and collaboration. Overwhelming, 93% of respondents felt the domain would benefit (Likert score of 4.6). As illustrated in **Figure 11**, the question resulted in the highest proportion selecting 5 out of 5 on the scale.

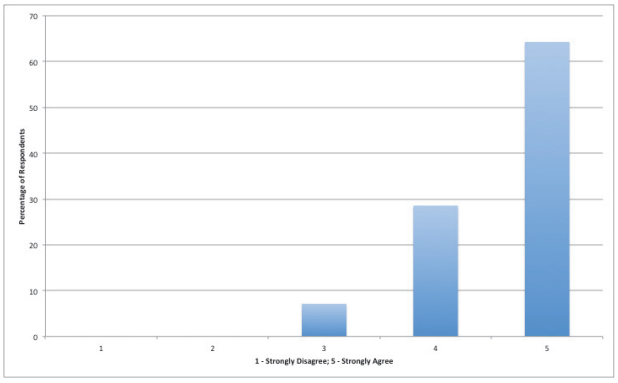

Figure 11. Improved Communication & Collaboration Between Stakeholders

An analysis of stakeholder responses to these questions revealed a close similarity, with no significant difference in opinions. This felt a little at odd to what would have been expected. Given these challenges are well known, it would have been expected that researchers would be more actively looking to such technologies to reduce the problem.

D. Legislative Aspects

The last section sought to explore how legislative aspects have an impact upon digital forensics. Asked whether they felt legislation was an inhibitor or enabler, participants were fairly even in their consideration – with an average Likert score of 3.3. As illustrated in **Figure 12**, this suggests a significant divide in the impact that legislation has. Whilst it is encouraging there is a very mild skew towards being an enabler, a 25% of respondents feel it is specifically an inhibiting factor.

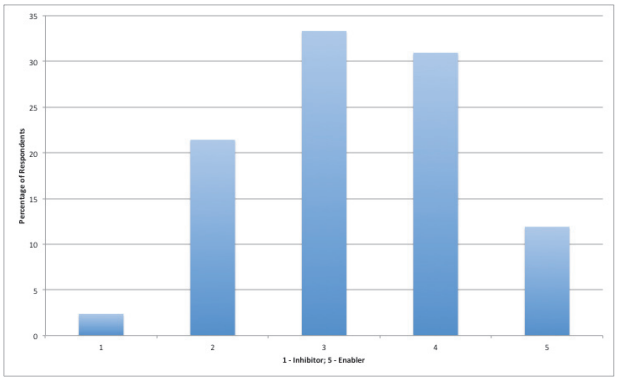

Figure 12. The Extent to Which Legislation is an Enabler or Inhibitor

Investigating the issue further, respondents were asked to what extent they felt legalization involving crossing borders was the issue. As illustrated in **Figure 13**, respondents did feel legalization involving different jurisdictions was a concern (74% and a average Likert score of 4).

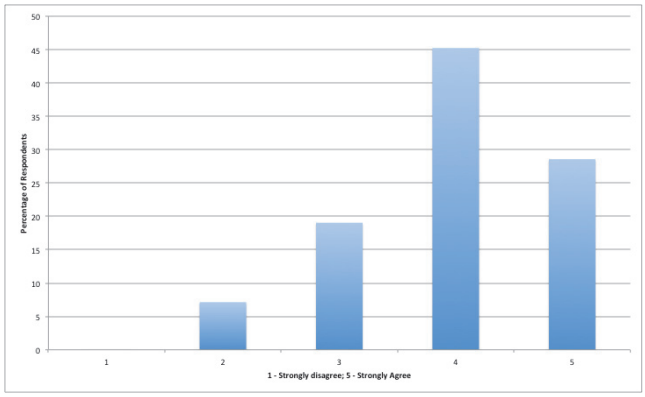

Figure 13. The Extent to Which Cross Border Legislation is a Barrier

The final question sought to examine to what extent current tools are capable of considering the legislative requirements. For example, limiting search and automated analysis to specific and permitted data areas but not others. This is required in countries where warrants provide permissions to analyze specific data areas and not others. For example, the USA has strong privacy laws that restrict investigators in what they analyze based upon what the suspect criminal activity is. Interestingly, respondents in general felt existing tools were capable of achieving this (as illustrated in **Figure 14**). However, to the author's best knowledge, none of the commercial tools are specifically equipped with the capability to take relevant national legislation into consideration. For example, data carving analyses will extract data from the complete image – not defined areas. It also requires the investigator to specifically understand the remit of the investigation and the nature of relevant legislation.

