



The Enhanced Digital Investigation Process Model

By

Venansius Baryamureeba, Florence Tushabe

Presented At

The Digital Forensic Research Conference

DFRWS 2004 USA Baltimore, MD (Aug 11th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<http://dfrws.org>



The Enhanced Digital Investigation Process Model


— — — — —
— — — — —

Venansuis Baryamureeba and **Florence Tushabe**
Makerere University, Institute of Computer Science

To be Presented at the Digital Forensics Research Workshop - 2004 Maryland, Baltimore on 11th August 2004.



Overview

- Previous Models
 1. The Forensics Process Model
 2. The DFRWS Process Model
 3. The Abstract Forensics Process Model
 4. The Integrated Digital Forensics Model (IDIP)
 - The Proposed Model
 - The Enhanced Digital Investigation Process Model (EDIP)
 - Concluding Remarks
- 



The Forensics Process Model



Collection Phase

Evidence Search, recognition, collection and Documentation

Examination Phase

To facilitate Visibility of evidence and explain it's origin and significance.

Analysis Phase

Looks at the product of the examination for it's significance and probative value

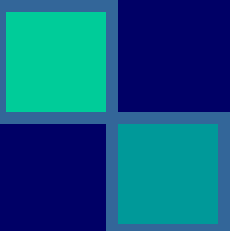

Reporting Phase

Involves writing a report outlining the examination process and pertinent data recovered.





The DFRWS Model

1. Identification – Event Crime Detection, Profile detection, Anomalous detection, complaints, system monitoring, Audit analysis etc
 2. Preservation – Case management, Imaging technologies, chain of custody, time synchronization
 3. Collection – Preservation, Approved methods, hardware and software; legal authority, loss less compression, sampling, data reduction, recovery techniques.
- 
- 




..... The DFRWS Model

4. Examination – Preservation, traceability, validation and filtering techniques, pattern matching, hidden data recovery and extraction.
5. Analysis – preservation, traceability, statistical, protocols, data mining, timeline, link
6. Presentation – documentation, expert testimony, clarification, mission impact statement, statistical interpretation and recommended counter measure.
7. Decision – the decision by final authorities like courts of law and corporate management.

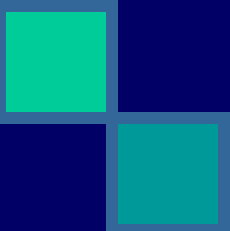



The Abstract Digital Forensics Model (ADFM)

1. Identification – determines an incident from indicators and determines it's type.
 2. Preparation – Preparation of tools, techniques, search warrants, monitoring authorization and management support.
 3. Approach Strategy – Develops an approach for maximizing collection of untainted evidence from crime scene.
- 

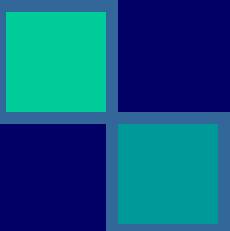



..... ADFM

4. Preservation – Isolation, securing and preservation of physical and digital evidence.
 5. Collection – recording of the physical scene and duplicate digital evidence.
 6. Examination – an in-depth systematic search of evidence.
 7. Analysis – determination of the significance of evidence and reconstructing fragments of data and drawing conclusions based on the evidence found.
- 
- 



..... ADFM

- 
8. Presentation – summary and explanation of conclusions.
 9. Returning Evidence – returning the physical and digital property to the proper owner.
- 

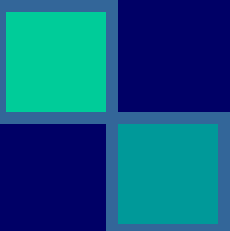



Differences between DFRWS Model and the Abstract Forensics Model

- Adds a description for all the phases.
- Places extra 2 phases between the identification and Preservation phases. Which are the preparation and Approach Strategy phases.
- The last phase (Decision) was replaced with returning evidence.




