HIGH-LEVEL INTEGRATED VIEW OF DIGITAL FORENSICS

CP Grobler[1], CP Louwrens[2]

University of Johannesburg[1]
Nedbank SA[2]
rsn@netactive.co.za[1]
buksl@nedbank.co.za[2]

ABSTRACT

We are living in a world where there is an increasing need for evidence in organizations. Good digital evidence is becoming a business enabler. Very few organizations have the structures (management and infrastructure) in place to enable them to conduct cost effective, low-impact and efficient digital investigations (Sommer, 2005). Digital Forensics (DF) is a vehicle that organizations use to provide good and trustworthy evidence and processes.

The current DF frameworks concentrate on reactive investigations, with limited reference to DF readiness and live investigations. However, organisations use DF for other purposes. The paper proposes that DF consists of three components: Proactive (ProDF), Active (ActDF) and Reactive (ReDF). ProDF concentrates on DF readiness and the proactive, responsible use of DF to demonstrate good governance and enhance governance structures. ActDF consider the gathering of live evidence during an ongoing attack with limited live investigation and ReDF deals with the traditional DF investigation. The paper discusses each component and the relationship between the components.

KEY WORDS:

Digital forensics, Digital forensic readiness, Information Security governance, live investigations, Proactive Digital forensics, Active Digital Forensics, Reactive Digital Forensics

HIGH-LEVEL INTEGRATED VIEW OF DF

1 INTRODUCTION

We are living in the knowledge age where information and knowledge is the most sought after commodity. Criminals, competitors and even employees exploit loopholes in current security architectures and control structures, use anti-forensic techniques and tools to hide their traces and apply forensic tools and techniques to obtain the required information to commit cyber crimes.

Organizations spend a lot of time, money, and effort in planning for incidents, natural disasters or security breaches by drafting incident response, disaster recovery and business continuity plans. These plans identify an incident and prescribe the best way to recover and continue with the business as quickly as possible. Very little thought is given to the identification and preservation of digital evidence and the correct structuring of processes for possible prosecution (Sommer, 1999).

Often, when asked for specific digital evidence, most organizations do not have all the evidence available (Clark, 2006). According to Sommer in the Guide to Investigations and Evidence (Sommer, 2005), most organizations underestimate the demand for digital evidence. Typically, evidence is required for fraudulent or disputed transactions; to support allegations of employee misbehaviour; to investigate suspected terrorism, to demonstrate due diligence with respect to good corporate governance, measuring legal and regulatory compliance; to avoid charges of negligence; to assist law enforcement and support insurance claims after a loss. This evidence is not only information stored, but can be logs generated by business processes, snapshots of systems, cell phone records, access control records etc. DF tools can retrieve the evidence required in a in a legally acceptable format and provide a chain of evidence and custody.

However, the nature of incidents and attacks has changed. Investigations need relevant, admissible live digital evidence for example volatile evidence (memory (RAM) content), swap files and network processes to determine the root-cause of an incident and to successfully prosecute the perpetrator. A famous example is the Code Red worm where you can only conduct a ’live’ investigation as the worm is memory resident and never writes to the disk. Many real-time systems cannot be powered down and investigations must be done on the live systems. Current DF investigation methodologies do not address the gathering of live evidence sufficiently.

There is a need for a comprehensive DF management framework (DFMF) that will

- Prepare organizations for DF investigations by the proactive identification and the availability of enough admissible evidence, and the restructuring of relevant processes to be forensically sound;
- Use DF tools and techniques to enhance governance frameworks in organizations;
- Gather and analyze live evidence during ongoing attacks; and
- Successfully investigate incidents to determine the root-cause of an incident and successfully prosecute a perpetrator.

The current DF models do not address the above-mentioned needs. The paper proposes a high-level framework that will consider 3 components, ProDF, ActDF and ReDF. The components will provide the backbone in the formulation of a comprehensive DFMF which is part of the broader study. The paper discuss the different components of DF by

- Defining and discussing the goals of ProDF;
- Defining and discussing the goals of ReDF,
- Defining and discussing the goals of ActDF; and
- Discuss how the different components interact to provide a high-level overview of DF.