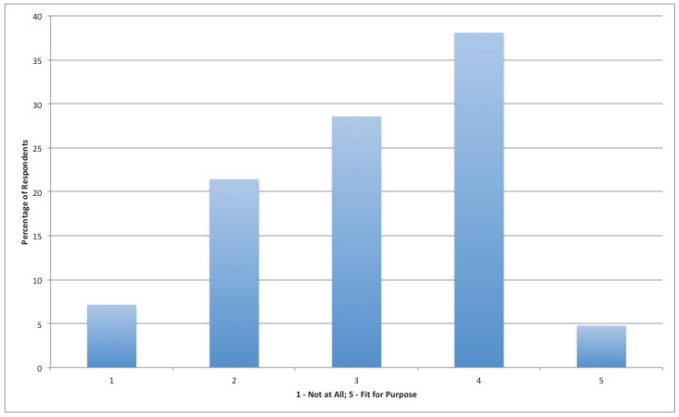

Figure 14. Forensic Tools Capable of Considering Legislation

IV. DISCUSSION

The survey has raised a number of considerations for the forensic community. Fundamentally, it has highlighted the importance and prioritization of key challenges. The domain of anti-forensics, including encryption and steganography, remain a significant current and future challenge for investigators. Unfortunately, with people becoming more mindful of information security, the further introduction of security within operating systems (e.g. full disk encryption within Microsoft and Apple Mac), the promotion of anti-

forensic technologies and wiping of media, the ability for investigators to locate relevant evidence will become increasingly challenging. As suggested by [4], forensic tools will have to become less focused upon identifying evidence that is criminal in its own right and become more intelligent in identifying artifacts that highlight misuse. For example, analyses will need to be developed that are capable of picking up trace evidence to the application of anti-forensic techniques. Whilst not evidence of the crime itself, it will provide invaluable intelligence to the examiner to how to best proceed.

There was an expectation when designing the survey tool, that given the wide range of challenges that exist within the domain, the responses to questions such as the current tool capabilities and current technology concerns would have revealed a higher proportion with the feeling that current approaches are not meeting the requirements. However, this was not the case. Without further information, it is difficult to suggest the reason for this; however, there does appear to be a disparity between the challenges and the impact they actually have in practice. For example, upon asking participants, what proportion of cases involved advanced data-hiding only 7 of the 42 respondents had on a frequent basis. If challenges are not manifesting themselves in practical cases, it is logically to assume these will have less of an impact.

The respondents have reaffirmed that the volume of data and the time taken to undertake an investigation are key limiting factors. Further exploring techniques and technologies for potentially reducing this issue resulted favorably suggesting future research should focus upon approaches such as criminal profiling and automation. In particular, [7] has presented an interesting application of criminal profiling to digital forensics. A key enabling technology in many other fields, AI, has provided approaches to data mine large volumes of data, have strong pattern associative capabilities and result in detection performances that outperform many other approaches [8-10]. There is some obvious concern over the applicability of such a technology within forensics; however, with careful implementation and configuration, AI techniques could become useful tools. It is likely such tools were reside initially within triage, with investigators still utilized to confirm their findings. However, as they advance and trust and reliability is established, AI-based approaches would be useful in dealing with standard cases (e.g. those that do not deploy advanced data hiding techniques).

The need for better communication and collaboration between researcher and practitioner communities is imperative for the creation of effective solutions particularly against the increasing range of challenges. Moreover, the nature of these challenges is incorporating a wider range of technology-based knowledge – forensics is no longer focused merely hard drive analysis but increasingly needing to understand complex distributed systems and innovative applications such as cloud computing and social networking. Researchers have the necessary knowledge but often lack the practitioner insight into problem.

