Anti-Forensic Threat Modeling

Bruno Hoelz, Marcelo Maues

Chapter 10

ANTI-FORENSIC THREAT MODELING

Bruno Hoelz and Marcelo Maues

Abstract The role of a digital forensic professional is to collect and analyze digital evidence. However, anti-forensic techniques can reduce the availability or usefulness of the evidence. They threaten the digital forensic examination process and may compromise its conclusions. This chapter proposes the use of threat modeling to manage the risks associated with anti-forensic threats. Risk management is introduced in the early stages of the digital forensic process to assist a digital forensic professional in determining the resources to be invested in detecting and mitigating the risk. The proposed threat model complements the incident response and digital forensic processes by providing a means for assessing the impact and likelihood of anti-forensic threats, evaluating the cost of risk mitigation and selecting tools and techniques that can be used as countermeasures. This renders the digital forensic process more robust and less susceptible to the consequences of anti-forensic actions.

Keywords: Forensic examination, anti-forensics, threat modeling, risk management

1. Introduction

In digital forensics, evidence can be found in computer systems and networks, and in devices ranging from cell phones to game consoles. Over the years, several digital forensic process models have been proposed to examine evidence. Some of these models deal with specific needs while others incorporate more general approaches. Most models, however, do not take into account the risks associated with anti-forensic actions (AFAs) [10].

An anti-forensic action attempts to reduce the availability or usefulness of digital evidence in the forensic process [6]. The anti-forensic result can be achieved via the use of a malicious tool or method, or through the use of legitimate protection mechanisms such as passwords and encryption.

The use of anti-forensic tools has increased, requiring greater attention to ensure the integrity of forensic results [3]. Despite the fact that anti-forensic actions constitute a threat to the digital forensic process, this concern is not reflected in the process models found in the literature. Overlooking these risks could compromise an entire investigation. The use of threat modeling during the digital forensic process can help address anti-forensic risks in a structured manner – mitigating the threats where possible or, at least, reducing their impact.

This chapter proposes an anti-forensic threat modeling process that complements the digital forensic processes suggested in the literature. The modeling process enables an expert to assess the risks posed by anti-forensic threats, providing an opportunity to devise strategies for handling the threats during forensic procedures ranging from collecting evidence to data analysis and reporting.

2. Threats to the Digital Forensic Process

A threat is a potential cause of an unwanted incident that, if manifested, may harm the operations and/or resources of an organization. Stoneburner et al. [12] define a threat as the "potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability."

Anti-forensic actions are considered to be permanent threats to a digital forensic process because they can result in evidence loss that can compromise an investigation. In this case, the threat-source is an attacker or suspect who benefits from the successful execution of an anti-forensic action. These actions can be classified into four types: (i) evidence destruction; (ii) evidence source elimination; (iii) evidence hiding; and (iv) evidence counterfeiting [6].

2.1 Evidence Destruction

Evidence destruction seeks to delete or corrupt data, rendering it unusable in the investigative process [4, 6]. This technique may leave some evidence. For example, overwriting a file may destroy the content partially or completely, but the software used to destroy the file can leave traces [6]. Methods for evidence destruction include:

- **Wiping:** Deletes files by filling their clusters with random data.

- **File Attribute Modification:** Changes file attributes or replaces them with random data.

- **User Activity Artifact Destruction:** Removes user activity artifacts such as Internet history, recently accessed files, file downloads and chat logs.

2.2 Evidence Hiding

Hiding actions seek to reduce or eliminate the visibility of evidence so that it is not discovered during a forensic examination. In this case, evidence is not destroyed or modified [6]. The presence of data hiding tools on a system is an indicator that a technique has been used. Evidence hiding methods include:

- **Hiding File System Structures:** Hides structures such as the slack space of an NTFS filesystem.
- **Encryption:** Renders file content unreadable.
- **Steganography:** Hides digital data in another file (e.g., image file).

