DF-C²M²: A Capability Maturity Model for Digital Forensics Organisations

Ebrahim Hamad Al-Hanaei
Security Lancaster Research Centre
Lancaster University, UK
e.alhanaei@lancaster.ac.uk

Awais Rashid
Security Lancaster Research Centre
Lancaster University, UK
marash@comp.lancs.ac.uk

***Abstract*— The field of digital forensics has emerged as one of the fastest changing and most rapidly developing investigative specialisations in a wide range of criminal and civil cases. Increasingly there is a requirement from the various legal and judicial authorities throughout the world, that any digital evidence presented in criminal and civil cases should meet requirements regarding the acceptance and admissibility of digital evidence, e.g., Daubert or Frye in the US. There is also increasing expectation that digital forensics labs are accredited to ISO 17025 or the US equivalent ASCLD-Lab International requirements. On the one hand, these standards cover general requirements and are not geared specifically towards digital forensics. On the other hand, digital forensics labs are mostly left with costly piece-meal efforts in order to try and address such pressing legal and regulatory requirements. In this paper, we address these issues by proposing DF-C²M², a capability maturity model that enables organisations to evaluate the maturity of their digital forensics capabilities and identify roadmaps for improving it in accordance with business or regulatory requirements. The model has been developed through consultations and interviews with digital forensics experts. The model has been evaluated by using it to assess the digital forensics capability maturity of a lab in a law enforcement agency.**

Keywords—Digital Forensics, Capability Maturity, ISO 17025, ASCLD-Lab.

I. INTRODUCTION

To date digital forensics labs that have implemented a quality management system with the view of gaining international accreditation have mostly done so by adopting and implementing the ISO/IEC 17025:2005 standard or the ASCLD-LAB International requirements. This has been driven by regulatory constraints, for instance, by the European Union as seen in Article 12 of Regulation (EC) No 882/2004[1] which states that to be designated as a recognised laboratory, laboratories have to be accredited in accordance with EN ISO/IEC 17025 on general requirements for the competence of testing and calibration laboratories. Consequently, in the absence of any defined accreditation standards for digital forensics labs, ISO 17025 and similar standards are being adopted (rather than adapted) to address the need for standardisation and accreditation along with some well-intended best practices and country specific legal requirements (where applicable). But their shortcomings and pitfalls when looking at non-traditional disciplines such as digital forensics are being overlooked due the lack of a viable, reliable, and alternative.

As a standard designed for test and calibration laboratories, ISO 17025 has proven to be good at helping enforce a quality management system and basic competency management system within digital forensics labs, but it has proven to be costly – both in terms of time and resources to implement and maintain. This is because the standard was designed for the more "traditional" forensic science disciplines such as chemical testing. Mapping and adapting the requirements to digital forensics can be subject to 'interpretation' by the ISO 17025 assessors and the examining body's Board of Directors, who often hail from a traditional scientific discipline such as Pharmacology and have limited understanding of digital forensic principles, accepted best practices and what is feasible, practical, acceptable and achievable.

Further compounding the situation are the increasing budgetary constraints affecting most digital forensics labs. They are limited as to how many personnel they can continue to recruit and train as well as the skill sets they can maintain, whilst the volume of cases referred to such labs and the volume of data requiring analysis continues to grow. Three years ago the maximum amount of data on a smart phone was perhaps 8GB. Today devices with 64GB storage are common and computer systems with hard drive capacities in excess of 500GB continue to be the norm. With case backlogs growing, labs are increasingly faced with the option to triage and preview cases (rather than conducting full-scale examinations), or to implement process automation (where possible), or look at adopting business process maturity models to see how they can effectively measure and improve their capability and process maturity. To date no model or framework exists that addresses the capability maturity requirements of digital forensic labs. Labs are mostly left with costly piece-meal efforts in order to try and address the various pressing legal, regulatory and business requirements.

In this paper, we address these issues by proposing a Digital Forensics Comprehensive Capability Maturity Model (DF-C²M²). Capability maturity models [6] have seen

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2004R0882:20060525:EN:PDF.

DOI 10.1109/SPW.2014.17

significant application and success in other disciplines such as software engineering. However, their applicability in digital forensics has remained largely unexplored.