Interesting, comparing the previous work by [4] with this research, almost a decade on, and some key differences and similarities appear. Whilst education/training was not an option provided in the list of current concerns, notably, it was not added in by any of the participants. Furthermore, an analysis of the respondents suggests a well educated and trained population. This suggests that training and education is an issue the industry has managed to contend with. However, issues of technology, encryption and tools highlighted in 2004 remain current and future challenges almost a decade on.

The findings have also highlighted significantly the increasing attention being given to developing areas of technology. Cloud computing and social networking were ranked in the top 5 future concerns. In one respect, the reason for this might be due to the changing location of the artifacts – moving away from the tried and tested hard drive onto systems that are complex, proprietary and not well understood by the forensics community [11]. However, these technologies also represent a second potentially more disconcerting trend – the behavior of individuals is changing. Increasingly individuals are no longer tied to a single computer, but instead have a multitude of devices and technologies with which they can access information. This will only increase and forensic investigators, procedures and tools are not designed for such examinations.

V. Conclusions & Future Work

The paper has presented a study that has both confirmed a number of challenges within digital forensics and also provided an understanding over their relative priority. Interestingly, amongst the usual suspects of anti-forensics and encryption, cloud computing and social networking have been identified as key future challenges.

Exploring the issues from the differing stakeholder perspectives of the research and practitioner did reveal some interesting aspects – with researchers focusing upon the new challenges and practitioners remaining focused upon issues that still have a direct impact. With the exception of cloud computing – which both parties agreed was the single top priority, practitioners highlighted for both the current concerns and future challenges, anti-forensics and encryption in the top three issues. However, for researchers, social networking and tool capability were amongst the top priority future challenges.

Future work must focus upon developing effective approaches to solving these challenges and provide a robust research environment that is proactively developing forensic-based solutions before practitioners identify them as issues. Future work must focus upon the technology horizon rather than merely "fire fighting" the issues. Consideration to forensic capabilities of evolving and new technologies needs to take place, so that a forensic capability exists at the outset of a new technology rather than years after the technology has been adopted (and misused!).

References

[1] Guidance Software, "EnCase Forensic v7", Guidance Software. Retrieved from http://www.guidancesoftware.com/encase-forensic.htm [Accessed 21/5/13]

[2] AccessData, “FTK – Forensic Toolkit”, AccessData. Retrieved from http://www.accessdata.com/products/digital-forensics/ftk [Accessed 21/5/13]

[3] M. Rogers, K. Seigfried, “The future of computer forensics: a needs analysis survey”, Computers & Security, vol. 23, no. 1, 2004, pp. 12-16.

[4] S. Garfinkel, “Digital forensics research: the next 10 years”, Digital Investigation, vol. 7, 2010, pp. 64-73

[5] G.G. Richard III, V. Roussev, “Next-generation digital forensics”, Communications of the ACM, vol.49, no. 2, 2006.

[6] A.J. Marcella, R.S. Greenfield, Cyber Forensics, Auerbach Publications, 2002.

[7] Rogers M. The role of criminal profiling in computer forensic investigations. Computers & Security, vol. 22, no. 4, 2003, pp. 292-298.

[8] S. Mukkamala, A. Sung, “Significant features for network forensic analysis using artificial intelligence techniques”, International Journal of Digital Evidence, vol. 1, no. 4, 2003.

[9] N. Beebe, J. Clark, “Dealing with terabyte data sets in digital investigations, Advances in Digital Forensics, vol. 194, 2005, pp. 3-16.

[10] B. Hoelz, C. Ralha, R. Geeverghese, “Artifical intelligence applied to computer forensics”, Proceedings of the 2009 ACM Symposium on Applied Computing, 2009, pp. 883-888.

[11] K. Ruan, I. Baggilli, J. Carthy, T. Kechadi, Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability: a Preliminary Analysis’, Proceedings of the 6th Annual Conference of the ADFSL Conference on Digital Forensics, Security and Law, Richmond, Virginia, USA.