RESEARCH ARTICLE OPEN ACCESS

A Comparative Analysis of Digital Forensics Models for Cybersecurity

Rajesh Kumar Goutam
Department of Computer Science, University of Lucknow, Lucknow
Email: rajeshgoutam82@gmail.com

Abstract:

The digital forensics plays crucial role in crime investigations and allows law enforcement agencies to seize, examine, preserve and collect evidences from computers and other communication devices to re reconstruct digital events. The significance of digital forensics continues to be increasingly prominent as it not only helps to gather evidences but also determines the timeline of events in crime. Digital forensics is all about to scientifically investigate and record authenticated results in legal document while ensuring its admissibility in court of law to aid prosecution. In this paper, we present a brief overview of three popular forensic models and evaluate them to highlight their key features and suitability in legal proceedings.

Keywords —**Digital Forensics, Cybersecurity, Digital Investigation.**

I. INTRODUCTION

Due to exponential growth in technology adoption and utilization of internet as intermediary tool to trigger crime highlights the need of a comprehensive approach commonly known as digital forensics. It enables us to identify, investigate, recover and preserve digital evidences scientifically and assists to handle cybercrime incidents affectively. The acquisitions of evidences are made from computer components, installed software, network segments, clouds and other internet enabled devices. V. Baryamureeba and F. Tushabe [1] defines the digital forensics as utilization of scientifically derived and proven methods towards identification, preservation, collection, validation, identification, analysis, interpretation and documentation of digital evidences derived from digital assets for the purpose of facilitating or furthering the reconstruction of events found to be malicious or helping to anticipate the illegitimate actions shown to be disruptive to planned operations [2].Digital forensics is crucial to resolve criminal cases, financial frauds, embezzlement, industrial espionage, spamming and stalking cases and to identify vulnerabilities and to uncover criminals. It revel the answer of following facts [3]:

1. It helps to find out reasons and to identify the goals of cyberattacks.
2. It helps to have containment and remediation to attacks.
3. It preserves digital evidences before their absolutions.
4. Retracing hacker's action and finding tools used to commit digital crimes.
5. Identifying the areas of digital assets which were accessed and exfiltrated.
6. Detection of breached integrity of stored data.
7. Duration computation of illegitimate access to network and resources.
8. Geolocating the criminals logins to know the true culprits.

II. Digital Forensic: A Multi-staged Process

Digital forensic is multi-staged process that helps forensic specialists to achieve high quality of digital evidences and ensuring their credibility and acceptability for court proceedings. S. Raghavan [4] suggests five stages of digital forensic as shown in figure.

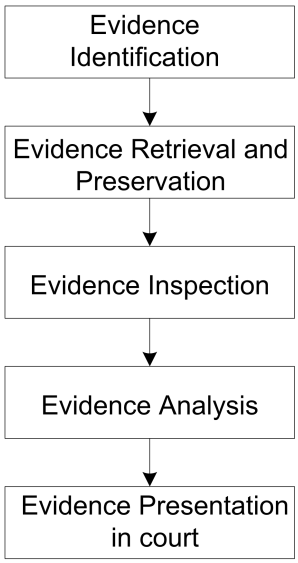

Fig. 1: Digital Forensic Stages

The first stage identifies potential devices as well as locations from which evidences can be collected. As digital evidences are inherently more delicate and become always at risk to have undesired alteration so it becomes imperative to handle and preserve them with utmost possible care to ensure its integrity and credibility. In Evidence Retrieval and Preservation stage the binary bitwise copy of digital contents is retrieved and preserved after its content verification with cryptographic tools like MD5 and SHA1. In this stage, we attempt to have forensic image of device by copying its bit-to-bit copy of data and ensuring its integrity too during investigation. Evidence inspection is the stage where forensic experts physically deal with evidences with a clear mindset to what needs to be collected. In analysis phase, the recovered data is interpreted in logical manner to determine its significance to the case and all the dots are connected to have complete picture. Timeframe analysis is performed to determine the timings of events recorded in system, to decide the possession at particular event and to determine the timestamp in file system metadata such as file creation, alteration and last accessed. The analysis phase attempts to find answer of followings facts:

1. How did evidence get there?
2. Where did it come from?
3. How is it relevant to legal Proceeding?

The last stage in digital forensic process is responsible for completely and accurately reporting key findings and making their admissibility in court in well prepared documentation form. The final report is prepared with proven techniques and methodologies so that it can get duplicate to reproduce same results.