2.3 Evidence Source Elimination

The elimination of evidence sources prevents evidence from being created. Unlike the other techniques, there is no need to destroy or hide evidence because the evidence is simply not created. However, the evidence source elimination process itself could produce evidence [6]. Methods for eliminating evidence creation include:

- **Disabling Logs:** Ensures that activity information is not recorded.
- **Use of Portable Applications:** Reduces the amount of evidence because the applications avoid leaving traces in the system.
- **Use of Operating System on Removable Media:** Reduces the amount of evidence because the operating system runs from a CD or thumb drive.

2.4 Evidence Counterfeiting

Evidence counterfeiting is the act of creating false evidence or manipulating it to compromise the conclusions of a digital forensic investigation. Falsified evidence may mislead the investigation by pointing to individuals other than the threat agent [6]. Evidence counterfeiting techniques include:

- **File Attribute Modification:** Modifies or tampers with file attributes such as timestamps.

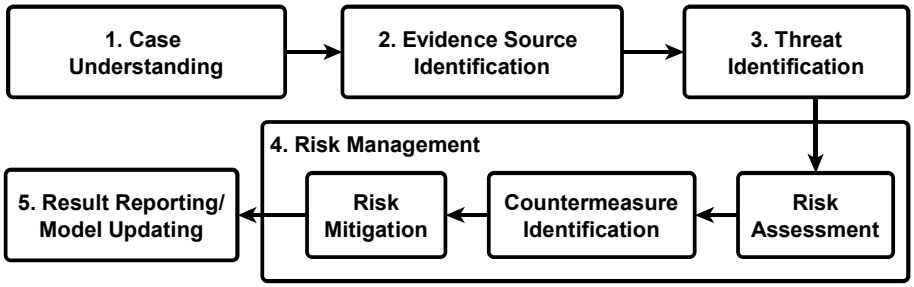

Figure 1. Threat modeling in the digital forensic process.

- **Spoofing:** Spoofs IP or MAC addresses.

- **Account Hijacking:** Creates fake evidence by impersonating the account owner.

3. Threat Modeling Applied to Digital Forensics

Threat modeling is a widely discussed subject in the context of secure software development. It allows for the identification, quantification and treatment of risks associated with a system in a structured manner [9].

A number of threat modeling approaches are described in the literature [2, 7, 9, 11]. Each model is created according to the structure and needs of an organization. This prevents direct comparisons of their quality and effectiveness.

In general, threat modeling has three main steps: (i) system understanding; (ii) asset and access point identification; and (iii) threat identification [8]. The first step is to learn about the operation of the system and define usage scenarios in order to reveal the essential characteristics of the system. This is crucial to understanding the attacker objectives. Next, the assets must be identified. These correspond to the attacker's targets, which must be protected. Access points should also be identified because they enable the attacker to reach the targets. The final threat identification step uses the information gathered in the previous steps to evaluate the risks and propose countermeasures.

In this work, threat modeling is applied to the digital forensic process. As shown in Figure 1, threat modeling involves five steps. The first step involves the collection of information about the case or incident. The second step focuses on identifying evidence sources that may be targeted. The third step deals with the identification of anti-forensic actions that may compromise the previously-identified evidence sources. The fourth step manages the risk, which involves risk assessment, countermeasure

identification and risk mitigation. The final step reports the results and uses the results to update the model.

3.1 Case Understanding

The purpose of this step is to gather information about the investigated case in order to assist decision making in the subsequent steps of the modeling process. This step is essential to the effectiveness of the proposed model. It involves the determination of the ability, motivation and financial profile of the suspect. A questionnaire is recommended to guide the collection of information. The questionnaire would feature questions such as:

- Are there reasons for the use of an anti-forensic method by the suspect?
- What are the suspect's technical skills?
- Does the suspect have the support of technically-skilled professionals?
- Are there reports of anti-forensic actions being employed in similar cases in the past?

