RESEARCH ARTICLE OPEN ACCESS

Digital Forensic Models Investigation with Cybersecurity

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

Abstract:

The role of digital forensic is crucial to fight against cybercrime, to trace cybercriminals and to solve digital mysteries. It recognizes and validates the participating devices that need to be examined to extract relevant evidences and suggests techniques to preserve these evidences to avoid any alteration and contamination. Effective investigation of devices requires globally accepted scientifically proven phases which are serially attached to form a model. Forensic models help to reveal who committed crime with what intention, followed what procedure and tools and to uncover intermediaries and targets. This paper examines three most prominent cyber forensic models and presents their phase wise comparison to know their effectiveness.

Keywords —**Cyber Forensics, Digital Forensics, Cyber Security**

I. DIGITAL FORENSIC

Digital forensic is crucial part of cyber security as it facilitates to investigate crime, extraction of evidences from digital devices, and examining collected evidences to identify the criminals, to estimate damages and to know how criminals committed the crime together with its intermediaries [1]. It uses scientifically driven and proven methods to identify, collect, preserve, validate, analyse and interpret the evidences and to have its documentation for legal proceedings. Initially, the resources that may contain are seized thereafter duplicators are used to generate replica of existing seized resource to have its duplicate copy to avoid the risk with integrity of original resource. Forensic experts examine physical area of resources, scrutinize files and folders with trails of actions performed over them, and investigate crucial logs. Instant messaging, e-mails, and browsing history are also inspected in connecting the dots and to draw conclusions [4].

Forensic is not limited to examine devices instead it is performed for intrusion detection due to network traffic. The entire traffic or its chunks are investigated for unauthorized access, malicious attempts, and data breaches as well as to know the illicit traffic pattern. Digital forensic is performed to establish different pieces of communications along with their timelines to have better understanding about question like who committed crime and how crime has happened under what circumstances and premises [5]. Forensic experts find the events of human communication check the attempts of file tampering and detect the events keyword usage to uncover mysterious [6].

II. FORENSIC MODELS

Although digital forensic is rapid growing field of research but still it faces several challenges. The need of investigation model that governs forensic procedure and decides organizational capability of cyber defences is still vital and awaited [7]. The lack of globally accepted standards and rules are just like barriers that result not only in loss in efficiency but also have possibility to lose critical evidences and knowledge [8]. Forensic model sets common procedures and guidelines that need to be adopted during investigation regardless of technologies used in illicit events. In literature, several forensic models have been proposed to date and each one suggests a sequence of actions and

multiple phases need to be performed during investigation [9]. The most three predominant models are being overviewed here.

A. Digital Forensic Investigation Model (DFIM)

Kruse and Heiser [3] emphasized on steps that should essentially need to be followed and proposed a model to facilitate digital forensic [1] [7]. DFIM constitutes three phases named acquiring the evidences, authenticating the evidences and analysing the evidences as shown in figure 1. It suggests crime scene shielding to avoid contamination of data and network traffic. The main attraction of DFIM is authentication of collected evidences that ensures no false positives are being analysed and participated in investigation process [1]. The authentication field validates the source of data and ensures that potential devices are being analysed to collect the evidences. DFIM uses scientifically proven methods to analyse collected data but do not emphasize on the needs of surveying about the locations from where evidences needs to be collected. DFIM is popular due to its simplicity and accuracy but not suitable for legal prosecution as it neither attempts for documentation of evidences nor makes evidences admissible to law enforcement agencies [1][2]. DFIM lacks reconstruction phase so investigators need to work with original evidences so this model has risks of evidences contaminated or loss. The DFIM mainly entails to integrity of evidences and its maintenance across its all three phases.