The next part of the paper discusses ProDF.

2 PROACTIVE DIGITAL FORENSICS

Being Proactive is defined as ‘creating or controlling a situation rather than just responding to it’ (Soanes C, 2005). ProDF, as discussed in this paper is the forensic preparation of an organization to ensure successful, cost effective digital investigations with minimal business activity disruption and ensuring that ‘good’ (admissible) evidence and sound processes are in place and available when needed for an investigation or during the normal flow of business.

There are specific requirements per country, jurisdiction and industry for admissible evidence. The quality of evidence will determine the success of any investigation. The paper proposes a definition for Comprehensive Digital Evidence (CDE) *as digital evidence that will have evidentiary weight in a court of law and that contains all the evidence necessary (relevant and sufficient) to determine the root-cause of the incident, link the attacker to the incident and will result in a successful prosecution of the perpetrator.* The paper will use CDE to refer to evidence that meets the legal requirements to be admissible in a court of law.

From the literature studied, most of the current DF models include a ‘preparation’ or a ‘DF readiness’ step (Beebe & Clark, 2005; Casey, 2004; CP Louwrens et al., 2006; Rowlingson, 2004). DF readiness is defined as: *the ability of an organization to maximize its potential to use CDE evidence whilst minimizing the costs of an investigation- adapted from Rowlingson (Rowlingson, 2004).*

However, organizations use DF in more areas. Nikkel (Nikkel, 2006) has identified external and internal drivers for the use of DF in organizations. External drivers are Legal and Regulatory requirements and best practices. Internal drivers are internal legal departments who need evidence after an incident; The ability to prove compliance e.g. legal compliance; The need for evidence by Human Resources for internal hearings; Risk management; The IT department to investigate e.g. security breaches or equipment misuse; The use of DF tools for non-forensic purposes e.g. password retrieval and disk recovery; and Continuous auditing by the internal audit department.

The paper propose a definition for Proactive DF *as the proactive restructuring and defining of processes, procedures and technologies to create, collect, preserve and manage CDE to facilitate a successful, cost effective investigation, with minimal disruption of business activities whilst demonstrating good corporate governance.*

The authors have identified the following goals for ProDF:

- Become DF ready;

- Enhance the Governance programs (IT and IS) of the organization by proving (assessing) the effectiveness of controls, measured against IT and IS objectives (related to business objectives);
- Improve IS / IT performance with the responsible use of DF tools to improve effectiveness and efficiency in organization;

The next part of the paper will briefly discuss each goal.

2.1 Become DF Ready

After comparing different viewpoints of DF readiness and preparation phases, the paper has identified the following goals for DF readiness (Beebe & Clark, 2005; CP Louwrens et al., 2006; Garcia, 2005; Rowlingson, 2004):

- *Provide and prepare the infrastructure* (systems and networks) to support DF investigations;
- *Develop an evidence management plan (EMP)* that will concentrate on the identification, legal gathering, preservation, handling, retrieving, retention and archiving of CDE. The EMP must include the construction of a digital evidence map that will contain all the information about the evidence i.e. category, location, retention time, reference procedures to collect and retrieve evidence, regulatory collection requirements (Casey, 2007); and the development of evidence management policies and procedures e.g. policy for secure storage, acquiring, preservation and handling of evidence, secure evidence policy and evidence transport;
- *Augment organizational risk mitigation plans* for example include evidence and process requirements in risk assessment, incident response, business impact analysis, business continuity and disaster recovery plans by linking the evidence requirement to the digital evidence map to determine the completeness and admissibility of the evidence; Implement an Intrusion Detection System (IDS) with active monitoring capabilities and define trigger events for ActDF investigations; Prepare for containments of incidents to include containment on live systems.
- *Develop a DF training and awareness strategy* with education, training and awareness programmes for organization;
- *Develop a management capability* that will define the management structure that will outline the internal and external DF investigators

and the role and responsibilities of the Computer Emergency Response Team (CERT);

- *Document and validate a DF investigation (DFI) protocol* against best-practice;
- To allow an *investigation to proceed at a cost* in proportion to the incident;
- To *minimize interruption* to the business from any investigation;

2.2 Enhance the Governance programs (IT and IS) of the organization by proving (assessing) the effectiveness of controls, measured against IT and IS objectives (related to business objectives).

