Chapter 27

A CONTROL FRAMEWORK FOR DIGITAL FORENSICS

S. von Solms, C. Louwrens, C. Reekie and T. Grobler

Abstract This paper introduces a control framework for digital forensics. It proposes a taxonomy for control objectives, categorized within the phases of the digital forensic process: planning and preparation, incident response, investigation and juridical/evidentiary. Using the taxonomy as a basis, a digital forensic reference framework, consisting of control groupings, control objectives and detailed control objectives, is defined. The control framework is intended to provide a sound theoretical basis for digital forensics as well as a reference framework for digital forensics governance within organizations.

Keywords: Digital forensics control framework, control objectives, governance

1. Introduction

Digital forensics (a.k.a. computer forensics) is a relatively new discipline, which has not as yet been adequately defined within a governance framework comparable to COBIT (Control Objectives for Information and Related Technology) [6] or ITIL (IT Infrastructure Library) [7]. The importance of digital forensics and its implementation within organizations are not well understood by organizations. According to Michael Bacon, evangelist and principal of archolutions.com [1]:

> *"Computer forensics is an area where many companies fear to tread—until they have to. It requires specialist training, not only in technology, but also in evidence gathering and presentation in court. Few corporates are prepared to invest the time and money in their own staff to train them up."*

A proper digital forensics governance framework is needed to address these issues. As no formal framework currently exists, we attempt to define one based on the literature in digital forensics and our experience

Please use the following format when citing this chapter:

von Solms, S., Louwrens, C., Reekie, C., Grobler, T., 2006 in International Federation for Information Processing, Volume 222, Advances in Digital Forensics II, eds. Olivier, M., Shenoi, S., (Boston: Springer), pp. 343–355.

in the discipline. The framework described in this paper incorporates control objectives (COs) and detailed control objectives (DF-DCOs), and is intended to provide a sound theoretical basis for digital forensics as well as a reference framework for digital forensics governance within organizations.

This paper begins by presenting the problem statement, definitions and phases of the digital forensic process, which form the basis for defining the relevant digital forensic control groupings. Next, the elements identified in the presentation are discussed briefly in formulating the control objectives (COs) and detailed control objectives (DCOs) for each phase. The consolidated COs and DCOs comprise the digital forensic control framework.

2. Digital Forensic Process

Digital forensics can be defined in different ways. We adopt the following definition for the purposes of this work:

> *Digital forensics comprises analytical and investigative techniques used for the preservation, identification, extraction, documentation, analysis and interpretation of computer media, which are digitally stored or encoded for evidentiary and/or root cause analysis.*

Casey [4] states that a standard operating procedure (SOP) should be performed whenever a computer is collected and/or examined. We call these SOPs "forensically-sound processes." Such processes maintain the integrity of evidence, ensuring that the chain of custody remains unbroken and that the collected evidence will be admissible in a court of law.

According to Kruse and Heiser [9], the digital forensic process involves four activities: (i) securing the evidence without contaminating it, (ii) acquiring the evidence without altering or damaging the original, (iii) authenticating that the recovered evidence is the same as the original seized data, and (iv) analyzing the data without modifying it. On the other hand, Carrier [2] identifies three phases in crime scene investigations: (i) system preservation, (ii) evidence search, and (iii) event reconstruction.

Kruse and Heiser as well as Carrier see the first step in the forensic process as securing/preserving the evidence in response to an incident, which is clearly reactive in nature. Rowlingson [12] argues that considerable effort should be put into "forensic readiness" to serve as an enabler for the subsequent incident response and investigation phases. Thus, planning and preparation must also be emphasized in the forensic process.

Kruse and Heiser [9] stress that criminal prosecution is one of the major goals of digital forensics. We can, therefore, postulate that the digital forensic process must also include a "juridical" or evidentiary phase. The term juridical is refers judicial proceedings or relating to the law.

3. Digital Forensics Control Framework

In our view, the digital forensic process has four phases: (i) planning and preparation (readiness), (ii) incident response (evidence preservation), (iii) investigation (evidence acquisition, authentication, search and analysis), and (iv) juridical or evidentiary (event reconstruction, root cause analysis and evidence presentation). The terms in parentheses denote the high-level control objectives for each phase.

The following sections discuss the four phases of the digital forensic process and their associated control objectives in detail.