Fig. 1: DFIM Phases

B. Digital Forensic Process Model (DFPM)

U.S Department of Justice proposed DFPM to investigate electronic crime scene and interpret the crime related incidents to have concrete results [12]. It has four phases named collection, examination, analysis, and reporting, and facilitates documentation of investigation results while ensuring its admissibility to court [2] [10]. Initially, crime-scene shielding is done to avoid contamination of devices and disturbance in traffic thereafter evidence search is performed to locate the devices that might contain relevant data about digital crime [2]. The collection phase acquires the evidences after seizing the internet enabled devices and network traffic and do not allow the original evidences to be lost or damaged as its can change the investigation direction. The examination phase allows checking the visibility of evidences and decides whether the collected evidence is relevant to investigation or not [11]. DFPM validates the source of evidences and attempts to reveal hidden and obscured information essential to resolve the dispute. The four phases with all activities has been depicted in following figure 2. DFPM also suffers with critics as its analysis phase is improperly defined and has ambiguity. DFPM considers analysis phase identical to interpretation which are completely distinct process [10].

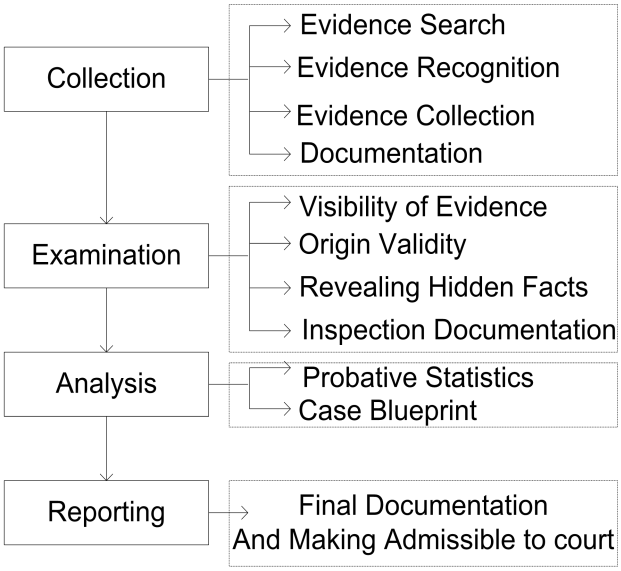

Fig. 2: DFPM Phases

C. Abstract Digital Forensic Model (ADFM)

Kruse Mark Reith, Clint Carr and Gregg Gunsch [10] proposed a standardized process for digital investigations which not only focus to collection of evidences but also emphasizes to need of preparation before to get start forensic [10]. ADFM is suitable for wide range of digital devices such as calculators, mobiles and computers for forensic and

presents a consistent and standardized methodology to collect evidences. ADFM has been formulated for unrealized digital devices too for future and facilitates analysing new digital and electronic technologies when applied for forensics [10]. This model is notable due to its crime-scene reconstruction ability as it interconnects all the events to have replica of scene. ADFM works in linear fashion and expands collection phase with preparation steps. The preparation phase includes to provide training to individuals to how to collect and preserve evidences, how to insert communication shield across whole scene, enhancing technical skills to prepare documentation and making it admissible to law enforcement agencies. ADFM believes that physical and digital property should be returned to its true owner after investigations and makes it practically possible with its last phase named returning evidence. The ADFM constitutes nine phases as shown in following figure 3.