Corporate Governance reports and legislation, for example: Sarbarnes-Oxley (*Sarbanes-Oxley Act*, 2002) and King 2 (*King II Report on Corporate Governance*, 2003) states that management is responsible and accountable for the IT infrastructure, applications and information of the organization. King 2 states that the board must ensure 'that a systematic, documented assessment of the processes and outcomes surrounding key risks is undertaken' (*King II Report on Corporate Governance*, 2003).

DF tools can be utilized to assess the controls implemented; the DF investigation process followed can provide the documented proof of the assessment. Management can then provide reasonable assurance and documentation to prove due diligence. The effective utilization of DF tools and techniques can enable management to enhance the governance structures of the organization by providing evidence to measure performance or compliance. DF readiness as defined concentrates on evidence availability and preservation and does not provide for assessment of controls.

Organization should manage the implementation and use of DF. The board must include DF in the management structure of the organization by assigning a position with responsibility and authority to a person. It must also clearly stipulate the relationship (and segregation of duties) between the DF team, Information Security, Risk Management, Internal Audit and Legal departments.

2.3 Improve IS / IT performance with the responsible use of DF tools to improve effectiveness and efficiency in organization;

It is essential to design, configure, and implement systems and processes in such a way to enable DF in the organization for example to design DF friendly file structures. The responsible use of DF tools and techniques can be used to improve the effectiveness of IT systems for example disk data recovery. The CSI 2008 computer (Richardson, 2008) indicates that 41% of respondents use DF tools and techniques as part of their security suite,

However, controls must be in place to prevent the unauthorized use of DF tools for example the use of password crackers and anti-forensic activities for example data destruction, manipulation and data hiding.

ProDF will therefore address the need to prepare organizations for DF investigations by being DF ready, and the responsible application of DF tools and techniques to enhance governance frameworks in organizations. The next part of the paper discusses ReDF.

3 REACTIVE DIGITAL FORENSICS

No organization is fully prepared for incidents. ReDF as defined by this paper concentrates on the traditional DF investigation that will take place after an incident has been detected. Should an incident occur, there should be an acceptable proven DF investigation protocol in place as specified by ProDF on how to conduct the investigation (CP Louwrens et al., 2006). The goals of ReDF are to:

- determine the root-cause of the incident;
- link the perpetrator to the incident;
- minimize the impact of an incident; and
- successfully investigate an incident;

The paper defines *Reactive DF as the analytical and investigative techniques used for the preservation, identification, extraction, documentation, analysis and interpretation of digital media which is digitally stored or encoded for evidentiary and/ or root-cause analysis and the presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of incidents.*

The authors have studied various DF methodologies or investigation protocols from literature and propose that the following phases with steps that should be included in the DF investigation protocol of an organization: (Barayumureeba & Tushabe, 2004; Beebe & Clark, 2005; Carrier, B & Spafford, 2003; Casey, 2004; Ciardhuain, 2004; CP Louwrens et al., 2006; Forrester & Irwin, 2007; Rowlingson, 2004).

3.1 Phase 1: Incident response and confirmation.

This phase includes the following steps: Detect an Incident / activity; Report the incident; Determine the assessment of worth (Validate incident Assess damage / impact), Incident Confirmation; Formulate a hypothesis; Obtain an authorisation – internal and external; Determine a containment strategy; Formulate an Investigation plan; Coordinate the resources; Accelerate the investigation; Notification of the investigation – *determine the relevance*.