3.1 Planning and Preparation Phase

This section focuses on the planning and preparation phase. Four high-level digital forensic control objectives (COs) and twenty-one detailed control objectives (DCOs) are defined for this phase, which collectively form Group I: Digital Forensic Readiness (see Table 1).

Digital Forensic Readiness: Digital forensic readiness is the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation. The goals of forensic readiness [12] are to: gather admissible evidence legally and without interfering with business processes, gather evidence targeting the potential crimes and disputes that may adversely impact an organization, allow an investigation to proceed at a cost in proportion to the incident, minimize interruption to the business from any investigation, and ensure that the evidence makes a positive impact on the outcome of any legal action.

The following ten steps describe the key activities involved in implementing a forensic readiness program [12]:

- Define the business scenarios that require digital evidence.
- Identify available sources and different types of potential evidence.
- Determine the evidence collection requirement.
- Establish a capability for securely gathering legally admissible evidence to meet the requirement.

- Establish a policy for secure storage and handling of potential evidence.
- Ensure monitoring is targeted to detect and deter major incidents.
- Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched.
- Train staff in incident awareness so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence.
- Document an evidence-based case describing the incident and its impact.
- Ensure legal review to facilitate action in response to the incident.

Computer Emergency Response Team: It is essential to establish a Computer Emergency Response Team (CERT) to ensure that the activities mentioned above are effectively utilized and executed following an incident. The CERT would have responsibilities and functions pertaining to planning and preparation, and incident response.

Policies Facilitating Investigations: Yasinsac and Manzano [12] note that enterprise policies can enhance computer and network forensics. They propose six categories of policies to facilitate digital forensic investigations: (i) retaining information, (ii) planning the response, (iii) training, (iv) accelerating the investigation, (v) preventing anonymous activities, and (vi) protecting the evidence.

The first four categories are included as high-level digital forensics control objectives in Group I: Digital Forensic Readiness (see Table 1). However, the first category (retaining information) is modified to "planning information retention requirements" to better describe the actions required during this phase. The remaining two categories (preventing anonymous activities and protecting the evidence) are included as detailed control objectives (DCOs). In all, Group I: Digital Forensic Readiness (Table 1) incorporates four high-level digital forensic control objectives (COs) and twenty-one detailed control objectives (DCOs).

3.2 Incident Response Phase

The incident response phase incorporates four high-level digital forensic control objectives (COs) and thirteen detailed control objectives (DCOs), which collectively form Group II: Evidence Preservation (see Table 2).

Table 1. Group I: Digital Forensic Readiness (4 COs with 21 DCOs).

DFR1 #	Planning Information Retention Requirements
DFR1.1	Define the business scenarios that require digital evidence.
DFR1.2	Identify available sources and different types of potential evidence.
DFR1.3	Determine the evidence collection requirement.
DFR1.4	Establish a policy for secure storage and handling of potential evidence.
DFR1.5	Establish a capability for securely gathering legally admissible evidence to meet the requirement.
DFR1.6	Synchronize all relevant devices and systems.
DFR1.7	Gather potential evidence.
DFR1.8	Prevent anonymous activities.

DFR2 #	Planning the Response
DFR2.1	Ensure monitoring is targeted to detect and deter major incidents.
DFR2.2	Implement intrusion detection systems.
DFR2.3	Specify circumstances when an escalation to a full formal investigation (which may involve digital evidence) should be launched.
DFR2.4	Establish a Computer Emergency Response Team (CERT).
DFR2.5	Establish capabilities and response times for external digital forensic investigation professionals.

DFR3 #	Digital Forensic Training
DFR3.1	Train staff in incident awareness, so that all understand their roles in the digital evidence process and the legal sensitivities of evidence.
DFR3.2	Develop an in-house investigative capability, if required.
DFR3.3	Enhance capability for evidence retrieval.

DFR4 #	Accelerating the Digital Forensic Investigation
DFR4.1	Document and validate an investigation protocol against best practice.
DFR4.2	Acquire appropriate digital forensic tools and systems.
DFR4.3	Ensure legal review to facilitate action in response to the incident.
DFR4.4	Define responsibilities and authority for CERT and investigative teams.
DFR4.5	Define circumstances for engaging professional investigative services.

Evidence Preservation: The purpose of this phase is to preserve the state of the crime scene. The first step in the incident response phase is to alert the CERT and initiate the incident response plan. One of the first tasks of the CERT is to secure all relevant evidence.

