Enhancing Cybercrime Investigation by Recommending an Extended Computer Forensic Framework

Neha Nihana Uliyam Moolayil[1], Mohammed Mujeebuddin[1] and Anjum Zameer Bhat[1#]

[1]Middle East College, Muscat, Oman
[#]Advisor

ABSTRACT

Over the previous years, technology has tremendously developed, having a huge impact on the nation by keeping it in line with the current trends and developments. While these developments have also impacted the nation in a positive ways, but negatives have also emerged. One of the well-known negative aspect of technology is cyber-crime. Cyber-crime has rapidly grown in recent years making the current computer forensic tools insufficient to investigate and analyze a cyber-crime within a time frame allowing the criminals to move freely in the society, resulting in unsolved and pending cases.

Computer Forensics is an important tool used in fighting cyber crime by providing set of rules and tools for examining and analyzing digital evidence. As the technology is increasing rapidly, with the number of devices used by a single person is increasing, this results in a challenging situation for forensics experts to analyze and process cyber crimes in an effective and efficient mode.

The Main purpose of this project is to recommend and a framework for investigation to enhance computer forensics. The project starts with discussing the recent cyber threats and attacks, while also focusing the need for cyber security. Also discussing the significance and importance of computer forensics with growing demand. Further, the recommended framework is compared with the current tools and techniques used for investigating a cyber-crime. A comparative study is done to prove that the proposed framework performs better than the existing techniques/models. The framework is employed & proved to be efficient in enhancing customizability, simplicity, and standards in collecting and organizing while conducting all stages of investigation by including preparation and review phases.

Introduction

Over the recent years, cyber security has drastically evolved with the increased amount of networks, devices and users. Cyber security is a concept that provides principles to defend devices and services of an organization or an individual from electronic attacks by spammers, hackers and cybercriminals in order to protect private and customer data against attackers. Organizations practice cyber security to defend its systems against phishing attacks, ransomware attacks, DoS attacks, data breaches and financial losses etc. (Kelley, 2022). Specifically, The DDoS attack remains one of the biggest concern for cybersecurity experts. This attack is used for preventing authorized users from gaining access to its services (Alatawi, 2021). The attacks utilize multiple hosts that are compromised for organizing attacks on target on a larger scale. It is a strong desire for cybersecurity experts to develop a strong defensive mechanism against existing and potential DDoS attacks (Alatawi, 2021). The universal use of network technologies and computers in all sectors of life has turned cyber security issue into a national security issue (Kemmerer, 2003).

As per (Kemmerer, 2003), In 2001 an internet worm cyber-attack named Nimda that had effects throughout the US within a time span of 1 hour attacking 86,000 systems. This event took place after a few days of 9/11. The occurrence of such attack raised consciousness on how systems are vulnerable to cyber-attacks. Similarly, A recent

analysis of the sapphire worm proved to be the fastest worm till date as it was able to attack systems worldwide within 10 minutes and was able to scan 55 million IP address per second and infecting approx. 75,000 users. These scenarios help in understanding the importance of cyber security in the 21st century (Kemmerer, 2003).

Based on the study conducted 2020, Cyber-attacks has been rated the fifth top risks in 2022 and will immensely increase till 2025. During the third quarter of 2022, the worldwide internet users experienced approximately 15 million data breaches, raising the percentage to 167 % compared to the previous quarter (Statista, 2022). As mentioned in the cybercrime magazine (Morgan, 2021), if the cybercrime industry would be measured as a country, with a total of $6 trillion USD it would be the worlds 3rd largest economy after US and China. It is expected that the global cybercrime could increase growth by 15 % every year, reaching $10.5 trillion USD annually by 2025 (Morgan, 2021). The cost evaluation of cyber crime includes destruction and damaging of data, money stolen, deletion of breached data and systems, theft of financial and personal data etc. (Morgan, 2021).

As the Cyber crime is a wide industry, the organizations invest and implement all means to protect and secure its network, data, and systems from getting breached/ attacked by the attackers. The organizations invest in various cyber security defense mechanisms which helps as a shield in guarding information, systems, and networks from cyber attacks by utilizing NDR (network detection and response), firewalls, EDR (endpoint detection and response) for identifying and analyzing while also reporting the incidents that occur inside the network (Welch, 2022).

As the amount, sophistication, severity, and rate of reported attacks is increasing. These attacks are sometimes not even detected therefore, it is very difficult to report them. The attackers are mostly able to hide their trails/path by accessing logging facilities, event logs by disabling or modifying them, so their activity goes unobserved (Kemmerer, 2003). Therefore, with the significant rise of technical cyber-crimes and unnoticed attackers, it is important to introduce computer forensics which helps in investigating and analyzing cyber-crimes using certain tools and techniques and collecting evidence to be presented in the court of law (Guo et al., 2011). Computer Forensics is a branch in cyber security where the attacks are investigated, and the culprits are prosecuted for the corresponding offenses.

Computer Forensics has become widely popular among the local and international law enforcement agencies and other government entities as it helps in securing the local cyberspace from attackers (Guo et al., 2011). It is currently practiced for judicial expertise in almost all enforcement activity.