3.2 Phase 2: Physical Investigation (if relevant)

Although it is a DF investigation, it is essential to include the physical crime scene to gather as much evidence as possible to ensure a successful investigation. Steps include to Secure the physical crime scene; Survey of crime scene for potential evidence; Search and collect (secure hardware, secure transport); Documentation (label and seal all evidence); Acquire the evidence; Analyze the evidence; Identify possible digital evidence – to be sent to Digital investigation team; Reconstruct the event; Make a finding; Transport the evidence; and Store the evidence.

3.3 Phase 3: Digital Investigation

During this phase the actual digital investigation will start. The steps followed during this phase are essential and will determine the success of the investigation. The steps are:

3.3.1 Evidence acquisition

This step includes Identification and seizure of evidence; Collection of evidence; Acquire the relevant evidence (recovery, harvesting, reduction) – if live evidence is required, activate the ActDF component; Ensure integrity (Preservation / forensic copy, Competent people, Secure evidence); Authenticate – timestamp; Transport of the evidence; Storage of the evidence; and Document the acquisition process.

3.3.2 Analysis

The investigative team will Revisit the investigation plan; Review the relevance of tools and expertise available; Develop a hypothesis; Analyze the evidence (Examine evidence – best evidence, Assess the evidence – means motivation and opportunity, Experimentation); Test the hypothesis (apply fusion and correlation); Reconstruct the event; Make a finding; Validate the results of analysis; Document the case; and Secure the documentation.

3.3.3 Service restoration

During this phase, the intention is to restore systems as fast as possible if necessary by interacting with information security risk management team to restore services ASAP;

3.4 Phase 4: Incident reconstruction

During this phase the investigation team will Consolidate physical investigation (phase 2) and digital investigation (phase 3) findings. If, during the reconstruction process, the investigation team identify missing evidence to support the hypothesis; phase 2 and / or 3 may be repeated to obtain the evidence. The final outcome of this phase will be a well documented report with supporting CDE that support the hypothesis.

3.5 Phase 5: Present findings to Management / authorities.

The investigation team will prepare the case by Considering the legal jurisdiction location requirements; Incorporate the timeline of the entire case; Determine the target audience; Prepare expert witness; Prepare exhibits; Use appropriate presentation aids; and Preserve the chain of custody. Present the case and preserve the evidence. The protocol must also provide an appeal process.

3.6 Phase 7: Dissemination of result of P/H / Incident closure

It is essential to review the outcome of the case to identify and apply lessons learned. Finally depending on the policies and requirements all evidence must be preserved, returned or disposed.

The phases as identified in this section seem to be a waterfall framework with some repetition if needed between the different phases. ReDF as discussed meet the need to investigate incidents to determine the root-cause of an incident and successfully prosecute a perpetrator. The next part of the paper will briefly discuss ActDF.

4 ACTIVE DIGITAL FORENSICS

When an incident occurs, the Intrusion Detection System (IDS) of an organization will detect it and the Incident Response (IR) protocol of the organization will be activated. It is however becoming essential to integrate live forensic investigation protocols with the IR protocol to ensure that relevant and admissible live CDE is available if required for investigatory purposes. IR protocols do not consider the importance of evidence identification, gathering and preservation of live data (Sommer, 1999).

Various tools and methodologies exist to conduct live investigations, but as it is a new field, it faces numerous challenges. According to Ioeng and Leung (Ieong & Leung, 2007) live forensic investigations are hampered due to missing definitions of live forensics; the absence of standard procedures in live investigations; and the certification and affectation of live evidence.

Traditional ReDF investigation methodologies will ensure that no changes are made to the evidence and the seized content. Live investigators uses software tools that make unavoidable changes to data acquired, the live investigative process must be documented in a forensic sound manner to maintain the chain of custody, so that the evidence gathered will be admissible in a court of law.

Live analysis is often associated with incident response and intrusion detection systems, but is auxiliary to the IS programs. Virus software is an example of a live analysis tool. Most of the live investigation tools and techniques are software based, however current research is considering the use of hardware devices to acquire evidence (Carrier, BD & Grand, 2004).