The novel aspects of the DF-C²M² model are as follows:

- The model is based on the same principles as used by the Open Source Security Testing Methodology Manual (OSSTMM) 2 . This enables digital forensic labs to implement the core accreditation requirements equivalent to ISO 17025 but adapted and designed to specifically suit the realm of digital forensics.
- The model enables measuring maturity along three key dimensions: people, processes and tools while enabling such an assessment to be tailored to a particular type of organisation, e.g., law enforcement or non-law enforcement setting.
- The model has been operationalised in a tool that enables organisations to measure their digital forensics capability maturity and identify roadmaps for improvement.

The rest of the paper is structured as follows. Section II provides an introduction to capability maturity models. Section III presents the DF-C^2M^2 model. Section IV presents the tool and its various features. Section V summarises evaluation of the model in a real law enforcement digital forensics lab. Section VI discusses related work. Section VII concludes the paper and identifies directions for future work.

II. Capability Maturity Models (CMM)

A CMM [6] is a framework for evolving an organisation from an ad hoc, less organised, less effective state to a highly structured and highly effective state. Use of such a model is a means for organisations to bring their practices under statistical process control in order to increase their process capability. A common misconception is that CMMs define a specific process. CMMs provide guidance for organisations to define their processes and then improve the processes over time. The guidance applies regardless of the particular processes that are performed. CMMs thus describe what activities must be performed to help define, manage, monitor, and improve the organisation's process (es) rather than exactly how the specific activities must be performed.

Based on analogies in the software engineering and other communities, some results of process and product improvement can be predicted. A first improvement expected as an organisation matures is predictability. As capability increases, the difference between targeted results and actual results decreases across projects. A second expected improvement is control. As process capability increases, incremental results can be used to establish revised targets more accurately. Alternative corrective actions can be evaluated based on experience with the process. As a result, organisations with a higher capability level will be more effective in controlling performance within an acceptable range. A third expected improvement as an organisation matures is process effectiveness. Targeted results improve as the maturity of the organisation increases. As an organisation matures, costs decrease, development time becomes shorter, and productivity and quality increase.

[2] http://www.isecom.org/research/osstmm.html

III. DF-C^2M^2 Model

The model is rooted in a comprehensive online survey of digital forensics experts in private labs and in law enforcement agencies as well as direct interviews with such experts. Furthermore, the model also draws upon the authors' practical experience of working in digital forensics labs or settings involving digital forensics.

The model provides a method to define, assess and measure maturity levels across the digital forensic lab and a feedback and rating system to allow organisations to plan for improvement and (collectively) to benchmark their maturity level against other comparative. The maturity of digital forensics capability can be at 6 levels (0 … 6) – 0 being the least and 5 being the most mature.

Level 0 – Person-Dependent Practices: This is for instances where the activity being performed is not documented. In other words, it is not recorded either in outline or in detail. The activity is entirely person dependent and the sequence, timing and result may vary during repetition. This requires a lot of supervision. There is no guarantee of either achieving the desired result or adhering to timelines. The activity is entirely ad hoc, with little communication between functions. The effectiveness of the activity is entirely dependent on individuals. Knowledge transfer may or may not happen if there is any change in the owner of the activity.

Level 1 – Documented Process: At this maturity level, there is a document that has been reviewed and approved by the supervisor or the approving authority as the standard process. But it may be doubtful that the activity being performed is as per the document. This may be because of a process drift or some drastic change since the document was drafted.

Level 2 – Partial Deployment: Here, the activity that is documented is being deployed, but there is inconsistency in the deployment. The process may not be deployed in totality. That is, it may not be deployed at all the intended locations, or though all functions, or by all the intended owners, or all the activities defined in the process are not being performed. This would mean that the document has not been designed to cater to such variations. There is inconsistency in results of different process owners.

Level 3 – Full Deployment: At this level, there is no inconsistency between the documented process and the deployed process. The process documented and deployed caters to all the intended locations, owners and all the activities that need to be performed. The process also shows seamless linkage between functions and other processes wherever there needs to be any interaction. This means that the process shows greater consistency of actions and better communication between functions.

Level 4 – Measured and Automated: The process has set itself goals such as adherence to timelines, customer

satisfaction, cost, etc. The process is also being measured against its goals. The process is system-driven by enablers such as using enterprise resource planning or customer resource management or any other custom-made software.

Level 5 – Continuously Improving: The goals set for the process are being analysed for achievements and improved regularly. The timelines, cost targets, satisfaction levels are being achieved regularly and the targets are also being tightened by using continuous quality improvement techniques such as Six Sigma and Kaizan, etc. The enabling system also is being improved and being made error-free by strategies such as mistake proofing.