There are various tools and techniques that are followed when investing, analyzing, recording and filing evidence of a cyber-crime. Some of them include Autopsy, FTK imager, volatility, registry recon, Cellebrite, Wireshark etc, also there are phases of computer forensics that include, identification → Collection → Preservation → Examination → Analysis → Presentation.

The existing investigation frameworks have strong hold on computer forensics as they provide high extent accuracy and strong evidence but lack standardization, customization and simplicity in conducting investigation requires long time span missing critical evidence and avoiding certain important steps in investigation.

Similar Work

While the suggested framework is among the first attempts at the development of investigation in computer forensic, efforts to enhance computer forensics investigation by automating evidence retrieval and identification by utilizing previous knowledge have been seen in this field.

This Section provides a brief summary of the research conducted on similar frameworks for investigation in computer forensics at different institutions and levels. This would provide a better understanding on framework suggested in this project.

A Case Based Reasoning Framework for Improving the Trustworthiness of Digital Forensic Investigations

A Study by the Department of Computing, Engineering and Information at Northumbria University, in United Kingdom, provided a framework to improve the trust of computer forensic investigation. (Horsman et al., 2012)

They have introduced a framework named CBR-FA (Case Based Reasoning Forensic Auditor) that helps in storing and reusing results from previous computer forensics examinations for auditing current computer forensics investigation. CBR-FA helps in providing a technique to evaluate digital forensics investigations with the purpose of providing the investigator with a level of reassurance and trust that the evidence related to the case is not missed.

The CBR-FA approach evaluates the Computer Forensic investigators investigation results. This audit would help the CF investigator to reassure that the findings of their investigation are consistent with the previous investigation results of a similar kind, which would result in the improvement of the level of trust associated with the investigation and provide reassurance to organization and the investigator.

Dialog: A Framework for Modeling, Analysis and Reuse of Digital Forensic Knowledge

In 2009, (Kahvedžić & Kechadi, 2009) at University College Dublin in Ireland developed a framework known as DIALOG (Digital Investigation Ontology) that reuses the knowledge of CF by using ontology structures.

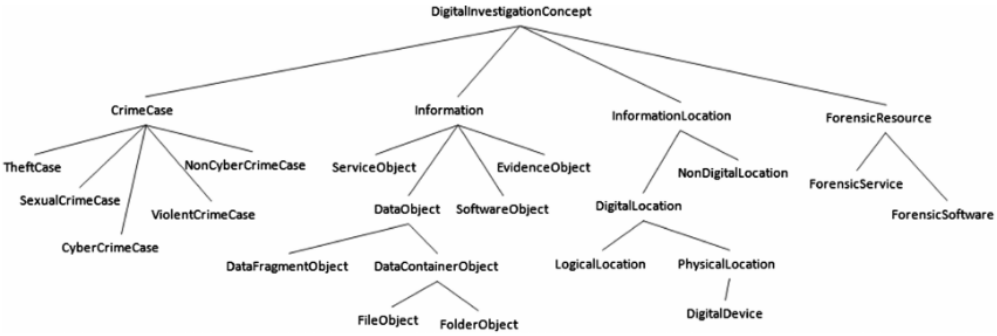

Figure 1. Digital Investigation Concepts

The developed framework DIALOG has the ability to compare registry structures and help in identifying missing registry keys and its usage. The Aim of this framework is to perform the analysis with the help of gathering and reusing data from the previous investigations conducted with the intention of automating registry analysis. As Shown in Fig.1, The DIALOG Framework enhances computer forensics through four main dimensions Crime Case, Evidence Location, Information and Forensic Resource. DIALOG plays a number of roles such as a knowledge repository, as a case manager, as an evidence unification mechanism, and as an investigation guide. (Kahvedžić & Kechadi, 2009)

Considerations Towards a Cyber-Crime Profiling System

In 2008, Similar Study was conducted at University of Pretoria, where the researchers provided a framework for an integrity-aware Forensic Evidence Management System (FEMS) (Arthur et al., 2008). This Framework provides investigators an automated analysis process with a holistic view of the forensic evidence at hand, thereby providing insights into the quality of investigative inferences.

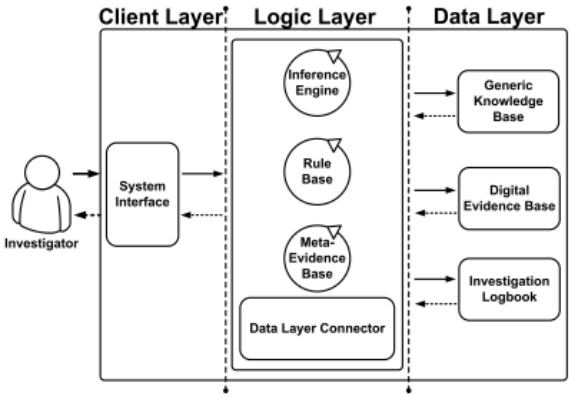

Figure 2. FEMS component-based architecture

The FEMS is designed using a component-based architecture as shown in Fig. 2. Specifically, the Data layer connector helps in providing the necessary abstraction between the investigator and raw evidence within the system. FEMS are detailed within the sub-sections such as, Client Layer Component, Logic Layer Components and Data Layer Component. (Arthur et al., 2008)