Live forensic investigations are currently being done by using remote forensic preservation and acquisition tools, e.g. EnCase Enterprise edition and ProDiscover (Casey & Stanley, 2004). These tools use live analysis techniques that will use software that pre-exist on the system during the timeframe being investigated (Carrier, Brian, 2006). The target machine is monitored from a remote site data can be acquired in a forensic sound way by the aid of a tool. Typical activities include keyword searches, copying and extraction of files and records from the live remote site. The user is not aware of the process and an investigation can continue without him being aware of it. The investigator can acquire evidence in a live production environment. Remote forensic investigations focus more in transforming ReDF examination procedures onto live, production environments.

The investigator can also use network forensics to identify sources of live network evidence. It is not possible to log all activities on a network, but it is essential that during a live investigation to identify potential sources for example DNS and whois servers, websites, ftp servers, local Ethernet servers, Bluetooth piconets, database servers, chat servers, network routing tables or reply messages of SOAP servlets (Nikkel, 2005). Evidence that can be gathered is for example slanderous web pages, illegal files, traffic from port scans, routing tables, wireless signal strength and direction.

Other software techniques identified by Carrier et al. (Carrier, BD & Grand, 2004) to gather live evidence include virtual machines, physical memory devices, hibernation and process pseudo files. All of the above techniques are software-based and rely on the operating system, but the operating system kernel is not a trusted resource as it can have a malicious kernel. This poses a threat to the reliability of the evidence. A second problem is that the operating system must execute a command and therefore will have to write to memory and therefore destroy evidence in the process.

Carrier et al. (Carrier, BD & Grand, 2004) has proposed a hardware based memory acquisition procedure. They propose the use of a hardware expansion card pre-installed in a PCI bus that will gather volatile evidence and write it to external storage device.

The rationale of the various techniques differs as remote online forensic investigations capture data disregarding the order of volatility (Ieong & Leung, 2007). The other live investigation techniques will consider the order of volatility of the evidence.

The authors have studied current ‘live or remote or real time’ methodologies and propose to include current live forensic tools and techniques, real time investigations as well as remote investigations as part of ActDF (Foster M, 2004; Ieong & Leung, 2007; Payer, 2004; Ren & Jin, 2005). There are no or very limited methodologies for ActDF investigations.

The paper proposes the following definition for ActDF: *Active DF is the ability of an organization to gather (identify, collect and preserve) CDE in a live environment to facilitate a successful investigation.*

The goals for ActDF are:

- Collect relevant live CDE (including volatile evidence) on a live system or production environment by using appropriate tools and technologies;
- Minimize the effect and impact of an ongoing incident; and
- Provide a meaningful starting point for a reactive investigation within the parameters of the risk control framework of the organization.

The paper identified the following phases for ActDF from the literature (Foster M, 2004; Ieong & Leung, 2007; Payer, 2004; Ren & Jin, 2005). It is essential to apply relevant incident / crime scene protocols (Casey, 2004) e.g. consider physical crime scene investigation requirements not to destroy any evidence. From literature studied, some of the current frameworks depend on the technology used. The authors formulated the following phases independent of any tool or technology:

4.1 Phase 1: Incident response and confirmation.

The investigator must adhere to the defined steps for this phase as specified by ReDF, but must determine which volatile or live evidence must be acquired to successfully investigate incident as it is prescribed by the ProDF component or potential missing evidence for new or unknown incidents; Formulate ActDF investigation plan; If risk management policies allow it continue with ActDF investigation, otherwise start the reactive investigation. There may also be a pre-defined trigger event to start active monitoring or other procedures as soon as an incident alert is activated. As ActDF deals with ongoing or real time incidents the containment strategy and plan is very important because the systems will remain live and may not be powered down.

4.2 Phase 2: ActDF investigation.

Evidence acquisition - (phase 3 of ReDF applies). Collect additional live evidence lacking from, or required by the CDE map using appropriate tools, technologies, or applications that will be required to profile the attacker, gather volatile evidence or to determine the source of the attack. Secure and authenticate all the extracted data by hashing immediately after collection process to preserve before analysis. It is essential to document all actions performed to prove that chain of custody of the evidence acquired was maintained.