With regard to the last question, the proposed model incorporates a catalog that records the occurrences of anti-forensic actions identified in previous investigations or actions reported in external sources such as research papers and security advisories.

3.2 Evidence Source Identification

This step attempts to identify the data storage media where evidence related to the investigation can be found. The identification of these resources is critical to identifying anti-forensic threats. Evidence can be obtained from various sources such as user files, operating system event logs, Internet browser history and file metadata. Sources also include devices such as digital cameras, game consoles and GPS devices. The more important the device is to the investigation, the more likely it is to be the target of an anti-forensic action.

3.3 Threat Identification

This step analyzes the evidence sources to see if any anti-forensic actions can be applied to compromise them. The classification of anti-forensic methods proposed by Harris [6] is used to categorize anti-forensic threats. As discussed above, anti-forensic methods can be classified as

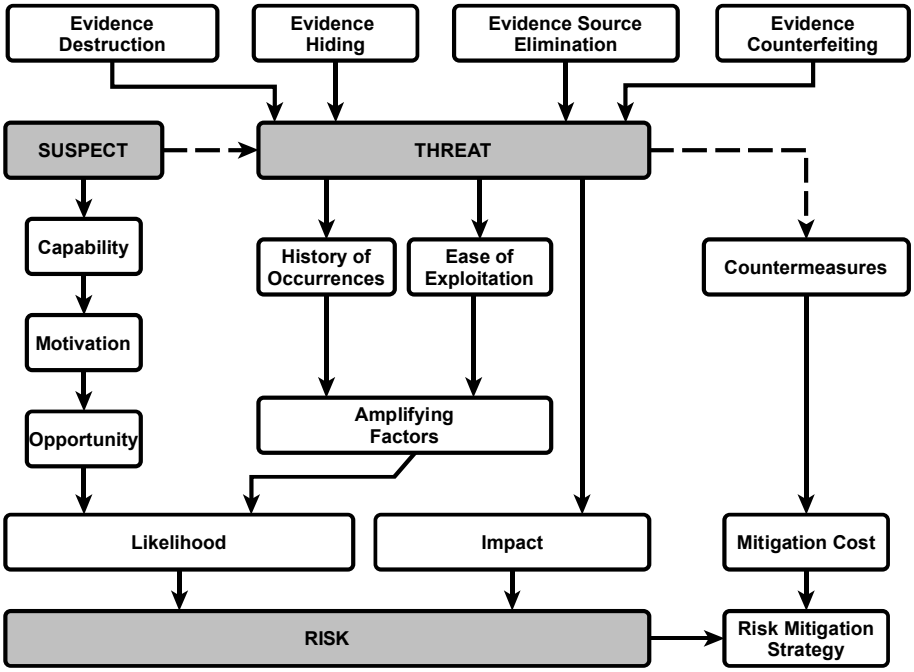

Figure 2. Risk management components.

evidence destruction, evidence hiding, evidence source elimination and evidence counterfeiting. For example, in a case where it is crucial to analyze the operating system logs (evidence source), the threat identification step should specify the actions that enable the logs to be modified or destroyed.

The proposed model incorporates a catalog of known anti-forensic threats to support threat identification. This catalog, which records anti-forensic methods, must be updated whenever a new anti-forensic method is reported or encountered.

3.4 Risk Management

This step estimates the risks that anti-forensic threats pose to the digital forensic process. It helps determine which risks should and should not be mitigated – dealing with every possible threat is not always feasible due to limited resources, including time. Risk management has three components: (i) risk assessment; (ii) countermeasure identification; and (iii) risk mitigation. Figure 2 summarizes the components involved in the risk management step.

Table 1. Capability assessment.

Score	Capability Assessment
5	The suspect has technical and financial limitations to employ the anti-forensic action.
15	The suspect has technical or financial limitations to employ the anti-forensic action.
25	The suspect has extensive technical and/or financial abilities to employ the anti-forensic action.