III. Digital Forensic Investigation Model (DFIM)

Although Digital forensic is new field of research but it has made remarkable progress. Researchers developed tools to collect and examine digital evidences, presented methodologies to set the appropriate direction of investigation and proposed several models to guide investigation, to ensure credibility of evidences and making them admissible to court. In literature, numerous investigation models have been proposed to date and each one attempts to refine the standard procedure of investigation with several phases and validations. Kruse and Heiser [5] proposed (DFIM) with three phases named acquiring evidence, authenticating evidence and analyzing evidence as shown in figure.

Fig. 2: DFIM Phases

DFIM mainly attempts to maintain the integrity of evidences and authenticates the validity of extracted data with test cases during investigation [6].

IV. Forensics Process Model (FPM)

M. Mukasey et al. [7] proposed Forensics Process Model to investigate electronic crime scene, containing four phases named collection,

examination, analysis and reporting as shown in figure.

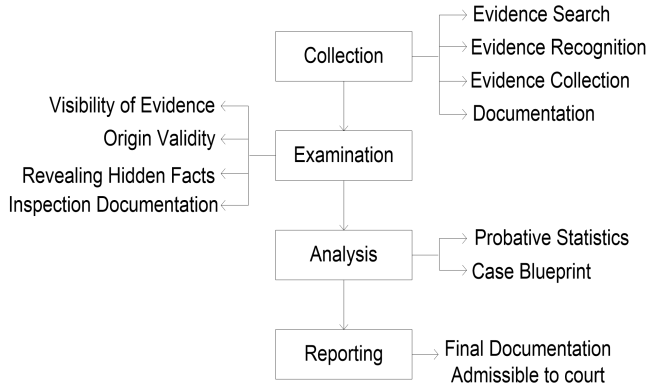

Fig. 1: FPM Phases

This model believes in integrity of evidences too and suggests to not to get performed collection and analysis process with novices due to risks of interruptions in evidences which can mislead entire investigation process. In the first phase collection covers evidence search, evidence identification, evidence gathering and evidence documentation. Its examination phase includes to justify the visibility of evidences, revealing the hidden facts and highlighting obscured information and making a complete picture of crime with admissibility in court of law. The analysis phase investigates the outcome of examination phase and checks its significance and relevancy to the legal prosecution. The reporting phase entails writing final report outlining the outcomes of all previous phases and securing pertinent statistics gathered from overall investigation. The forensic process model suffers with ambiguity in its analysis phase.

V. Abstract Digital Forensics Model

A technology independent forensic model named Abstract Digital Forensic Model (ADFM) presents a clearer and structured way for investigation. Mark Reith et al. [8] combined key aspects of Digital Forensic Process Model and Forensics Process Model, and extended DFRW as Abstract Digital Forensics Model. The authors introduced three crucial steps Preparation, Approach Strategy and Returning Evidences to refine traditional digital investigation process [9]. ADFM constitutes nine phases as shown in figure.

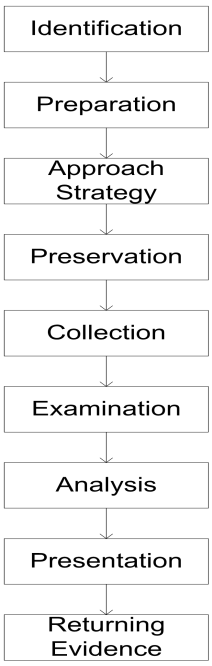

Fig. 4: ADFM Phases

VI. Analysis of the DFIM, FPM and ADFM

DFIM does not entail the preparation of tools and strategy before evidence extraction and also lack the preservation phase to maintain the integrity of collected evidences. The FPM extended DFIM and incorporated reporting phase to facilitate documentation of scientifically collected facts with admissibility to court of law. The key features of all these three models have been depicted in following table 1

TABLE I
Key Features of DFIM, FPM and ADFM

Investigation Model	Phases	Key Features
Digital Forensic Investigation Model (DFIM)	Acquire Authenticate Analysis	• It is Simple model • It lacks Reporting step • Popularly known as 3A Model • No provision for documentation of investigation process • Guarantees evidence integrity. • It is silent admissibility of evidences to court.
Forensics Process Model (FPM)	Collection Examination Analysis Reporting	• FPM includes Reporting. • Examination phase covers authentication. • It allows documentation for investigation. • Analysis phase of FPM is ambiguous and improperly

		defined. • Analysis and Interpretation deliver identical results.
Abstract Digital Forensics Model (ADFM)	Identification Preparation Approach-Strategy Preservation Collection Examination Analysis Presentation Returning Evidence	• ADFM supports preservation of evidences before making its replica. • Third phase duplicates its second phase. • It has separate step to choose appropriate tools and strategy planning before evidence acquiring. • It has ability to reconstruct data fragments and draw conclusions. • Technology independent. • Consistent and Standardized framework for digital forensic.