It is important to automate and activate the appropriate evidence collection tools, technology or applications as soon as possible (Can be immediately after an incident alert has been issued). Ieong et.al suggests to: Impose minimal user intervention; Ensure that all actions performed are necessary and least intrusive; Ensure minimal modification of static digital evidence; Data acquisition should follow the order of volatility and priority of digital evidence collection; Acquire non-priority or volatile evidence through traditional evidence collection ; and Copy or extraction of data should only be performed when original data and timestamp is not affected (Ieong & Leung, 2007).

Analysis (phase 3 of ReDF applies). Analyze preliminary evidence to determine if sufficient evidence has been gathered to reconstruct the incident and to support the initial hypothesis; Document all activities at all times to ensure the integrity of all evidence; Maintain the chain of evidence and custody; and Validate the processes at all times during the Active DF evidence investigation phase. It is important to ensure the reliability and admissibility of the results.

4.3 Phase 3: Event reconstruction.

This phase uses the results from the analysis step to do a limited reconstruction of the incident. The aim is to determine if the missing or live required evidence has been acquired to determine when to terminate active DF investigation. The termination conditions will be prescribed by the Risk management framework for example cost too high, enough CDE, impact reassessed etc. Repeat phase 2 if live evidence is still lacking.

4.4 Phase 4: ActDF termination.

If sufficient evidence has been gathered or the investigation is terminated due to other reasons, the investigators will prepare documented case files with CDE for the reactive investigation team to complete investigation. As soon as the ActDF investigation is terminated, the reactive component will continue to analyze and reconstruct the incident using all evidence (including static CDE or physical evidence) required to conclude the investigation.

The ActDF component meets the need to gather live evidence during ongoing attacks. The next part of the paper will discuss the relationship between the different components of DF to demonstrate the dependency between the components.

5 RELATIONSHIP BETWEEN PRODF, REDF AND ACTDF.

Using the definitions and goals of ProDF, ReDF and ActDF it is clear that the different components of DF are dependent on each another. Both active and reactive investigations depend heavily on the quality and availability of CDE, the soundness of processes, education level of investigators and staff and the availability of acceptable tools and technologies which is determined by ProDF component.

To demonstrate the relationship figure 1 depicts the typical flow of activities once an incident alert is issued by the IDS of the organization.

The incident alert or accusation (1) is the starting point of an investigation; Organizations can define a trigger event (2) that will start live data acquisitions as soon as certain types of incidents alerts are detected. The next step is to determine the assessment of worth (3) – to determine if the suspicious activity is an incident (Consider if it is intentional, criminal, or determine the reliability of the source of the alert and the potential impact of incident). The result of the assessment of worth step will determine the next step in the process as it will determine the whether to investigate or not. These two steps will always take place after any suspicious activity. The result of the two steps will be either ‘no incident’ (4) or ‘incident confirmation’ (5).

After an incident has been confirmed, a hypothesis will be set. It is then important to determine if sufficient evidence exist to investigate the incident (6). To determine if there is sufficient evidence, the investigator must consult the digital evidence map of the organization (7), as well as the risk profiles and risk profile case scenarios.

If there is not sufficient evidence or the need for live evidence, ActDF must start (8), otherwise the ReDF component will be activated (9).

Once the investigator is satisfied that sufficient evidence exist, the ActDF component is terminated and the ReDF component will be activated (9).

