A Digital Forensics Capability Maturity Model for Organizations

Dr. Timothy Proffitt

Lonestar College, Email timothy.g.proffitt@lonestar.edu, tim@timproffitt.com

Abstract: Digital forensics is continuing to be a vital, expanding, and relevant technology field. Investigations in law enforcement, private investigators, human resources teams, and cybersecurity may heavily rely on digital forensics. Digital forensics may be conducted by an individual or a team in a manner that fails to produce relevant or complete judgments for a stakeholder. To assist in improving the digital forensics method used by a team or individual, this research created a model to provide measurements of key forensic capabilities.

Key words: Capability Maturity Model Integration, digital forensics, investigations, digital evidence, litigation support, DFIR, mobile device security, hard drive forensics.

1. Introduction

A forensic analyst will commonly proclaim that the technology you own will betray you. Additionally, it can be difficult to find an organization or entity that does not rely on some form of technology for its core processes. According to Garfinkel (2010), digital forensic analysis has become a desirable request for all manner of investigations. Technology consistently produces data, metadata, and logging evidence. Securing an organization’s sensitive data and infrastructure has become a priority and attacks against those targets are becoming more sophisticated. Karie and Karume (2017) described the rising threats of cyber-crimes against organizations and the need to implement processes to adequately respond with digital forensic capabilities. With the increase in cyber-crimes, entities will want to provide equal increases in the efforts of maturing forensic investigations.

The purpose of this research was to present a Capability Maturity Model Integration (CMMI) based model for digital forensics. A stakeholder of a digital forensic team may use the model as a mechanism to measure an organization’s digital forensic capabilities. The model could also help teams to understand what gaps may exist in their current state and what steps could be followed to reach a more mature level. The model provides a calculated score that may be used to understand an overall maturity level of the forensics program. This Digital Forensics Capability Maturity Model Integration (DFCMMI) model was tested in multiple organizations by digital forensic experts for usability, clarity, and applicability.
This research is structured in the following format. The first section describes the CMMI and the literature review of the common digital forensic frameworks that provide an understanding of DFIR best practices. The second section describes the research conducted to produce the model and the third section provides the DFCMM and results. The fourth section outlines the use of the tool and the fifth section provides conclusions and directions for future research.

2. Related Works

This section provides a literature review on the field of digital forensics processes, capability maturity models, and organizational best practices for forensic teams. The concept of digital forensics came about from the body of knowledge on forensic science and digital forensic investigations can have a variety of concentrations. Stemming from the computer revolution in the late 1970s, the most common form of digital forensics was to support criminal or civil cases where evidence could be found in the technology being used. Forensics in the private sector may include corporate investigations of employees, fraud, and cyber-intrusion investigations. The 1978 Florida Computer Crimes Act provided the first legislation by which a person could be prosecuted and was eventually followed by the federal Computer Fraud and Abuse Act of 1986. Since that time, digital forensics on servers, laptops, desktops, networking devices, cloud infrastructure, and mobile phones has greatly increased.

2.1 Capability Maturity Model Integration (CMMI)

The CMMI is a popular framework for evaluating or appraising where an organization’s maturity ranks within a defined program. The CMMI could show where an organizational program is ad-hoc and unorganized as compared to a highly structured and repeatable program. The CMMI was originally developed by the Software Engineering Institute, a cohort of government groups, and industry experts. The CMMI was originally designed to have an application towards software engineering but was quickly generalized to other areas of program appraisal. In January of 2013, the CMMI Institute was formed at Carnegie Mellon to continue the research and dissemination of the framework. Practitioners should take notice that the CMMI is not a standard and does not provide detailed information about achieving the goals being measured. The framework was more designed to serve as a guideline to understanding current implementations and alternative mechanisms to implement maturity levels in the program.

The CMMI defines a capability model method to measure levels across the framework. The five maturity levels are defined as initial, managed, defined, quantitatively managed, and optimizing. The CMMI framework offers a statistical means for organizational management to rank and understands how to improve the process being evaluated. A CMM should provide guidance on what actions can be performed to improve the process rather than explicitly listing steps to achieve the next level of maturity. Al-Hanaei & Rashid (2014) explained that as the organization capability increases, the results produced will better align with expectations and accuracy. As results improve from the CMM, an organization should experience decreased costs, decreased development time, increased productivity and increased quality.

2.1.1 Defining the CMMI Levels

- CMMI level 0 is defined as incomplete. At level 0, processes are not executed or are executed incorrectly. Processes are
executed with no goals and without clear standards.