IV. DF-C²M² ASSESSMENT AND EVALUATION TOOL

The DF-C²M² model is supported by a tool that enables an organisation to:

- Assess and measure its digital forensics capability and its maturity;
- Plan digital forensic services pertaining to people, tools, and processes;
- Quickly utilise a knowledge base and repository of procedures, policies, forms and validated test methods;
- Determine skills profiles;
- Implement training and corrective actions;
- Plan and monitor improvements

The tool provides a menu to allow the assessor to tailor the requirements to a particular organisation type i.e. Law enforcement (LE), non-LE organisation, judiciary, etc. and the role of the unit, e.g., digital forensic examinations of cybercrime investigations. For each organisation type, a service catalogue of planned or proposed services is provided. This catalogue covers services in several categories, namely:

- Computer Forensics;
- Mobile Device Forensics;
- Digital Audio Forensics;
- Digital Video Forensics;
- Live and Network Forensics;
- Cybercrime Analysis services;
- Digital Evidence Handling Support services.

These categories of services cover the range of services that digital forensics labs or units may be required to provide to the customer base.

From a strategy and planning perspective, the service catalogue may also serve as a roadmap of which services a digital forensics Lab would like to implement over say a three-year plan, and identify which services from the list are essential to the unit's goals, objectives and success, and which services should be considered as optional. Based on the service catalogue, an organisation would be able to more effectively design a roadmap for implementing these services. Furthermore, by identifying the process, tools and skills requirements for each service the organisation can more accurately determine costs for implementing such services, the relative value of each planned service and also factor in the most pressing demand and requirements from the customer base.

As shown in Figure 1, using the tool, an organisation can assess its digital forensic maturity level from case assessment (initial report) through to analysis of results and quality assurance review. Figure 2 shows the overall dashboard view of an organisation's digital forensics capability maturity while Figure 3 shows a zoomed-in view of the competency maturity of particular digital forensics examiner and investigator roles.

Category	Score	Average/5	Maturity Level
Assessment	71	3.94	Level 3 - Full Deployment
Collection	102	3.92	Level 3 - Full Deployment
Examination	119	3.97	Level 3 - Full Deployment
Analysis	40	4.00	Level 4 - Measured & Automated
Reporting	49	4.08	Level 4 - Measured & Automated
Review	18	3.00	Level 3 - Full Deployment
Overall Score		399	
Overall Maturity		3.82	

Figure 1: DF-C²M² Tool: Maturity Level Assessment

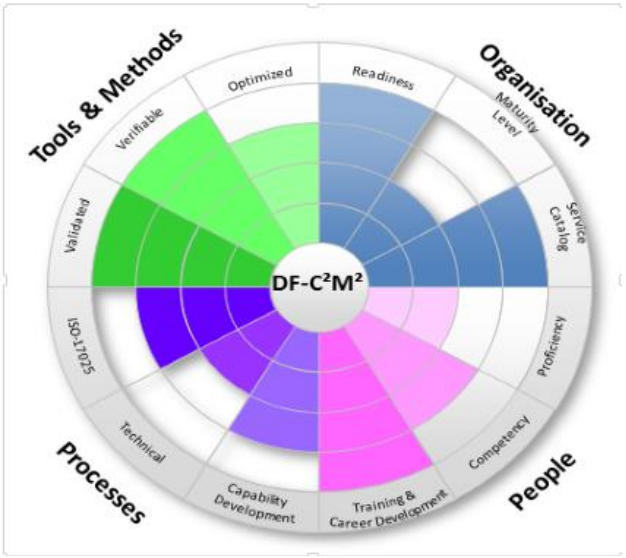

Figure 2: DF-C²M² Dashboard – Overview of Maturity along different dimensions

V. EVALUATION

We have evaluated DF-C²M² in a law enforcement digital forensics lab in order to study its effectiveness in assessing the maturity of digital forensics capabilities in real-world scenarios. The evaluation took the form of a 'consultative audit' and was conducted on-site by one of the authors. This involved introductory meeting and overview with key stakeholders; reviewing processes and documentation; interviews with key administrative and a subset of select

technical personnel; an interactive discovery workshops on DF-C²M²; observing tasks and procedures; review of customer feedback; review of any relevant supporting documentation and records and a summary and final report of findings including a SWOT analysis based on DF-C²M².