DFRWS Investigative Model

At the First Digital Forensic Research Workshop (DERWS) in 2001, they proposed a general digital forensic investigation process (Yusoff et al., 2011). The Model comprises of 6 phases that include

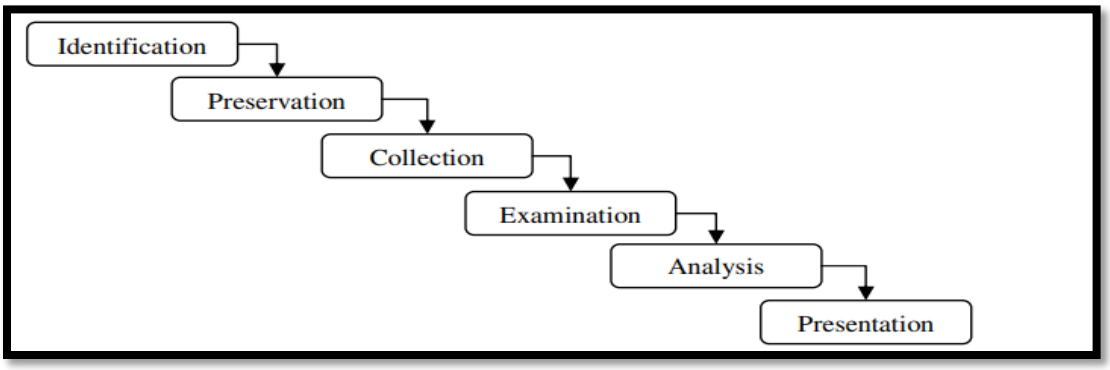

Figure 3. DFRWS Investigation Model

In the Identification phase, audit analysis, system monitoring and profile detection takes place which is then followed by preservation phase that involves tasks such as setting up a proper case management and to ensure a trustworthy chain of custody. As mentioned, this phase is critical as it helps in ensuring the collected data is free from contamination. In the collection phase, the data is collected based on the methods approved by using various recovery techniques. The Examination phase and Analysis Phase are considered crucial as it includes evidence recovery, validation, tracing of data that is encrypted. In the last phase of Presentation, the task related to documentation, expert testimony etc. is analyzed (Yusoff et al., 2011).

D4I - Digital Forensics Framework for Reviewing and Investigating Cyber Attacks

In 2020, a framework was proposed in computer forensics at the University of Macedonia, Greece. The computer forensics Framework was developed for reviewing and investigating cyber attacks known as D4I Framework . This framework helps in enhancing the examination and analysis phases. D4I is divided into two phases.

In the 1st Phase the framework proposed a digital artifacts categorization and mapping to the cyber-kill chain steps of attacks while in the 2nd phase it provided a detailed steps instructing the examination and analysis phases (Dimitriadis et al., 2020).

Literature Review

In this section certain literature linked with the objectives is summarized to briefly examine the most common cyber security threats and attacks and to understand the stages of computer forensics followed by the most common computer forensic tools of investigation. Also the loopholes in computer forensics would be identified from different literatures.

A Survey of Emerging Threats in Cybersecurity

A study conducted at IRO ICT Centre in Australia describes the emergence and exponential growth of cyber attacks resulting in unsafe and critical consequences (Jang-Jaccard & Nepal, 2014). It emphasis on the malware attack which among the common choice of weapon used by attackers. The Article presents a brief discussion of the most exploited vulnerabilities in the existing network layers, software layers, hardware layer. They have also mentioned current mitigation techniques that are used in minimizing the possibility of an attack. Several new attack patterns in emerging technologies were also discussed. The types of malwares such as Trojans, Virus, Worms, Rougueware etc. were defined following the mediums though which they are spread. The article clearly helped in understanding the most common attacks on hardware, software and network and provided certain countermeasures (Jang-Jaccard & Nepal, 2014).

	Hardware	Software	Network
Common attacks	• Hardware Trojan • Illegal clones • Side channel attacks (i.e. snooping hardware signals)	• Software programming bugs (e.g. memory management, user input validation, race conditions, user access privileges, etc.) • Software design bugs • Deployment errors	• Networking protocol attacks • Network monitoring and sniffing
Examples of countermeasures	• Tamper-Resistant Hardware (e.g. TPM) • Trusted Computing Base (TCB) • Hardware watermarking • Hardware obfuscation	• Secure coding practice (e.g. type checking, runtime error, program transformation, etc.) • Code obfuscation • Secure design and development • Formal methods	• Firewall • Intrusion prevention and detection • Virtual Private Network (VPN) • Encryption

Figure 4. Common attacks and countermeasures

Cyber-attacks keep increasing with new approaches and new technologies. Based on the article, mostly the attackers tend to modify the existing malware signatures for exploiting the flaws that exist in the new technologies such as social media, cloud computing, smartphones critical infrastructure etc, (Jang-Jaccard & Nepal, 2014). In other cases the attacker try to find loopholes in the technologies in order to inject malware. As these new technologies have billions of users the hackers take advantage of this by reaching out to vast number of victims quickly and efficiently (Jang-Jaccard & Nepal, 2014).