- **CMMI level 1** is defined as *performed*. At level 1 processes are chaotic and ad hoc. At this level, an organization would not expect a stable outcome and productive activities at this level are attributed to the experience of the person or team involved. Organizations at this initial level would not expect a quality outcome from this process.

- **CMMI level 2** is defined as *managed*. Visibility has been provided for management to understand the status of the processes and controls are in place. At the managed level, services are expected to follow project plans that meet standards and requirements.

- **CMMI level 3** is labeled as *defined*. At the level the defined level, processes are clearly understood, documented, followed, and consistent. Defined mature processes are improved by the attributes of greater detail, proactive quality controls, deeper understanding of relationships, and detailed metrics.

- **CMMI level 4** is defined as *quantitatively managed*. This level exhibits a program by which subprocesses are reviewed by statistical means to improve control over the larger processes. Detailed measurements are collected and analyzed. Variations would be identified and analyzed for improvements to quality. Level 4 processes are more mature than a level 3 processes by the quantitative measurements that are taken and used for decision-making.

- **CMMI level 5** is *optimized*. At level 5 processes are continually improved through technology innovation. Improvements are measured and evaluated. The organization's ability to quickly impart change as opportunities is a result of a cycle of constant process improvement. Level 5 processes are at a higher maturity because of the analysis of variations and predictability.

CMMI maturity levels cannot be skipped or passed over. The more mature levels are built on the success of the lower levels. The CMMI Institute claims that an organization at a lower maturity level can attempt to perform processes at a higher level but must understand that there is a risk of inconsistency. Overall, the CMMI provides an easy framework that can be modified to fit most situations and in the case of this research, can be used to show maturity levels of a digital forensic program.

### 2.2 Understanding Common Digital Forensics Frameworks and Guidelines

An experienced forensic investigator will follow a common guideline either mandated by their organization or a method in which they have been trained. Standardizing on a forensic guideline has many benefits and most of the advantages derived from a commonality of processes and the ability to contrast results across investigations (Jafari & Satti, 2015; Selamat, Yusof & Sahib, 2008). To better understand how to measure an organization’s maturity of digital forensic processes, a review of the common digital forensic models is needed. Salamat’s research described 13 different digital forensic investigation frameworks that could be leveraged by an organization or individual to complete an investigation. The digital forensic frameworks published in the body of knowledge have a common analysis process and can vary from four phases up to 21 phases. Common to most process models are the phases of collection, examination, analysis, and reporting. This section provides a literature review of the common digital forensic models found in the industry.

#### 2.2.1 A Framework for Digital Forensic Science (DFRWS Conference)

The DFRWS conferences produced a model titled “Road Map for Digital Forensic Research” that described the six-step process of identification, preservation, collection, examination, analysis, and presentation of digital forensics (Jafari & Satti, 2015; Palmer, 2001; Pollitt, 2007; Reith, Carr, &
This model explained that forensics is not a single process but a grouping of tasks that distill into functions. These functions are based on the role of the investigation and bounded by constraints defined by a set of requirements. The DFRWS framework was designed to be extended, refined, introduce a DFIR vocabulary and used as a practice tool.

2.2.2 NIST Special Publication 800-101

The SP 800-101 was published by the National Institute of Standards and Technology as a guideline for performing forensics on mobile devices. According to Ajijola, Zavarsky, and Ruhl (2014), 800-101 provides a unique in-depth look at applicable technologies and the corresponding connections to specific forensic procedures. Ayers, Brothers, Jansen (2014) claimed the 800-101 publication provides procedures for validation, preservation, acquisition, examination, analysis, and reporting. The publication defines mobile forensic toolsets, preservation procedures, acquisition, and examination. A classification system is described that allows investigators to easily compare extraction methods of differing toolsets. Evidence preservation objectives are clearly outlined for securing the scene, documentation of scene, communication shielding, and onsite processing. Additionally, the 800-101 publication explains the acquisition process in steps of identification, tool selection, device memory acquisition and device considerations (Yang & Lai, 2012).

2.2.3 Abstract Digital Forensics Model (ADFM)

Reith, Carr, and Gunsch (2002) presented the ADFM as an enhanced model based on data from DFRWS. ADFM composes of nine phases that included investigation, preparation, approach, presentation, collection, examination, analysis, preservation, collection, examination, analysis, presentation and returning. The ADFM model introduced a comprehensive pre and post-investigation procedures that had not been previously defined. The added phases in the ADFM, as compared to the DFRWS, focused on the end of the investigation. Presentation of the findings and relinquishing the evidence were detailed.