Comments

- 
- The third phase (Approach strategy) is to an extent a duplication of the second phase (preparation). (No phase between to distinguish them)
 - Practically, the Preparation phase should come before the identification
- 

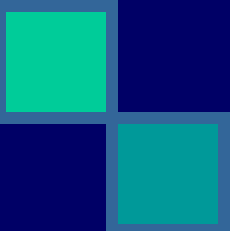



The Integrated Digital Investigation Process Model (IDIP)

- 1. Readiness Phases
 - 2. Deployment Phases
 - 3. Physical Crime Investigation Phases
 - 4. Digital Crime Investigation Phases.
 - 5. Review Phases
- 

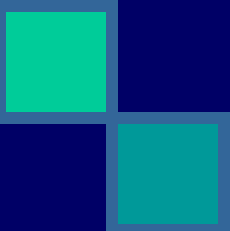



1. Readiness Phases

- 
1. Operations Readiness Phase – human capacity training.
 2. Infrastructure Readiness Phase – sufficient infrastructure like equipment, transport, communication facilities.
- 



2. Deployment Phases

- 
3. Detection and Notification Phase – Incident is detected and appropriate people notified.
 4. Confirmation and Authorization – Confirms the incident and obtains legal approval.
- 



3. Physical Crime Scene Investigation Phases

5. Preservation phase – preserves the physical crime scene so that evidence is later collected by trained personnel.
6. Survey phase – investigator walks through the physical crime scene and identifies pieces of physical evidence.
7. Documentation phase – capturing as much information as possible from the crime scene e.g photographs, videos, sketches.




.....Physical Crime Scene Investigation Phases

7. Search and Collection phase – in-depth search and collection of the scene, additional evidence is identified.
8. Reconstruction – organising the results from analysis and developing a theory for the incident.
9. Presentation phase – presents the physical and digital evidence to court or corporate management.

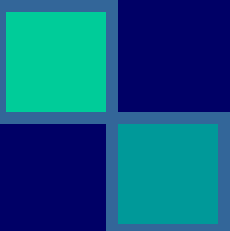



4. Digital Crime Scene Investigation Phases

11. Preservation phase – preserves the digital crime scene so that evidence is later collected by trained personnel.
 12. Survey phase – investigator transfers relevant data to a controlled location.
 13. Documentation phase – Properly documenting the digital evidence when it is found.
- 

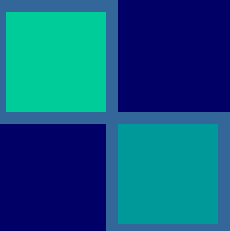



..... Digital Crime Scene Investigation Phases

- 
13. Search and Collection phase – in-depth analysis of the digital evidence is performed.
 15. Reconstruction – putting the pieces of the digital puzzle together and developing investigative hypotheses.
 16. Presentation phase – presents the digital evidence that was found to the physical investigative team.
- 

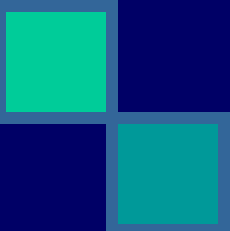



5. Review Phases

- 
17. Review Phase – the whole investigation is reviewed and areas of improvement identified.
- 



Comments

- 
- It simplifies the forensic process by grouping the phases into an abstract and manageable manner.
 - It highlights reconstruction.
 - It differentiates between the digital and physical crime scenes.
 - Emphasizes the review of the whole process, while putting the preparation phase before detection of the incident.
- 




However....

- It depicts the deployment phase (Detection and confirmation) as being independent of the digital and physical investigations.
- It depicts the forensic process as linear.
- It doesn't draw a clear distinction between investigations at the victims and suspects crime scene.
- It contains two reconstructions – may sometimes contradict.



The Enhanced Digital Investigation Process Model (EDIP)


- It is based on the Integrated Digital Investigation Process (IDIP) Model.
 - Consists of 5 major phases consisting of 14 phases altogether.
- 



Definitions

A. Physical Crime Scene Investigation

Is the investigation that takes place at the primary crime scene.