Recent Cyber Security Attacks and Their Mitigation Approaches – An Overview

Based the research performed at Federation university, Australia, the Author explains how people, organizations and governments across the globe are facing challenges by losing their information and money due to cyber-attacks (Chowdhury, 2016). The article provides a deeper understanding on the recent cyber security stacks and the economic downfall as a result of growing cyber-attacks. The Article helps to analyze the increase in exploitation of a system that resulted in creating more opportunities for current cyber crimes to take place. The Fig shows the percentage of attacks that took place in May 2016,

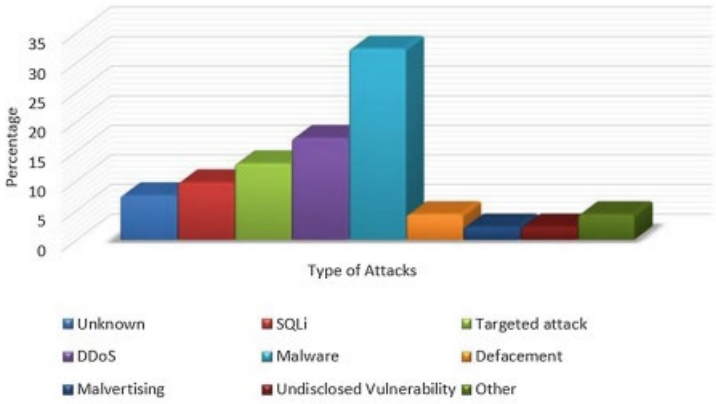

Figure 5. Recent cyber security attacks

The Article described each of the attacks with respect to the countermeasures and also described them under four categories that include cyber terrorism, cyber vandalism, cyber war and cyber espionage. The article further mentions the impact of cyber attacks caused countries such as USA with half of the population been a victim, China with 41% of the hacking traffic followed by turkey, Russia, brazil, india and other countries. A report in 2014 June, shows the cost of 400 billion dollars in economy through cybercrimes which is expected to become a trillion-dollar industry.

Cyberattacks: Why, What, Who, and How?

Cybersecurity is becoming even more critical day by day for individuals and organizations as it affects the continuous business operations. In this article Liu and Cheng provided a better understanding on cyberattacks by listing Why, What, Who and How (Liu & Cheng, 2009). They have analyzed the challenges associated to cybersecurity while considering the current attack patterns and trends.

The Article helps in highlighting the initial cause of cybersecurity problems where the bugs in the software, defects in configuration and flaws in design can lead to vulnerabilities that could result in exploitation and breach of system. As shown in the fig below.

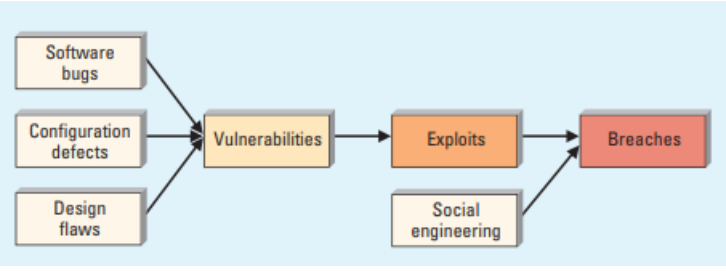

Figure 6. Steps followed for conducting cyber attacks

Further the article defines vulnerabilities, Breaches, Social engineering and exploitation while also analyzing them. The Article mentions how the attackers tend to rely more on their own creativity rather than using tools and techniques for launching an attack (Liu & Cheng, 2009). It describes the basic steps that an attacker follows to launch an attack these include conducting reconnaissance, scanning targets, exploiting systems establishing footholds and profit. By the end, the article mentions certain upcoming trends such as Automation and sophistication of tools, smaller vulnerability remediation window, increasing asymmetric threats, decreased response and recovery time etc (Liu & Cheng, 2009).

Cyber Security Attack Prediction: A Deep Learning Approach

These days cyber-attacks are increasing at a higher pace making it difficult and insufficient for existing detection mechanism to prevent cyber-crimes (Ben Fredj et al., 2020). There is a necessity of designing and implementing enhanced detection systems in order to reduce crime and cope up with the newer technologies. The recent approaches using machine learning became attractive in the industry as it is capable of detecting and preventing crimes using certain algorithms (Ben Fredj et al., 2020). This study proposed a newer models such as MLP (multilayer Perception), RNN (Recurrent Neutral Network) and LSTM (Long Short term memory) that will help in predicting the type of attack that is possible going to happen. The Article helps in understanding different cyber attack prediction methods and the models and tools used in enhancing them (Ben Fredj et al., 2020).