Table 2. Motivation assessment.

Score	Motivation
5	The anti-forensic action does little to the criminal act.
15	The anti-forensic action contributes to the criminal act.
25	The anti-forensic action is essential to the criminal act.

Risk assessment is performed by combining the threat likelihood and impact [12]. The threat likelihood is estimated by considering factors related to the suspect (threat agent) and factors related to the anti-forensic action, called amplifying factors. The likelihood is rated as low, medium or high, according to the total score assigned to each factor. The impact is estimated by the digital forensic professional's ability to recover potential evidence when facing an anti-forensic threat. The impact is also rated as low, medium or high. Finally, the risk is determined using a risk matrix that is generated by combining the likelihood and impact ratings.

The suspect's capability, motivation and opportunity are key factors in estimating the threat likelihood [13]. In the proposed model, the capability expresses suspect's technical and financial resources for executing the anti-forensic action. The motivation is related to the benefit of the anti-forensic action to the suspect. For example, the anti-forensic action may camouflage the criminal action; in credit card fraud cases, encryption is often used to hide stolen credit card data. Opportunity refers to the circumstances that favor the success of the anti-forensic action. The suspect may, for example, consider that an action will not be identified during the forensic examination. Tables 1 though 3 list scores that are used to assess a suspect's capability, motivation and opportunity.

Table 3. Opportunity assessment.

Score	Opportunity
0	It is part of the routine of a digital forensic expert to treat the anti-forensic action and resources (software and hardware) and trained personnel are available to handle the anti-forensic action.
10	It is not part of the routine of a digital forensic expert to handle the anti-forensic action, but resources (software and hardware) and trained personnel are available to handle the anti-forensic action.
20	It is not part of the routine of a digital forensic expert to handle the anti-forensic action and/or resources are not available (software and hardware) or trained personnel are not available to handle the anti-forensic action and/or it is very difficult to handle the anti-forensic action.

In addition to the suspect's capability, motivation and opportunity, certain other factors can increase the likelihood of an anti-forensic action. These amplifying factors [13] are:

- **History of Occurrences:** Whether or not the anti-forensic action has been used in other situations.
- **Ease of Exploitation:** The amount of resources necessary to execute the anti-forensic action. The existence of tools and documentation of the method and a vulnerability contribute to the ease of exploitation.

Table 4. History of occurrences.

Score	History of Occurrences
0	There is no record of the anti-forensic action in previous reports.
5	The anti-forensic action is rarely used.
10	The anti-forensic action is sometimes used.
15	The anti-forensic action is widely used.

Tables 4 and 5 are used to determine the score of the amplifying factors. The final likelihood is estimated by adding the scores assigned to each factor (low, medium or high) as shown in Table 6. The score for each factor is set so that the factors related to the suspect (capability, motivation and opportunity) are adequate to yield a high likelihood of an anti-forensic action.

Table 5. Ease of exploitation.

Score	Ease of Exploitation
5	Limited resources (no tools) exist for executing the anti-forensic action.
10	Some resources exist for executing the anti-forensic action.
15	Many resources (tools and documentation) exist for executing the anti-forensic action.

Table 6. Likelihood of threat by score.

Final Score	Likelihood
Below 35	Low
35 to 60	Medium
Above 60	High

The amplifying factors score increases the likelihood of occurrence, but on its own, it cannot establish a high likelihood for the anti-forensic action. However, in a scenario involving an anti-forensic action that is easily and often used, the amplifying factors score would increase the likelihood of the threat from low to medium and from medium to high.