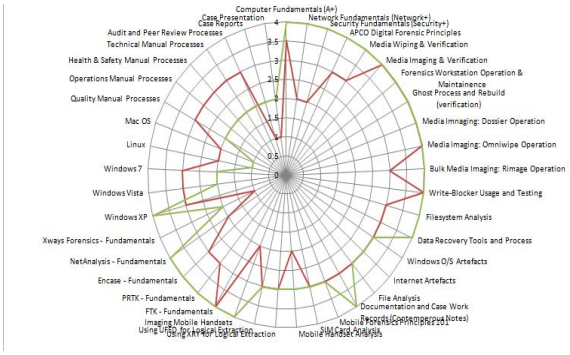

Figure 3: Zoomed-in view of assessment of competencies of particular roles

Table 1: Summary of DF-C²M² Findings

Category	Score	Max.	Avg./5	Maturity Level
Assessment	51	90	2.83	Level 2
Collection	70	130	2.69	Level 2
Examination	97	150	3.23	Level 3
Analysis	35	50	3.50	Level 3
Reporting	49	60	4.08	Level 4
Review	18	30	3.00	Level 3

The findings of DF-C²M² are summarised in Table 1. As shown, the lab had a reasonably mature set of processes, competencies and tools in place in the lab. The areas of least maturity were with regards to assessment and collection. This is because, the lab in question was not solely responsible for collection and handling of digital evidence at crime scenes and, in view of the fact that most departments in the organisation had not been trained in Digital Evidence Handling; there was significant room for improvement for the organisation. Furthermore, we identified crosscutting gaps with regards to non-implementation of training plans at times, which led to fast-tracking of personnel without pre-requisite courses. The reporting aspects were the most mature. In addition, to the above gaps, DF-C²M² helped to identify roadmaps with regards to process automation and advanced skills development.

VI. Related Work

A number of reference models for digital forensics have been proposed in literature to date. A full review is beyond the scope of a short paper. Here we highlight some of these models. Palmer [5] defined a generic investigation process that can be applied to all or the majority of investigations involving digital systems and networks. Carrier and Spafford proposed [3] a digital investigation process framework was based on the investigation process of physical crime scenes. They define the digital crime scene as the virtual environment created by software and hardware where digital evidence of a crime or incident exists. Baryamureeba and Tushabe [1] enhanced this framework by separating the investigations at the primary and secondary crime scenes while depicting the phases as iterative instead of linear. Beebe and Clark [2] proposed a multi-tier process after they reviewed that most of previous forensic frameworks were single tier process but in fact the process tends to be multi-tiered. Kohn et al. [4] proposed a new framework by merging several existing frameworks. In this framework, two requirements have been identified as needed at every level namely, the legal requirements of a specific system and documentation of all the steps taken. In these and other works, the focus has remained on elaborating or enhancing the investigative process. Capability maturity assessment and operationalising this into roadmaps, as is the case in the present paper, have not been considered to date.

VII. Conclusion and Future Work

In this paper, we have proposed a capability maturity model for digital forensics. The model is aimed at enabling organisations to measure their maturity, identify and prioritise areas for improvement. This enables organisations to build roadmaps for future improvements to reach desired capability maturity levels. The model is supported by a tool that provides visual representations of capability gaps and strengths. Our evaluation in a real-life law enforcement lab has shown promise that the model is able to identify key areas of improvement that are of relevance to particular operational contexts. Our work in the immediate future will focus on further evaluations in such real-life settings which will then be used to feedback and improve the model and the tool. We also aim to contribute to relevant standardisation or accreditation initiatives that may be aimed at bridging the gap from general competency standards to those specifically aimed at digital forensics.

VIII. References

[1] V. Baryamureeba, F. Tushabe, "The enhanced digital investigation process model", Proceedings of the Digital Forensic Research Workshop, Baltimore, MD, 2004.

[2] N. L. Beebe, J. G. Clark, "A hierarchical, objectives-based framework for the digital investigation process", Proceedings of the Digital Forensic Research Workshop, Baltimore, MD, 2004.

[3] B. Carrier, E. H. Spafford, "Getting physical with the digital investigation process", International Journal of Digital Evidence, 2003.

[4] M. Kohn, J. Eloff, M. Oliver, "Framework for a digital forensic investigation", Proceedings of Information Security South Africa (ISSA) from Insight to Foresight Conference, 2006.

[5] G. Palmer, "A roadmap for digital forensic research", The digital forensic research working group, 2001.

[6] M. C. Paulk, B. Curtis, M. B. Chrissis, C. V. Weber, "Capability maturity model, version 1.1", IEEE Software, 10 (4), pp.18-27, 1993.