Foundations of Computer Forensics: A Technology for The Fight Against Computer Crime

The study conducted in USA and published in the computer law and security report of the evolution of computer forensics (Wang et al., 2005). It describes computer forensics as rapidly growing disciple that has roots in forensic science, information security and computer security technology which aims to acquire electronic evidence from computer systems for prosecuting cyber criminals. The article describes the emergence and growth of computer forensics and its importance of presenting electronic evidence in the courts. The Article further defines the processes and procedures that take place when an computer forensic investigation is done. The steps include securing the suspected system, securing potential evidence, collection of evidence, analyze the evidence and the last step is to prepare the evidence (Wang et al., 2005). The Article provided a clear understanding about the software and tools used for conducting investigation and preserving evidence (Wang et al., 2005). The article also explains how the EUCTOSE project provides a intelligent solution for ensuring that the evidence is reliable and legally obtained. EUCTOSE is an expert-based cybercrime advisory tool which can help in informing investigators on the appropriate procedures that needs to be followed on every step of investigation (Wang et al., 2005)

Cyber Forensics Tools: A Review on Mechanism and Emerging Challenges

The research conducted at Sri Lanka Institute of Information Technology in 2021 describes Computer forensics as the science that determines the evidential value of a crime scene and related evidence that could be utilized for assigning appropriate penalties to individuals that have committed the crime (Fernando, 2021). The Article provides in-depth knowledge on computer forensic science and tools used for investigation. Computer forensics tools are designed and aligned for a specific task or as a suite that is capable of handling many forensic operations inline with corresponding digital frameworks (Fernando, 2021).

The Article mentions certain drawbacks of computer forensic tools such as lack of accuracy, data extraction capacity, responsiveness encryption and compatibility issues with system. The Article Further briefed each forensic tools (Computer forensic, Network forensic, Mobile forensic, Database forensic) that include EnCase, Autopsy, FTK,

Volatility, Mail Viewer, Wireshark, XRY etc. By the end the article discussed challenges of using these tools in each forensic sector (Fernando, 2021).

Research On Some Relevant Problems in Computer Forensics

Based on the study, the article analyzes computer forensics and the relevant problems such as legal aspects, technology etc. (Wang & Lee, 2013). This article was chosen to understand the loop holes of computer forensics and the ways to combat them. The Article describes the rapid development of information technology and the increase of users over the internet. This Research provided in depth analysis and exploration of criminal activities in communication networks on the basis of forensic tools (Wang & Lee, 2013).

The Article helps in understanding the legal issues of computer forensics where by it mentions the importance of presenting reliable and accurate information in the courts. As the Data on the computer can be tampered or deleted therefore it needs to be stored and secured so that its integrity and credibility remains valid. The article explained the process of investigation performed in computer forensics. Further the article provided a discussion on the computer forensic models (Wang & Lee, 2013).

A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions

The Study conducted in this article covers all aspects of computer forensics including the steps of investigation, tools used for investigation, techniques and challenges of computer forensics. The Article discussed the Steps of computer forensic that include,

Figure 7. Common Computer forensic Investigation Model

The article divided computer forensic into sevral domains such as Operating System forensics, Disk and file System Forensics, Live Memory Forensics Web Forensics, Email Forensics, Network Forensics, Multimedia Forensics and Others (Javed et al., 2022). It described each of them in detail to provide better understanding.

	Autopsy	Redline	BEC	OSF	PD	XWays	Encase	FTK	MA
License	Open	Freeware	Proprietary	Proprietary	Open	Proprietary	Proprietary	Open	Proprietary
Platform	Window, Linux, OS X	Window (XP- 2008)	Window (all), Android Mac OS, Linux	Window Vista, 7, 8, 10 Server (2000, 2003, 2008, 2012	Window 2000/ 2003/ 2008/XP/ Vista/ Window7, Linux.	Window (all) DOS	Window, MAC, Linux, DOS, Machine	Windows, XP/Vista /7/8/10	Computer, Mobile, Cloud
Supported Image File Formats	Raw Single, Raw Split EnCase	Raw, .mans file	Atola, Raw , DMG, EnCase, FTK, AFF X-Ways CTR, SMART	Raw, Split, A. F. S, Virtual, EnCase, SMART (.S01), VHD (.VHD)	Raw, EnCase, A. F. S	Raw Encase V. I	Raw, VMware, EnCase, Safeback.	Raw, SMART, EnCase, Snapback, Safe back	Raw

Figure 8. Computer Forensic Tools and supported image formats

Further the Article mentioned several tools that are used in forensic investigation such as Autopsy, Redline, EnCase, FTK, XWays Forensics. The Article provided a comparative study on the features of different computer forensic tools as mentioned in Fig. (Javed et al., 2022)

Also, the Article Provided the direction for future research that included generation of structured data, advanced forensic tools, AI and digital forensics etc. Also the challenges such as Technological, legal and resource were discussed and detailed (Javed et al., 2022).

Comparative Study

A Comparative Study was performed between different computer forensic frameworks to identify the limitations and loopholes of the existing frameworks and to design a framework that is capable of overcoming the limitations.