The computation of the likelihood of a threat is illustrated for missing data hidden in the filesystem slack space. In this case, a medium likelihood is obtained as follows:

$$\begin{aligned} \text{Likelihood} &= (\text{Capability} + \text{Motivation} + \text{Opportunity}) \\ &\quad + (\text{History} + \text{Ease of Exploitation}) \\ &= (15 + 15 + 10) + (5 + 10) = 55 \text{ (Medium)} \end{aligned} \tag{1}$$

Having determined the likelihood of the threat, it is necessary to determine its potential impact. The anti-forensic action could impact the recovery and presentation of evidence with probative value [5]. Table 7 shows the three impact levels, low, medium and high.

After calculating the likelihood and impact, the risk of the anti-forensic threat may be obtained by combining the results according to the risk matrix presented in Table 8.

The level of tolerance to risk is subjective and should be evaluated in the context of other threats. Some low-risk threats can be tolerated in the case of a simultaneous threat of medium risk if the resources to handle the threats are limited. Therefore, the risk level alone does not

Table 7. Impact levels.

Impact Level	Description
Low	Evidence will no longer be recovered.
Medium	Usable evidence will no longer be recovered.
High	Probative value of evidence is lost and can compromise the prosecution of the suspect.

Table 8. Risk level matrix adapted from [12].

		Likelihood		
		Low	**Medium**	**High**
Impact	**Low**	Low	Low	Low
	Medium	Medium	Medium	Medium
	High	Medium	High	High

determine the obligation to take action. This depends on the available countermeasures and the cost of mitigating the risks.

After determining the risk level of a threat, it is necessary to identify the countermeasures that can minimize the impact and prevent evidence loss. The proposed model incorporates a catalog that records the countermeasures to threats. This catalog also specifies the techniques and tools that must be used in each situation. Of course, the catalog must be updated as and when new countermeasures are developed or reported.

Table 9. Cost of implementing countermeasures.

Cost	Conditions
Low	Requires little effort and time to employ.
Medium	Requires moderate effort and time to employ.
High	Requires a lot of effort and time to employ.

After identifying the available countermeasures, the risk mitigation step evaluates the specific countermeasures that should be employed. This depends on the risk and the available resources, including the cost of implementing each countermeasure. The cost, which is classified as low, medium or high, is estimated by considering the time and effort involved, as shown in Table 9. Some countermeasures can be very costly and, depending on the risk, may be deemed unnecessary. Naturally, this

Table 10. Mitigation strategy matrix.

		Implementation Cost		
		Low	**Medium**	**High**
Risk	**Low**	Mitigate	Accept	Accept
	Medium	Mitigate	Mitigate	Accept
	High	Mitigate	Mitigate	Mitigate

decision would vary according to the resources available to an organization.

As an example, consider a countermeasure for minimizing the risk of missing data that is hidden in the filesystem slack space. In this situation, the countermeasure does not require much effort or time because forensic tools are available for analyzing the slack space. Therefore, the cost of implementing the countermeasure is low.

Table 10 shows the mitigation strategy matrix that assists in deciding whether or not to mitigate the risk. The combination of risk and cost of the countermeasure in the matrix suggests one of two outcomes: (i) mitigate the risk; or (ii) accept the risk. Mitigation involves the application or implementation of the countermeasure. On the other hand, the risk is accepted if the cost of implementing the countermeasure is deemed too high or no countermeasure is available.

In the case of missing data hidden in the filesystem slack space, the best option is to mitigate the risk by applying the available countermeasure. This is because the risk level is considered to be medium and the cost of applying the countermeasure is low. Note, however, that the cost depends on the resources, including time, that are available to the digital forensic professional or the organization.

3.5 Result Reporting and Model Updating

In this step, a report is generated with the results of the previous steps. This report can be used to review the assessments made by the digital forensic professional and to register the threats that were not considered initially, but that were discovered during the examination process. Information from the report should also be used to update the model catalogs.