1. Preservation phase – preserves the physical crime scene.
 - i. Securing and protecting the crime scene
 - ii. Identifying, removing and separating witnesses.
 2. Survey phase – investigator walks through the physical crime scene.
 - i. Identifies pieces of physical evidence.
 - ii. Determines the extent of the search
 - iii. Develops a preliminary theory
 - iv. Identifies potential evidence
- 



..... physical crime scene investigation

- 
3. Documentation phase – to capture as much information as possible

Taking photographs, sketches and videos


4. Search and Collection phase – in-depth search and collection of the scene for additional potential physical evidence.
- 

5. Presentation phase – electronic evidence is transported and delivered to the digital investigation team.




B. Digital Crime Scene Investigation

Is the investigation that takes place at the digital crime scene.

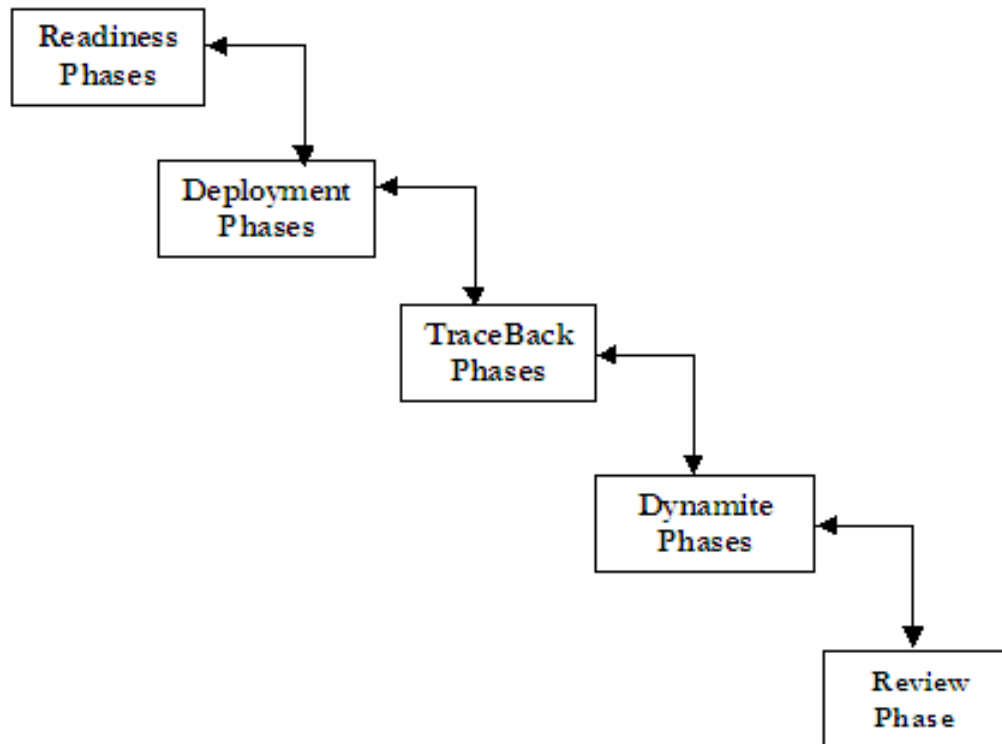
1. Preservation phase – preserves the digital crime scene.
 - i. Synchronization.
 - ii. Duplication – bit by bit copies
 - iii. Analysis.
 2. Survey phase – investigator separates potentially useful data from imaged dataset.
Recovery of damaged, hidden, deleted and manipulated data.
- 



.....Digital Crime Scene Investigation


3. Search and Collection phase – in-depth analysis of digital evidence.
 - i. Reveals hidden, deleted, swapped and corrupted files.
 - ii. Fusion, correlation, graphing, mapping and timelinning of files.
 - iii. Investigative hypotheses developed.
 4. Documentation – to record the digital evidence, it's location and probably how it was interpreted.
- 

Phases of the EDIP Model





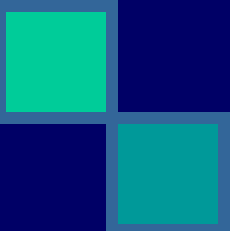

1. The Readiness Phases

- Same as in the IDIP Model
 1. Operations Readiness phase
 2. Infrastructure Readiness phase.
- 



2. The Deployment Phases

Provides a mechanism for an incident to be detected and confirmed.