Table 1. Comparative study between different computer forensic frameworks

Aspects / Framework	Standard	Accurate	Customizable	Reliable	Simplicity
D4I (Defense Digital Forensic Framework Integration)	✓	✓	✗	✓	✗
DFRWS (Digital Forensic Research Workshop)	✗	✓	✓	✓	✗
DIALOG (Digital Investigation Analysis and Logging Framework)	✓	✓	✗	✓	✓
CBR-FA (Cognitive-Based Framework for Forensic Analysis)	✓	✓	✗	✓	✗
Recommended Extended Computer Forensic Framework	✓	✓	✓	✓	✓

Based on the study conducted, D4I Framework limits customizability and similarity while performing investigation but performs accurate and reliable investigation. DFRWS Framework does not entertain standardized investigation which is an important aspects that needs consideration. Also simplicity of investigation needs enhancement. The DIALOG Framework follows a standard approach making it accurate and reliable but lacking customizability and simplicity while performing investigations. The CBR-FA Framework also limits customizability and simplicity while performing investigations. The Recommendation Computer forensic will enhance the discussed limitations by introducing 2 phases that is preparation and review phase that will focus on enhancing standardization, customizability and simplicity during investigations.

Design

Theoretical Workflow Framework Diagram

The Theoretical workflow diagram for computer forensics framework serves as a visual depiction of the procedures and actions required in carrying out a computer forensic investigation. The illustration can aid in directing investigators through the different phases of the examination and ensuring that all pertinent data is gathered and examined in a systematic and comprehensive way. The Key steps including evidence identification, preservation, analysis, and presentation are included in process diagrams. Within each stage, it could additionally contain supporting activities including data collection, storage media picture creation, keyword searches, and metadata analysis.

Through a Standard workflow design, Investigators may make sure they are gathering and evaluating evidence in a consistent and trustworthy manner without missing crucial steps by adhering to a structured process, which is critical when presenting results in court.

THEORATICAL WORKFLOW FRAMEWORK DIAGRAM

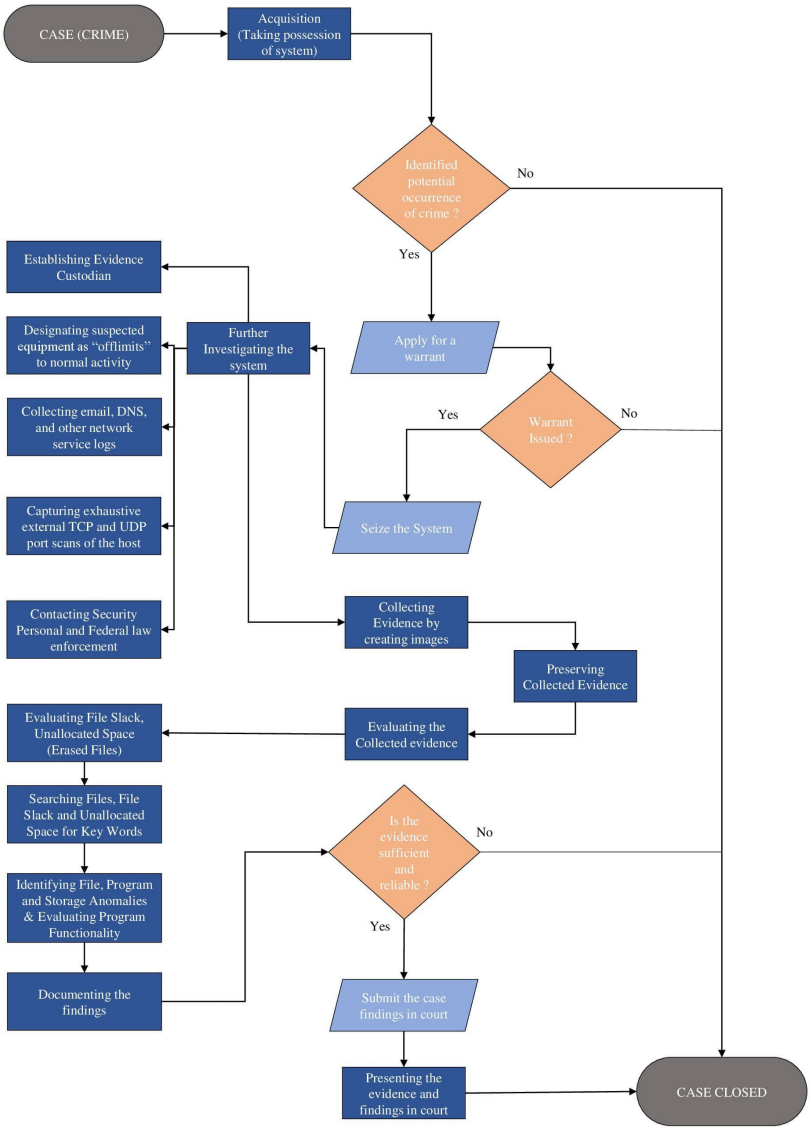

Figure 9. Theoretical Computer forensic workflow Diagram

In Figure 9, A Crime has been identified and a Case is opened. The initial step of computer forensics is to take possession of the system (Acquisition). An exact copy of the original evidence is created that would be analyzed without altering or damaging the original data. If the forensic officer identifies a potential occurrence of crime, a warrant is requested or else the case is dismissed. Once the Court issues a warrant further investigations are conducted. The further investigation are initiated by establishing evidence custodian, designating suspected equipment, collecting email, DNS and other network service logs, Capturing exhaustive external TCP and UDP port scans of the host & involving security personal and federal law enforcement. Once the evidence is collected by capturing images, the next step the forensic officer needs to take is to preserve the collected evidence in a form that the evidence is secured and cannot be altered or damaged.