2.2.4 Systematic Digital Forensic Investigation Model (SDFIM)

Agarwal, Gupta, Gupta, and Gupta (2011) presented SDFIM based on the DRFWS model. The SDFIM was designed to provide a detailed approach for practitioners to build applicable policies and procedures. The SDFIM describes an eleven-stage model. Emphasis is placed on the stages that include documentation of scene, communication shielding, evidence collection, preservation, and examination.

2.2.5 Integrated Digital Investigation Process (IDIP)

Carrier and Spafford (2003) integrated all available models and investigative procedures at the time of the research into a map of their digital investigative process. This framework is organized into five groups consisting of 17 phases. Readiness, deployment, crime scenes, investigations, and review comprise this process. The IDIP highlighted a review phase in which the whole investigation is reviewed in order to note improvements that could mature the next investigation.

2.2.6 ISO/IEC Standard 27037

The 27037 standard provides guidelines for identification, collection, acquisition, and preservation of digital evidence. The intent of the
authors was to provide a practical platform for digital forensic investigators to facilitate the usability of evidence (Ajijola, Zavarsky, and Ruhl, 2014). Veber & Smutny (2015) claimed this ISO focused on the collecting and storing of the evidence above other processes in a traditional forensics model.

2.2.7 Network Forensic Generic Process Model (NFGPM)

Fenu & Solinas (2013) and Pilli, Joshi, and Niyogi (2010) described the NFGPM as a 9-phase forensic standard. Network forensic is applicable in environments where security tools are deployed in egress points that allow packet inspection. The detection phase in NFGPM is initiated from alarms generated by the security tools rather than the investigator being called to the crime scene. The incident response phase is then conducted by the team to better understand the alarm and whether to incident needs to be elevated into a formal response. Collection, preservation, examination, and analysis in NFGPM then aligns with the other models such as the DFRWS.

2.3 Other Forensics Based CMMI

The literature review revealed other models based on the CMMI framework. AL Hanaei & Rashid (2014) created the DF-C-M that was focused on creating a modular management decision framework. Al Hanaei’s model utilized assessments and planning tools to measure compliance. The DF-C-M model was designed to fill the gaps of ISO 27037, ISO 27041 and other models rather than a direct tool to measure maturity. Kerrigan’s (2013) framework, A capability maturity model for digital investigations, was based on a CMMI and focused on regulatory crime, entities in Ireland, response rates, and computing devices. The Kerrigan model is a heavily cited paper and provided a good primer for measuring a forensics program, however, this model is missing newer areas of forensics, such as network-based artifacts that are being incorporated into this research.

3. The research

The development of the DFCMMI provided a mechanism to benchmark the maturity of a digital forensic program. According to Kerrigan (2013), digital evidence plays a significant role in any investigation that may be conducted by an organization or law enforcement. From the literature review of the existing frameworks and models covered in the above sections, it can be understood that most of these frameworks have similar approaches. Some frameworks focus on certain areas of the investigation while others in different areas. However, all of these processes work toward a common goal and often utilize the same toolsets and procedures. This research proposed a maturity model by applying the CMMI to the common processes and steps of the digital forensic frameworks found in the body of knowledge. This grouping process was designed to achieve a forensic CMMI that allows entities to better understand what the next steps could be to improve their specific digital forensic investigations. This research approach involved a literature review, qualitative style interviews of subject matter experts, and testing of the model in several organizations.

3.1 Constructing the Model

In the initial phase of building the DFCMMI model, sections were constructed based on the literature review and experience of the researcher. The DFCMMI was then shared with digital forensic experts to be applied as a tool in a corporate organization or relevant environment. Qualitative data was then collected from the participants on the application of the model, feedback on the descriptions found within the DFCMMI, and answers from a short questionnaire on the use of the model. The feedback was then incorporated
into the model and sent back to the participants to ensure their feedback was properly represented.

3.1.1 Experts

The DFCMMI was shared with DFIR experts and researchers for use in measuring a forensics program. Several experts were invited to join in this research and 9 provided data for this research. Qualitative data collected was collected from the participants to be analyzed in improving the first draft of the DFCMMI maturity model. Suggestions by an expert were evaluated, potentially added to the model, and sent back out to the remaining participants in an updated release of the model. Any qualitative suggestions received in a consensus greater than 80 percent of the participants resulted in a change to the model.

3.1.2 Survey

The participants were provided a survey with the DFCMMI model to better understand the potential impact the model could have on the measurement of a digital forensics program. The qualitative survey asked the experts to rank different aspects of the model and to score the impact of the questions using a five-point Likert scale. The scale utilized the number five as strongly agree and one as the strongly disagree. The questionnaire and results are found in Appendix A.