Evidence Transportation: The FBI's *Handbook of Forensic Services* [5] outlines a procedure for packing and shipping evidence, including computers and other electronic devices. A file should be stored

Table 2. Group II: Evidence Preservation (4 COs with 13 DCOs).

EPV1 #	Incident Response
EPV1.1	Initiate incident response plan.
EPV1.2	Activate the CERT.
EPV2 #	**Secure Evidence**
EPV2.1	Secure the physical environment of the crime scene.
EPV2.2	Secure all relevant logs and data.
EPV2.3	Secure volatile evidence, including laptops.
EPV2.4	Secure hardware.
EPV2.5	Label and seal all exhibits.
EPV2.6	Preserve chain of evidence.
EPV3 #	**Transport Evidence**
EPV3.1	Securely transport evidence.
EPV3.2	Preserve chain of custody during transport.
EPV4 #	**Store Evidence**
EPV4.1	Store evidence in safe custody room.
EPV4.2	Control access to evidence.
EPV4.3	Preserve chain of custody in storage.

on WORM (write-once-read-many) media, with a cryptographic hash stored offline in a physically secure container. Chain of custody documentation should be updated to reflect tracking numbers and other information [13]. Integrity of data that has undergone network transport may be proven via cryptographic hashing prior to sending and after receiving the data, and then comparing the hash values [13].

Evidence Storage: The objective of physical evidence storage is to provide a provable means of restricted access to evidence. Ultimately, a secure container in an audited access controlled room with camera monitoring and limited traffic would provide a foundation for the secure physical storage of evidence [13].

3.3 Investigation Phase

This section specifies five high-level digital forensic control objectives (COs) and eight detailed control objectives (DCOs) for the investigation

Table 3. Group III: Forensic Acquisition (5 COs with 8 DCOs).

FACQ1 #	**Ensure Integrity of Evidence**
FACQ1.1	Follow established digital forensic investigation protocols.
FACQ1.2	Write-protect all evidence source media.
FACQ2 #	**Acquire Evidence**
FACQ2.1	Acquire evidence in order of volatility.
FACQ2.2	Acquire non-volatile evidence.
FACQ3 #	**Copy Evidence**
FACQ3.1	Make forensic copies of all evidence.
FACQ4 #	**Authenticate Evidence**
FACQ4.1	Authenticate all evidence as identical to the original.
FACQ4.2	Time stamp all copies of the authenticated evidence.
FACQ5 #	**Document Acquisition Process**
FACQ5.1	Document all actions through chain of custody documentation.

phase, which collectively form Group III: Forensic Acquisition (see Table 3). The main aspects of the investigation phase are discussed below.

Forensic Acquisition: Forensic acquisition typically amounts to collecting volatile data (RAM, register state, network state, etc.) and imaging (forensic duplication) of disks. This process must use forensically-sound methods and conform with the widely-accepted order of volatility (OOV), which takes into account the fact that collecting some data affects other data.

Forensic Duplication: Forensic duplication of target media produces a "mirror image" of the target system. It also provides a working copy of the target media for analysis without the danger of altering or destroying potential evidence [11]. File-level copies, such as normal backups, do not yield all the potential evidence (e.g., deleted files, residual data on slack space and unallocated clusters).

Evidence Authentication: The integrity of the data/evidence must be unquestionable throughout preservation, acquisition, analysis and presentation. For this reason, the data should be cryptographically

hashed both collectively and individually, and the hashes themselves should be time-stamped.

Time-Stamping: According to Tan [13]: "Electronic documents will only stand up in court if the who, what and when they represent are unassailable." Evidence presented in court must, therefore, be time-stamped whenever possible.

Chain of Evidence Preservation: It is of paramount importance that the chain of evidence remains unbroken to ensure that an intact causal chain exists. Casey [3] introduces a scale (Casey's Certainty Scale) by which the trustworthiness of digital evidence can be assessed.

Chain of Custody: The objective of a chain of custody document is to track who had access to a given piece of evidence, when and, optionally, for what purpose. The life of a chain of custody document should start when the data is first considered as "potential evidence" and should continue through the presentation of the item as evidence in court [13].