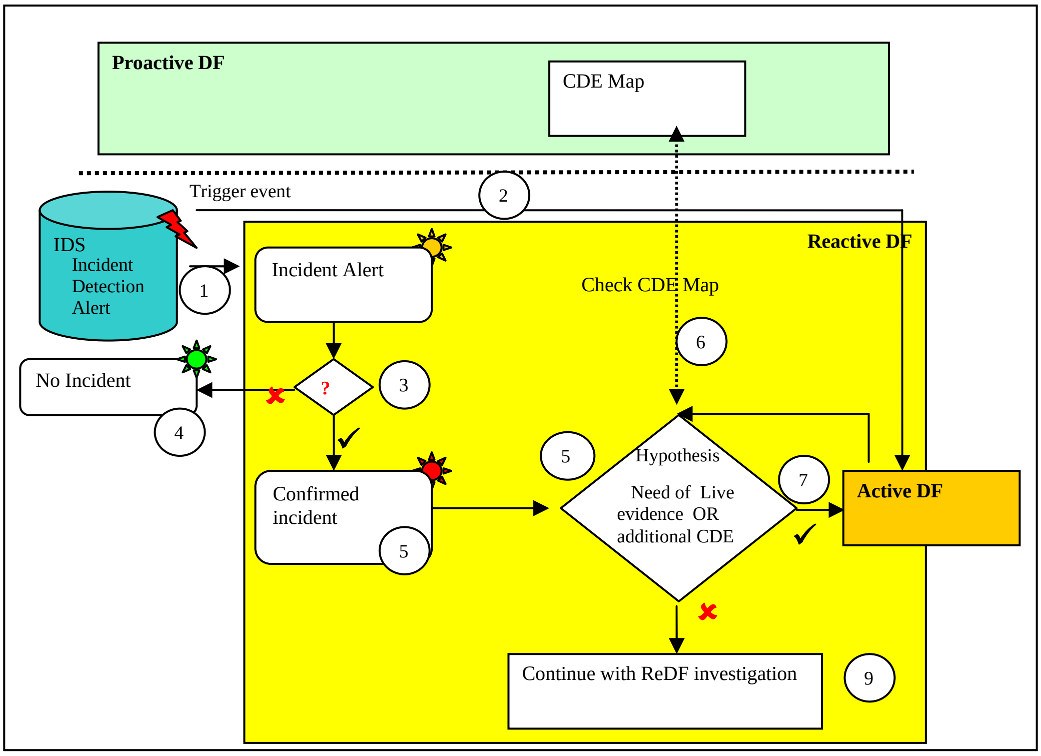

Figure 1: Relationship between DF components

The three components ProDF, ActDF and ReDF address all the needs for a DFMF as identified in paragraph 1 of the paper. The authors will use the 3 components to propose a DF management model manage and implement DF in an organization by investigating what is required in terms of *PROCESS* (What, Where, How, When), *POLICIES* required (What, Where, How, When, Why), *PEOPLE* (Who), *GOVERNANCE* (Why, How), *LEGAL* and *JUDICIARY* (Why, How) and *TECHNOLOGY* (How, Where). This model will be discussed in another paper.

6 CONCLUSION

Current DF frameworks do not cover all applications DF as discussed in this paper, but concentrate on digital investigations. The paper has proposed an integrated view of DF containing three components: ProDF, ReDF and ActDF.

The ProDF component deals with DF readiness i.e. the preparation of the organization for all known incidents to ensure that the required CDE is available to investigate an incident successfully. Staff will be trained and IR processes, policies and procedures will exist to guide next step should an incident occur. Proper management structures should be in place to prescribe who will be responsible for what and when in the organization.

ProDF also propose the responsible use of DF tools and techniques for other purposes than investigations for example assessment of controls and availability of evidence to prove due diligence with respect to good corporate governance and to enhance governance frameworks.

ReDF is the traditional DF investigation after an incident has been detected. It will use all CDE available to determine the root-cause of the incident, reconstruct the incident and prepare a case for prosecution in a court of law or internal hearing. After an incident is confirmed and live evidence is required or if it is an ongoing attack, the ActDF component will be activated.

The ActDF component will deal with the gathering of live evidence in a real time, or in a live environment. It is not a complete investigation, but will only gather required live evidence or missing evidence required and then hand the evidence and documentation over to the ReDF component to complete the investigation.

The paper has discussed the relationship between the different components. The successful implementation of ProDF will provide a solid foundation for the implementation of DF in organisation. ReDF and ActDF concentrate on providing an acceptable protocol to ensure successful investigations.

7 REFERENCES

Barayumureeba, V & Tushabe, F 2004, 'The enhanced digital investigation process model', paper presented to DFRWS 2004.