The forensic officer further evaluates the collected evidence by evaluating File Slacks, Unallocated Space or Erased files, Searching the files for key words, Identifying File, Program and Storage Anomalies & Evaluating Program Functionality and finally documenting the findings from the investigation conducted. The Forensic officer reviews the evidence and decides if the evidence is sufficient and reliable, if the officer is satisfied with the investigation conducted and the findings documented, then the case files are submitted to the court of law. During the proceedings, the officer is required to present the reliable evidence in court, and it is up to the court to provide the judgment and finally the case is closed.

Standard Enhanced Framework Design

Based on the Understanding of the limitations and drawbacks of current computer forensic framework a suitable an enhanced framework was designed to suite the growing trends in computer forensics. Standardization, Customizability & Simplicity are the main aspects that are focused on the enhanced computer forensic framework.

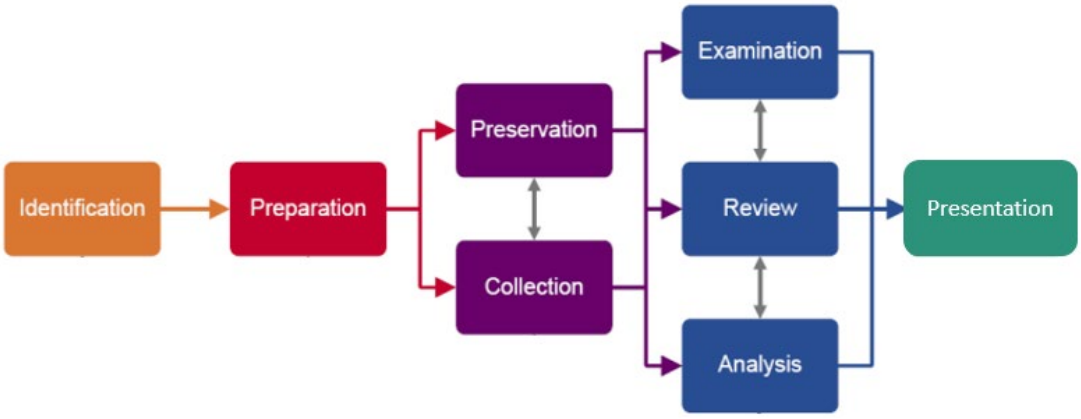

Figure 10. Proposed Standard Enhanced Computer Forensic Framework Design

Based on the Study, most of the computer forensics frameworks include phases such as identification, preservation, collection, examination, analysis and presentation while ignoring the two important phases that includes Preparation and Review. The Aim of this Proposed Enhanced Computer forensic Framework is to over come the limitations faced by previous frameworks with respect to Standardization, Customizability & Simplicity and to incorporate the existing frameworks to compile a reasonably complete model.

In the Proposed Framework, Identification is the first phase. The initial client encounter, where the investigator learns about the case and the goals of the inquiry, marks the beginning of the identification phase. The investigator further performs a preliminary analysis of the system or equipment in issue to find possible evidence sources. To ascertain the extent and complexity of the investigation, the identification phase could involve carrying out witness interviews, examining the relevant material, and undertaking a risk assessment.

Further, For an inquiry to be effective, the Preparation phase is essential. In this phase, the investigation's objectives and scope are specified, its resources and limitations are noted, and an investigation plan is created. The investigator may need to create rules for handling sensitive or secret material as well as identify any legal or ethical problems.

The Preservation phase involves taking precautions to prevent the prospective evidence from being altered or damaged. To avoid remote access, the investigator may protect the system or device by creating a forensic image of the

storage medium and isolating the system from the network. In order to maintain track of the transportation of the evidence, chain of custody documentation is established in this phase.

In the Collection phase, the possible evidence must be obtained in a legally acceptable approach. Data collection methods that the investigator may employ could include live analysis, transferring data to an external device, and network forensic analysis. The integrity of the gathered data is checked, and the chain of custody records are updated.

In order to establish the facts of the case and discover relevant details, the gathered evidence is analyzed during the examination phase. The investigator may employ a range of methods and devices, including timeline analysis, keyword searches, and file carving. During investigation, hidden or deleted data may be discovered and analyzed, along with file attributes and metadata.

In the Review phase, the accuracy and reliability of the investigation is evaluated. The investigator has the responsibility to examine every step of the investigation, including the techniques employed, the information gathered, and the analyses that were conducted. The objective of this phase is to find any mistakes, contradictions, or omissions in the investigation so that, if needed, remedial action could be taken. Documenting the procedure for investigating and creating a final report may also be part of the review phase.

The findings from the examination phase are considered during the analysis phase. To derive meaning from the facts and create a theory of the situation, the investigator may employ deductive and inductive reasoning. The phase of analysis may include finding patterns, connections, and abnormalities in the data.

The Presentation phase involves notifying the parties of the investigation's findings and conclusions. For use in court, the investigator may produce reports, exhibits, or testimony. Working with other experts, such as attorneys or law enforcement, to build a plan for utilizing the evidence in the legal system may also be part of the presenting phase.