3.4 Forensic Analysis Phase

Carrier [2] refers to forensic analysis as "evidence searching." He identifies four key actions: surveying the available evidence, setting a hypothesis, search for data to support or refute the hypothesis, and documenting the findings.

We define six high-level digital forensic control objectives (COs) and fourteen detailed control objectives (DCOs) for this phase, which collectively form Group IV: Forensic Analysis (see Table 4). A discussion of the main aspects of the forensic analysis phase follows.

Investigation Planning: All relevant information regarding the incident needs to be reviewed to determine what expertise is required and which forensic tools would be the most appropriate to use.

Hypothesis Development: A set of hypotheses must be developed to cover the most likely scenarios. Next, a set of criteria should be developed to either prove or disprove a specific hypothesis.

Evidence Acquisition: The evidence should be acquired using the most suitable forensic tool. It is important to use tools that have a proven track record and will be acceptable in court.

Table 4. Group IV: Forensic Analysis (6 COs with 14 DCOs).

FAN1 #	**Plan Investigation**
FAN1.1	Review all available information regarding the incident.
FAN1.2	Identify expertise required.
FAN1.3	Identify most suitable tools to be utilized.
FAN2 #	**Develop Hypothesis**
FAN2.1	Develop a hypothesis to cover most likely scenarios.
FAN2.2	Define criteria to prove or disprove the hypothesis.
FAN3 #	**Acquire Evidence**
FAN3.1	Acquire evidence using the most suitable tools available.
FAN3.2	Analyze evidence using the most suitable tools available.
FAN3.3	Conform to the requirements of the "best evidence rule."
FAN4 #	**Test Hypothesis**
FAN4.1	Reconstruct sequence of events.
FAN4.2	Compare evidence with other known facts.
FAN5 #	**Make Finding**
FAN5.1	Make a finding that is consistent with all the evidence.
FAN5.2	Document the finding.
FAN6 #	**Document Case**
FAN6.1	Document all aspects of the case.
FAN6.2	Enter documentation into safe custody.

Best Evidence Rule: Courts sometimes require the original written material, recordings and photographs to exhibited as evidence [3]. This was intended to prevent witnesses from misrepresenting such materials and simply accepting the testimony regarding the contents. With the advent of photocopiers, scanners, computers and other technology that create effectively identical duplicates, copies became acceptable in place of the originals, unless a genuine question was raised about the authenticity of the original, the accuracy of the copy or if, under the circumstances, it would be unfair to admit the copy in lieu of the original. Because an exact duplicate of most forms of digital evidence can be made, a copy is generally acceptable. In fact, presenting a copy of digital evidence is usually more desirable because it eliminates the risk

that the original will be accidentally altered. However, this may vary according to the jurisdiction. Section 15 of the South African Electronic Communications and Transactions Act 25 of 2002 (ECT Act) provides that the rules of evidence must not be applied to deny the admissibility of a data message purely because it is constituted by a data message, or on the grounds that it is not in its original form, if it is the best evidence that the person adducing it can obtain.

Hypothesis Testing: The hypothesis must be tested against the acquired evidence and should enable investigators to reconstruct credible sequences of events. It should also be compared to other known facts [2].

Findings: Once all possible evidence has been considered, a finding can be made that is consistent with all the known facts. The finding—as well as the reasoning behind it—should be documented.

Documentation: The case must be thoroughly documented. This includes all the investigative actions taken, extracts of the evidence, deductions and findings. It is important to note that these facts may be called into question in litigation many years after the investigation.

3.5 Juridical/Evidentiary Phase

The juridical/evidentiary phase is arguably the most important phase in the digital forensic process as it determines if all the preceding effort will bear fruit or come to nothing. This phase involves three steps that must be taken to ensure a successful conclusion to the case: case preparation, case presentation and evidence preservation. Three high-level digital forensic control objectives (COs) and ten detailed control objectives (DCOs), corresponding to Group V: Evidence Presentation, are defined for this phase (see Table 5).

Case Preparation: Legal requirements vary according to jurisdiction. Due to the nature of cyber crime, many investigations will involve international components and may require investigators to conform to several differing legal requirements.

Expert witnesses must be identified and thoroughly prepared. Exhibits must also be prepared taking the target audience into consideration. These can include presentation aids like graphics, slide shows, photographs, hardware and even live demonstrations.

Table 5. Group V: Evidence Presentation (3 COs with 10 DCOs).