ADFM has ability to recognize key locations from which evidences can be collected. It authenticates the evidences and validates locations to ensure the integrity of extracted data. The following table 2 shows the stepwise comparison of ADFM, FPM and DFIM.

TABLE II
FONT INVESTIGATION PHASES IN ADFM, FPM AND DFIM

Phases	ADFM	FPM	DFIM
Collection	✓	✓	✓
Examination	✓	✓	✓
Analysis	✓	✓	✓
Reporting	✓	✓	
Preparation	✓		
Preservation	✓	✓	
Approach Strategy	✓		
Presentation	✓	✓	
Identification	✓	✓	✓
Return Evidence	✓		
Decision			
Review			
Reconstruction	✓		
Documentation			
Authorization	✓		✓
Survey			
Traceback		✓	
Testing			
Reconnaissance	✓		

VII. ANALYSIS AND COMPARISON OF THE DFIM, FPM AND ADFM

The earliest forensic model employed to computer forensic is popularly known as DFIM. It constitutes three phases acquire, authentication and analysis and attempts to maintain the integrity of digital evidences. DFIM presumes digital investigation data is fragile, highly volatile and can be easily modified, disrupted and damaged. Therefore, DFIM attempts to ensure that investigation data is collected and preserved correctly with validated source prior to its analysis phase. The second step ensures that recovered evidence is the replica of originally seized one as tampered and contaminate evidence may loss its exact meaning and may cause its dismissals from court proceedings too. The analysis phase processes unaltered data with intact integrity and validity and maps relationships with other activities and facts to solve the case. The DFIM lacks step to potential admissibility of collected evidences before court for legal prosecution [10]. FPM refined DFIM and introduced reporting step to entail writing a report outlining the examination outcomes and to proceed towards admissibility to court. FPM is generalized forensics model equally applicable to computers or other electronic devices and lists the distinct types of evidences can be collected with their potential locations [10]. Although, reporting step makes FPM more suitable than DFIM for legal proceedings but suffers with ambiguity as its analysis phase improperly defined. The examination and analysis phases sometimes deliver identical facts as no proper distinction made during their interpretation. The Abstract Digital Forensic Model presents a good reflection to forensic process and provides a clear and structured way for investigation. The three significant phases named preparation, approach strategy and returning evidence makes ADFM more effective and flexible over DFIM and FPM as it ensures isolated and secure evidence extraction with unaltered integrity.

VIII. CONCLUSIONS

Digital forensic models guide us about the scientific procedures that need to be undertaken during the investigation, regardless of the technology being used to trigger malicious attempts. In this paper, we investigate three key forensic model and examined that DFIM does not believes in preparation and reporting steps that signifies its

incompleteness in digital forensic process. A subsequent model FPM extended DFIM with its reporting step but was not capable to reconstruct the malicious events. We examined that ADFM believes in preparation of methodology used to extract evidences, emphasizes on protection of evidences to ensure its integrity and have the ability to reconstruct the incidents.

.

REFERENCES

[1] Venansius Baryamureeba and Florence Tushabe, "The Enhanced Digital Investigation Process Model", Institute of Computer Science, Makerere University, 2004.

[2] A Report, "A Road Map for Digital Forensic Research", The Digital Forensic Research Conference, USA, 2001.

[3] A report available at: https://ermprotect.com/blog/what-is-digital-forensics-and-when-do-you-need-it/.

[4] Sriram Raghavan, "Digital Forensic Research: Current State-of-the-Art", CSI Transactions on ICT, 2013, pp. 91-114.

[5] Warren G. Kruse and Jay G. Heiser, "Computer Forensics: Incident Response Essentials", Wesley, 2002..

[6] Venansius Baryamureeba and Florence Tushabe, "The Enhanced Digital Investigation Process Model", Digital Forensic Research Conference (DFRWS), Institute of Computer Science, Makerere University, Kampala Uganda, 2004

[7] Michael B. Mukasey, Jeffrey L. Sedgwick, David W. Hagy, "Electronic Crime Scene Investigation: A Guide for First Responders", special report, U.S Department of Justice, April, 2008

[8] Mark Reith, Clint Carr and Gregg Gunsch, "An Examination of Digital Forensic Models", International Journal of Digital Evidence, 2002

[9] *Kwaku Kyei, Pavol Zavarsky, Dale Lindskog and Ron Ruhl, "A Review and Comparative Study of Digital Forensic Investigation Models", 2013*

[10] Brian D. Carrier and Eugene H. Spafford, "An Event-Based Digital Forensic Investigation Framework", Digital Investigation