4. Applying the Threat Model

This section shows how the proposed threat model can be incorporated in a digital forensic process. The digital investigation process

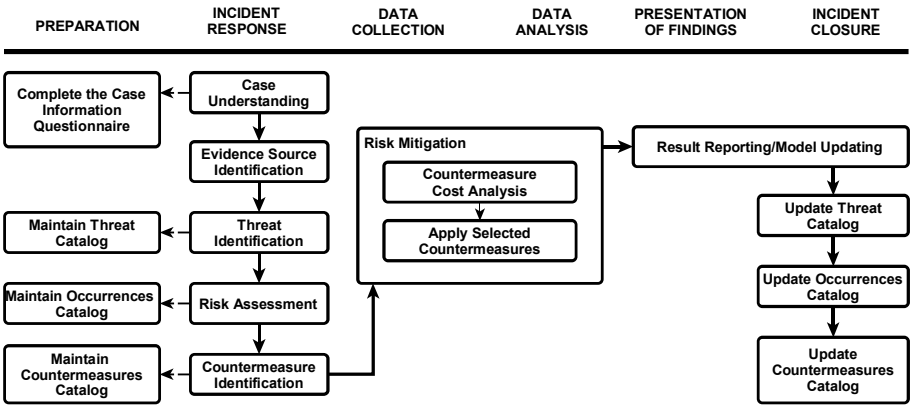

Figure 3. Threat model actions in the digital forensic process.

model proposed by Beebe and Clark [1] is employed because it covers the majority of the processes proposed in the literature. The model has six steps: (i) preparation; (ii) incident response; (iii) data collection; (iv) data analysis; (v) presentation of findings; and (vi) incident closure.

The preparation phase involves taking technical and administrative actions prior to an incident to maximize the collection of evidence. The incident response phase defines the strategy to be adopted in the subsequent data collection and analysis phases. The presentation of findings phase covers the presentation of results through the forensic report. Finally, the incident closure phase involves an assessment of the entire process to enhance future investigations.

The threat model actions are integrated in the various phases of the digital forensic process. Figure 3 shows that the first step of the threat model is executed during the incident response phase. However, before this, during the preparation phase, the case information questionnaire is completed and the catalogs are maintained; all this information is used in the incident response phase. The use of the threat model results in a list of countermeasures for treating anti-forensic threats that pose risks to the digital forensic examination. The countermeasures are applied during the data collection and/or data analysis phases, but after a cost analysis is performed. During the presentation of findings phase, the threats are articulated formally, the countermeasures are applied and the results are recorded. During the incident closure phase, the catalogs are updated with information pertaining to the incident. Note that, during the preparation phase, the catalogs are also updated with new threats, countermeasures and lessons learned from other incidents. Updating the

Table 11. Risk assessment.

Threat	Likelihood						Impact	Risk
	Mo	Ca	Op	Hi	Ea	Total		
Full-disk encryption	25	25	20	10	15	95 [H]	H	H
Steganography	15	25	10	0	10	60 [M]	M	M

H = High, M = Medium, Mo = Motivation, Ca = Capability, Op = Opportunity, Hi = History of Occurrences, Ea = Ease of Exploitation

catalogs frequently enhances decision making during the threat modeling process.

An investigation of a child exploitation case is used to illustrate the application of the proposed model. In this case, the suspect, who has no criminal history, is known to possess advanced computer skills. This information is determined in the first case understanding step. In the second step – evidence source identification – potential sources of digital evidence are considered, such as the suspect's digital camera, mobile devices, computers and storage media. In the third step, threat identification, potential threats to the evidence are identified based on the information recorded in the threat catalog.

The example considers data hiding threats involving full-disk encryption and steganography. Table 11 shows the computation of the risk associated with each threat.

Table 12. Countermeasures and mitigation strategy.