- 
3. Detection and notification Phase.
 4. Physical Crime Scene Investigation phase.
(Preservation, Survey, Search and collection, Documentation, Presentation)
 5. Digital Crime Scene Investigation phase.
(Preservation, Survey, Search and Collection, Documentation)
 6. Confirmation phase.
 7. Submission phase – physical and digital evidence is submitted to legal entities.
- 



3. Traceback phases



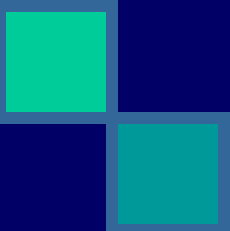

The Perpetrator's primary crime scene is traced.

- 
8. Digital Crime Scene Investigation
IP addresses easily traced using nslookup, dig, tracert from a DNS server
 9. Authorization – from local authorities



4. Dynamite phases

They investigate the primary crime scene.

10. Physical Crime Scene Investigation Phase
(Preservation, Survey, Search and collection, Documentation, Presentation)
 11. Digital Crime Scene Investigation phase.
(Preservation, Survey, Search and Collection, Documentation)
 12. Reconstruction – identifying the best investigative hypothesis using evidence gathered.
 13. Communication – final interpretations and conclusions presented to legal entities.
- 
- 



5. Review Phase.



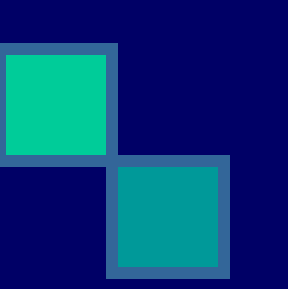
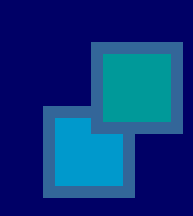
14. The Review Phase

- Same as in the IDIP Model
 - The whole investigation is reviewed and areas of improvement identified.
- 

	IDIP	EDIP
Review Phases/ Review Phases	<ul style="list-style-type: none"> ■Operations ■Infrastructure 	<ul style="list-style-type: none"> ■Operations ■Infrastructure
Deployment phases/ Deployment phases	<ul style="list-style-type: none"> ■Detection and notification ■Confirmation and Authorization 	<ul style="list-style-type: none"> ■Detection and notification ■Phy crime scene Inv ■Dig crime scene inv ■Confirmation ■Submission
Physical Crime Scene Investigation phases/ Traceback phases	<ul style="list-style-type: none"> ■Presentation ■Survey ■Documentation ■Search and Collection ■Reconstruction ■Presentation 	<ul style="list-style-type: none"> ■Dig crime scene inv ■Authorization
Digital Crime Scene Investigation phases/ Dynamite Phases	<ul style="list-style-type: none"> ■Presentation ■Survey ■Documentation ■Search and Collection ■Reconstruction ■Presentation 	<ul style="list-style-type: none"> ■Phy crime scene Inv ■Dig crime scene inv ■Reconstruction ■Communication
Review phase/Review	Review	Review

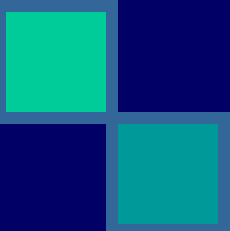



The Proposed Model (EDIP)

- 
1. Depicts the forensic process as iterative as opposed to linear.
 2. Re-defines the phases in the physical and digital crime scene investigation phases.
 3. Re-defines the Deployment phase.
 4. Differentiates the investigations at the primary (suspect) and secondary (victim) crime scenes.
- 

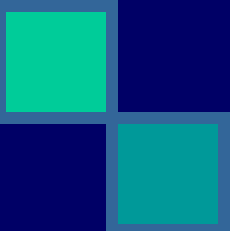


.....The proposed Model (EDIP)

- 
5. Highlights tracing back to the perpetrators scene.
 6. It reserves only one reconstruction (at the end) but provides for investigative hypotheses during the entire process.
 7. Suitable for cybercrime investigations
- 



Concluding Remarks

- 
- The previous forensic process models like the Forensic process model, the DFRWS-2001 model, The ADFM, and The IDIP model.
 - Introduced a modified and enhanced forensic model – the EDIP model.
 - More details can be found in the paper is found at <http://makerere.ac.ug/ics/1/academics/research/>
- 