Beebe, N & Clark, J 2005, 'A hierarchical, objectives-based framework for the digital investigations process ', *Digital Investigation, Elsevier*, vol. 2, pp. 147-67.

Carrier, B 2006, 'Risks of live Digital Forensic analysis', *Communications of the ACM*, vol. 49, no. 2, pp. 56 - 61.

Carrier, B & Spafford, E 2003, 'Getting physical with the digital investigation process', *International journal of Digital Evidence*, vol. 2, no. 2.

Carrier, BD & Grand, J 2004, 'A Hardware-Based Memory Acquisition Procedure for Digital Investigations', *Digital Investigation Journal*, no. 1(1).

Casey, E 2007, 'Digital Evidence maps - A sign of the times', *Digital Investigation, Elsevier*, vol. 4, no. , pp. 1-2.

Casey, E 2004, *Digital Evidence and Computer Crime*, 2nd ed, Elsevier Academic Press.

Casey, E & Stanley, A 2004, 'Tool review - remote forensic preservation and examination tools', *Digital Investigation*, vol. 1, pp. 284-97.

Ciardhuain, SO 2004, 'AN extended model of cybercrime investigations', *International journal of Digital Evidence*, vol. 3, no. 1.

Clark, A 2006, 'Are you ready for Forensics?' <http://www.inforenz.com/press/20060223>.

CP Louwrens, S vonSolms, C Reeckie & Grobler, T 2006, 'A control Framework for Digital Forensics', paper presented to IFIP11.9 International Conference on Digital Forensics, Orlando Florida.

Forrester, J & Irwin, B 2007, 'A Digital Forensic investigative model for business organisations', paper presented to IFIPSec 2007, Sandton.

Foster M, WJ 2004, 'Process Forensics: A pilot study on the use of checkpointing technology in computer forensics', *International journal of Digital Evidence*, vol. 3, no. 1.

Garcia, J 2005, 'Proactive and Reactive Forensics', viewed 5 September 2005,

<http:rediris.es/cert/doc/reuniones/af05/proactive_n_reactive_forensics.pdf>.

Ieong, R & Leung, H 2007, 'Deriving Cse-specific Live Forensics Investigation Procedures from FORZA', paper presented to Symposium on Applied Computing archive

Proceedings of the 2007 ACM symposium on Applied computing Seoul, Korea, 2007.

King II Report on Corporate Governance, 2003.

Nikkel, BJ 2005, 'Generalizing sources of live network evidence', *Digital Investigation*, vol. 2, no. 3, pp. 193-200.

Nikkel, BJ 2006, 'The Role of Digital Forensics within a Corporate Organization', paper presented to May 2006, IBSA Conference, Vienna.

Payer, U 2004, 'Realtime Intrusion-Forensiscs A proptotype implementation', paper presented to Terena Networking conference.

Ren, W & Jin, H 2005, 'Honeynet Based Distributed Adaptive Network Forensics and Active Real Time Investigation', paper presented to 2005 ACM Symposium on Applied Computing, Santa Fe, New Mexico, USA., March 13-17, 2005,.

Richardson, R 2008, *CSI Computer Crime & Security Survey*, CSI.

Rowlingson, R 2004, 'A ten step Process for Forensic Readiness', *International journal of Digital Evidence*, vol. 2, no. 3.

Sarbanes-Oxley Act, 2002, USA, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf . >.

Soanes C, HS 2005, *Oxford Dictionary*, 3 edn, Oxford University press, 10: 0-19-861022-X, <http://www.askoxford.com/dictionaries/?view=uk>.

Sommer, P 1999, 'Intrusion Detection Systems as Evidence', *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. Volume 31 , , no. I23-24 (December 1999), pp. 2477 - 87

Sommer, P 2005, 'Directors and Corporate Advisors' Guide to Digital Investigations and Evidence', *Information Assurance Advisory Council*, viewed 3 June 2007, <http://www.iaac.org.uk/Portals/0/Evidence%20of%20Cyber-Crime%20v12-rev.pdf>.