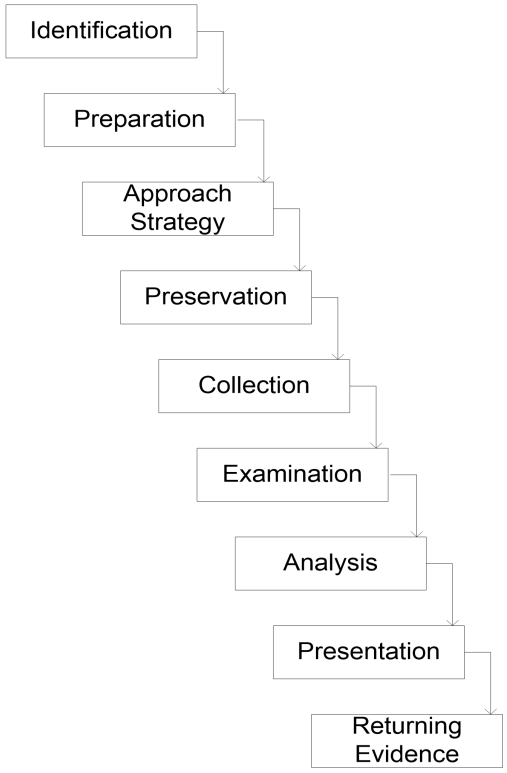

Fig. 1: ADFM Phases

III. DISCUSSON AND COMPARISION

All Digital evidences are essential to set accountability and accuse a person in court. Digital evidences become the key component for law enforcement agencies to resolve a case as these have revealing potential but at the same time these are fragile too and can be easily modified, tampered and ruined if not protected and handled properly. DFIM emphasize on preservation of integrity of evidences, ensures the authenticity of resources and validates methods and tools while collecting the evidences. Its authentication process makes it suitable for forensic as it does not contain false positive and false negatives. One of its most criticisms is lack of documentation phase that is essential part of digital forensic so it is often treated as incomplete model. The following table 1 shows the stepwise comparison of ADFM, FPM and DFIM.

TABLE I
INVESTIGATION PHASES IN ADFM, DFPM AND DFIM

Phases	ADFM	DFPM	DFIM
Collection	✓	✓	✓
Examination	✓	✓	✓
Analysis	✓	✓	✓
Reporting	✓	✓	
Preparation	✓		
Preservation	✓	✓	
Approach Strategy	✓		
Presentation	✓	✓	
Identification	✓	✓	✓
Return Evidence	✓		
Decision			
Review			
Reconstruction	✓		
Documentation			
Authorization	✓		✓
Survey			
Traceback		✓	
Testing			
Reconnaissance	✓		
Communication Shielding	✓		
Reconnaissance	✓		
Non-volatile evidence	✓		
Reconstruction	✓		
Testify	✓		

Return of Evidences	✓		

DFPM extended DFIM and added reporting phase to prepare complete documentation of investigation and also making its admissibility to court. The analysis phase causes confusion while deciding the coverage and scope of analysis as it is improperly defined and has ambiguity. DFPM treats analysis and interpretation phases similar and identical while both are completely distinct. DFIM and DFPM do not follow scientifically driven globally accepted standardized procedure so its investigation results become some less reliable and sometimes fails to convince court. ADFM follows standardized procedure and emphasizes on the need of preparation phase to decide which tools need to be utilized to investigate which resources by which individuals to assure the credibility of evidences. ADFM separates analysis phase from examination phase and believe in communication shielding to avoid disturbance in investigation scene. Its returning evidences phase assures that seized devices are returned to its legal owner once investigation gets complete.

IV. CONCLUSIONS

In this paper, the different phases of DFIM, DFPM and ADFM have been inspected to determine their suitability, operability and utility. All these models have been compared to know their efficiency and accurateness and found DFIM lacks the reporting steps thus it is not preferred to forensic digital devices as documentation is integral part of forensic procedure to assist court to know actually what happened and how it has taken place. DFPM is basically an extend version of DFIM that includes reporting phase to eliminate weakness in DFIM. As preparation phase checks the authenticity of evidences and validity of their sources and DFPM does not believe in preparation phase so sometimes DFPM investigate irrelevant devices to obtain evidences. ADFM extends DFPM with preparation phase and removes the ambiguity problem with DFPM. It facilitates the reconstruction of crime-scene that avoid the chances of evidence contaminated and get ruined as investigation is performed on replica not on original evidences.

REFERENCES

[1] Michael Kohn, JHP Eloff and MS Olivier, “Framework for a Digital Forensic Investigation”, Proceedings of the ISSA-2006 from Insight to Foresight Conference, Sandton, South Africa, July 2006

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

[3] Kruse II, Warren and Jay, G Heiser, Computer Forensic: Incident Response Essentials, Addison-Wesley

[4] A Report, “A Road Map for Digital Forensic Research”, The Digital Forensic Research Conference, USA, 2001.

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

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

[7] Warren G. Kruse and Jay G. Heiser, “Computer Forensics: Incident Response Essentials”, Wesley, 2002..

[8] 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

[9] 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

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

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

[12] Brian D. Carrier and Eugene H. Spafford, “An Event-Based Digital Forensic Investigation Framework”, Digital Investigation