3.1.3 Analysis of the Model

The overall phases of the DFCMMI were constructed based on the research conducted during the literature review and qualitative Likert results collected from the survey. According to the participants, the model scored 4.5 out of 5 in judgment as a valuable measuring tool. The survey results indicated that participants found the model to be easy to apply at 4.5, a clear intent at 4.5, and provided for understanding of where a program could be matured at 4.5, and as an intuitive application at 4.0. These results show that the model can be easily applied to an organization to quickly understand the maturity level of the forensics program and what necessary steps are needed for improvements.

3.2 Digital Forensics Capability Maturity Model (DFCMMI)

This research presented a digital forensics process model to be used as a tool to benchmark the maturity of an organization’s digital forensics program. The DFCMMI is defined by five major sections that include preprocesses, acquisitions, examinations, presentation, and management. The DFCMMI can be found in Appendix A.

3.2.1 Scoring Using the Model

The DFCMMI major sections have weighted scoring that increases as the forensics program aligns to the more mature objectives.

<table>
<thead>
<tr>
<th>Calculated Score</th>
<th>Level of Maturity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 20 points</td>
<td>Ad-hoc level</td>
</tr>
<tr>
<td>20 to 40 points</td>
<td>Reactive Level</td>
</tr>
<tr>
<td>40 to 60 points</td>
<td>Managed Level</td>
</tr>
<tr>
<td>60 to 75 points</td>
<td>Proactive Level</td>
</tr>
<tr>
<td>Greater than 75</td>
<td>Optimized Level</td>
</tr>
</tbody>
</table>

Table 1. Calculations for DFCMMI maturity.

When scoring a DFIR program that is currently aligning at an incomplete level, the program would receive a zero score. If the DFIR program aligns with the Managed-Optimized level, the program would score 4 points for that objective. The overall scoring from the DFCMMI of the forensic program may allow an organization or stakeholder to have a better understanding of what the present capabilities are and what steps can be taken to mature their program to the next level.
3.2.2 Preprocesses Section

The preprocess section of the DFCMMI model focuses on triage procedures, identification of devices on the scene, documentation of the scene, physically securing the evidence and isolation procedures. Measurements of the preprocess section may assist in understanding the improvements that can be made in preparation of the materials, sources, and evidence for acquisition by the forensics team. Processes in this section include onsite triage, identification, documenting the scene, physical device preservation, and evidence isolation.

3.2.3 Acquisition and Preservation Section

The acquisition and preservation section follows the securing of the scene and primarily deals with evidence collection. This phase includes drive acquisition, memory acquisition, network event collection, eDiscovery, hashing, and mobile device collection. Measurements of the acquisition and preservation section may assist in understanding the improvements that can be made in collecting the digital evidence from all applicable sources, mobile devices and necessary steps for the chain of custody.

3.2.4 Examination and Analysis Section

The examination and analysis section follows the acquisition section and primarily focuses on examining the contents of the digital evidence collected by the forensic examiner. This phase includes evidence analysis, forensic toolsets documentation, and e-discovery. Measurements of the examination and analysis section may assist in understanding the improvements that can be made in collecting the technical analysis of the evidence, selection of toolsets, and necessary documentation.

3.2.5 Presentation Section

The presentation phase follows the examination and analysis phase and focuses on the examiner presenting judgments based on the findings from the investigation. This phase includes reporting and lessons learned. Measurements of the presentation section may assist in understanding the improvements that can be made in how judgments are displayed, categorized, and presented to the stakeholders of the investigation.

4. Recommendations

Based on the research presented, additional processes or activities need to be added to the DFCMMI. There is still some emerging process needing to be studied and added to the model. Forensic steps and best practices will need to be developed for cloud computing, IoT, drones, and emerging gaming systems. As technology continues to expand in features and logging, the opportunity for forensic metadata is increased. As new legal requirements are developed or standards created by regulatory bodies, additions may be added to improve the effectiveness of the DFCMMI in these areas.

5. Conclusion

The CMMI was found to be a useful tool to be paired with forensic processes in order to build a model for measuring a forensic team’s maturity. The DFCMMI contained five sections with multiple subsections that each allow for scoring by a management team, forensic expert or stakeholders in an organization. The expert participant’s results indicated that the DFCMMI model may be used effectively to evaluate the maturity of a digital forensic program. In understanding what steps can be taken to improve a program and taking actions to improve the forensics processes, investigations can result in better judgments, reporting, and applicability. The model should be used in teams to gauge where
process, tools, or training can be used to improve the results of investigations.

References