Threat	Risk	CM	Cost	Strategy
Full-disk encryption	H	CM1	M	Mitigate
Steganography	M	CM2	H	Accept

H = High, M = Medium, CM = Countermeasure

Two countermeasures are identified, CM1 and CM2. CM1 involves the acquisition of data while the computer system is running with its volumes mounted. CM2 involves searching for signs of steganography applications and artifacts. The mitigation strategy matrix shown in Table 12 considers the risks and the implementation costs of the countermeasures in order to decide which mitigation strategy should be adopted. In this case, the threat of full-disk encryption should be mitigated while

the threat of steganography should be accepted. During the last step, a report is produced that contains the assessments of all the previous steps along with the decisions that were made. The occurrences catalog is updated after the threat is confirmed. Note that in some cases – as in the threat of encryption being used – countermeasures may have to be applied before confirming the existence of the threat.

5. Conclusions

This research advocates the use of threat modeling to handle anti-forensic threats to the digital forensic process. The threat modeling process adapts and incorporates concepts and methods originally proposed for the software development domain. The threat modeling process has five steps: case understanding, evidence source identification, threat identification, risk management, and results reporting and model updating. The model complements the phases commonly used in the digital forensic process while systematically introducing anti-forensic risk management activities in the workflow.

Risk management is introduced in the early stages of the digital forensic process in order to assist forensic professionals in making decisions about investing resources to detect and mitigate risks due to anti-forensic actions. The proposed threat model complements the incident response and digital forensic processes by helping assess the impact and likelihood of anti-forensic threats, the cost of risk mitigation and the selection of techniques and tools that may be used as countermeasures. Consequently, the digital forensic process becomes more robust and less susceptible to the negative consequences of anti-forensic actions.

Future work will focus on the application and evaluation of the threat model in real investigations. Efforts will also be made to develop and disseminate threat and countermeasure catalogs that will enhance risk management in digital forensic investigations.

References

[1] N. Beebe and J. Clark, A hierarchical, objectives-based framework for the digital investigation process, *Digital Investigation*, vol. 2(2), pp. 147–167, 2005.

[2] S. Burns, Threat Modeling: A Process to Ensure Application Security, InfoSec Reading Room, SANS Institute, Bethesda, Maryland, 2005.

[3] E. Casey (Ed.), *Handbook of Digital Forensics and Investigation*, Elsevier Academic Press, Burlington, Massachusetts, 2010.

[4] R. Chandran and W. Yan, A comprehensive survey of anti-forensics for network security, in *Managing Trust in Cyberspace*, S. Thampi, B. Bhargava and P. Atrey (Eds.), CRC Press, Boca Raton, Florida, pp. 419–447, 2013.

[5] R. de Beer, A. Stander and J. Van Belle, Anti-forensic tool use and their impact on digital forensic investigations: A South African perspective, *Proceedings of the International Conference on Information Security and Digital Forensics*, pp. 7–20, 2014.

[6] R. Harris, Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, *Digital Investigation*, vol. 3(S), pp. S44–S49, 2006.

[7] J. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla and A. Murukan, *Improving Web Application Security: Threats and Countermeasures*, Microsoft, Redmond, Washington, 2003.

[8] S. Myagmar, A. Lee and W. Yurcik, Threat modeling as a basis for security requirements, *Proceedings of the Symposium on Requirements Engineering for Information Security*, 2005.

[9] Open Web Application Security Project, Application Threat Modeling, Columbia, Maryland (`www.owasp.org/index.php/Application_Threat_Modeling`), 2015.

[10] J. Sachowski, *Implementing Digital Forensic Readiness: From Reactive to Proactive Process*, Elsevier, Cambridge, Massachusetts, 2016.

[11] A. Shostack, *Threat Modeling: Designing for Security*, John Wiley and Sons, Indianapolis, Indiana, 2014.

[12] G. Stoneburner, A. Goguen and A. Feringa, Risk Management Guide for Information Technology Systems, Special Publication 800-30, National Institute of Standards and Technology, Gaithersburg, Maryland, 2002.

[13] S. Vidalis and A. Jones, Analyzing threat agents and their attributes, *Proceedings of the Fourth European Conference on Information Warfare and Security*, pp. 369–380, 2005.