EP1 #	Prepare Case
EP1.1	Determine target audience (court, disciplinary hearing, inquiry).
EP1.2	Assemble evidence required for presentation.
EP1.3	Prepare expert witnesses.
EP1.4	Prepare exhibits.
EP1.5	Prepare presentation aids (graphics, slides, hardware).
EP1.6	Preserve chain of custody.

EP2 #	Present Case
EP2.1	Present evidence in a logical, understandable way to ensure that the court can critically assess every bit of information and understand the relevance to the case.
EP2.2	Make use of graphics and physical examples to illustrate difficult or critical concepts, if needed.
EP2.3	Ensure that a digital forensic specialist is at hand to assist in providing expert evidence.

EP3 #	Preserve Evidence
EP3.1	Preserve the evidence after the case has been presented, as it may be needed in case of appeal or if new evidence is obtained.

Vacca [14] lists four tests that should be applied to evidence: (i) authenticity, (ii) reliability, (iii) completeness, and (iv) freedom from interference and contamination.

Case Presentation: Evidence must be presented in a logical, understandable way to ensure that the court can critically assess every bit of information and understand its relevance to the case.

Since the investigative process can be attacked by the defense, regardless of how overwhelming the evidence might be, specific care should be taken to stress that an internationally accepted forensic process had been followed and that the chains of evidence and custody have remained intact throughout the process.

Evidence Preservation: Evidence must be preserved securely after the case has been presented as it may be needed again in case of appeal or if new evidence becomes known.

4. Conclusions

The digital forensics reference framework presented in this paper incorporates five high-level digital forensics control objectives: (i) digital forensic readiness, (ii) evidence preservation, (iii) forensic acquisition, (iv) forensic analysis, and (v) evidence presentation. These five digital forensic control groupings are refined into 22 control objectives (COs), which are further refined into 66 detailed control objectives (DCOs). Several of the DCOs relate to "forensically-sound processes," which must be executed in sequence or in conjunction with each other. The reference framework is intended to provide a sound theoretical basis for digital forensics as well as a foundation for the practical implementation of digital forensics governance within organizations.

We are currently engaged in mapping the digital forensics control objectives (COs) against well-established governance frameworks like COBIT, ISO/IEC 17799 [8] and ITIL [7]. Interested readers are referred to [10] for preliminary results of this effort.

References

[1] I. Armstrong, Computer forensics: Detecting the imprint, *SC Magazine*, August 2002.

[2] B. Carrier, *File System Forensic Analysis*, Addison-Wesley, Upper Saddle River, New Jersey, 2005.

[3] E. Casey, *Digital Evidence and Computer Crime*, Academic Press, London, United Kingdom, 2001.

[4] E. Casey (Ed.), *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, Elsevier Academic Press, London, United Kingdom, 2004.

[5] Federal Bureau of Investigation, *Handbook of Forensic Services* (www.fbi.gov), 2003.

[6] Information Technology Governance Institute, *COBIT: Control Objectives for Information and Related Technologies*, Rolling Meadows, Illinois, 2000.

[7] Information Technology Infrastructure Library (www.itil.co.uk), Office of Government Commerce, London, United Kingdom.

[8] International Organization for Standardization, *ISO/IEC 17799: Code of Practice for Information Security Management*, Geneva, Switzerland, 2000.

[9] W. Kruse and J. Heiser, *Computer Forensics: Incident Response Essentials*, Addison-Wesley, Reading, Massachusetts, 2002.

[10] C. Louwrens and S. von Solms, The relationship between digital forensics, corporate governance, information technology governance and information security governance, in *Digital Crime and Forensic Science in Cyberspace*, P. Kanellis, E. Kiountouzis, N. Kolokotronis and D. Martakos (Eds.), Idea Group, Hershey, Pennsylvania, 2006.

[11] K. Mandia, C. Prosise and M. Pepe, *Incident Response and Computer Forensics*, McGraw-Hill/Osborne, Emeryville, California, 2003.

[12] R. Rowlingson, A ten step process for forensic readiness, *International Journal of Digital Evidence*, vol. 2(3), pp. 1-28, 2004.

[13] J. Tan, Forensic readiness (www.webproxy.com/research/reports/acrobat/atstake_forensic_readiness.pdf), July 17, 2001.

[14] J. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, Charles River Media, Hingham, Massachusetts, 2002.