Discussion

Benefits and Need for Preparation and Review Phase for Enhancing Computer Forensic Framework

The Introduced phases which include the preparation and review phase are critical in enhancing standardization, customizability, and simplicity of the framework in computer forensic investigation.

The investigator might set up standard operating procedures and guidelines for the investigation at the preparation phase. This can guarantee that the investigation is carried out in a repeatable and consistent manner, lowering the possibility of mistakes and inconsistencies. The investigation may also be made to fit a specific need by the investigator, who can then identify those needs and adjust their strategy allowing the Framework to be customizable. The investigation can be made easier and more productive by making sure that all required equipment and resources are readily hand.

The investigator can assess the efficiency of the investigation structure employed throughout the review phase. This assessment can help identify any areas where the investigation might require enhancement, which will eventually contribute to the framework's improvement and standardization. By identifying distinctive case requirements that might have been ignored during the preparation phase, customization can also be improved.

Additionally, by identifying aspects of the framework that are unnecessarily difficult or time-consuming, the review phase might make it simpler. Investigators may save time and money by simplifying the investigation process, which also makes it easier to use the framework.

As a result, both the preparation and review phases are crucial for improving the framework's standardization, customizability, and simplicity in computer forensic investigation. Investigators can ensure that the framework is successful, efficient, and adaptable to a variety of different scenarios by developing explicit processes and protocols and reviewing the results of the investigation.

Conclusion

An enhanced computer forensic framework is necessary for carrying out exhaustive and efficient inquiries that are precise, reliable, and transparent. A tailored and improved computer forensic framework may be created by identifying and fixing the shortcomings of the current frameworks, such as D4I, DFRWS, DIALOG, and CBR-FA. To guarantee that investigations are successful, efficient, and ethical, this framework should prioritize customization, training, standard operating procedures, and ongoing development. By using this framework, digital forensic analysts may carry out investigations that adhere to their individual needs and guarantee the accuracy, dependability, and transparency of their findings. Additionally, the improved and customized framework can aid in addressing the difficulties brought on by the constantly changing digital environment and the growing complexity of digital forensic investigations. In summary, it is essential for the functioning of justice and the public's protection that an improved computer forensic framework be developed and put into practice in order to guarantee integrity and reliability of digital forensic investigations.

References

Kelley, K. (2022) What is Cybersecurity & Importance of Cyber Security, Simplilearn. https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security#:~:text=Cybersecurity%20is%20crucial%20because%20it,information%20systems%20are%20all%20included.

Kemmerer, R. A. (2003). Cybersecurity. *25th International Conference on Software Engineering, 2003. Proceedings.* https://doi.org/10.1109/icse.2003.1201257

Alatawi, F. (2021). Defense mechanisms against distributed denial of service attacks: Comparative review. *Journal of Information Security and Cybercrimes Research*, *4*(1), 81–94. https://doi.org/10.26735/lqez4186

Statista. (2022). *Data Records breached worldwide 2022*. https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/#:~:text=During%20the%20third%20quarter%20of,2020%2C%20nearly%20125%20million%20cases.

Morgan, S. (2021). *Cybercrime to cost the world $10.5 trillion annually by 2025.* Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Welch, B. (2022). *Cyber defense.* Cyber Defense. https://www.ironnet.com/topics/what-is-cyber-defense

Guo, H., Jin, B., & Huang, D. (2011). Research and review on Computer Forensics. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 224–233. https://doi.org/10.1007/978-3-642-23602-0_21

Horsman, G., Laing, C., & Vickers, P. (2012). A Case based reasoning framework for improving the trustworthiness of Digital Forensic Investigations. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 682–689. https://www.researchgate.net/publication/236268819_A_Case_Based_Reasoning_Framework_for_Improving_the_Trustworthiness_of_Digital_Forensic_Investigations

Kahvedžić, D., & Kechadi, T. (2009). Dialog: A framework for modeling, analysis and reuse of Digital Forensic Knowledge. Digital Investigation, 6. https://www.researchgate.net/publication/222657206_DIALOG_A_framework_for_modeling_analysis_and_reuse_of_digital_forensic_knowledge

Arthur, K. K., Olivier, M. S., Venter, H. S., & Eloff, J. H. P. (2008). Considerations towards a cyber crime profiling system. *2008 Third International Conference on Availability, Reliability and Security*. https://ieeexplore.ieee.org/document/4529507

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, 3(3), 17–31. https://airccse.org/journal/jcsit/0611csit02.pdf

Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - digital forensics framework for reviewing and investigating cyber attacks. *Elsevier*, 5. https://doi.org/10.1016/j.array.2019.100015

Jang-Jaccard, J., & Nepal, S. (2014). A Survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973–993. https://www.sciencedirect.com/science/article/pii/S0022000014000178?via%3Dihub

Chowdhury, A. (2016). Recent cyber security attacks and their mitigation approaches – an overview. *Applications and Techniques in Information Security*, 54–65. https://doi.org/10.1007/978-981-10-2741-3_5

Liu, S., & Cheng, B. (2009). Cyberattacks: Why, what, who, and how. *IT Professional*, 11(3), 14–21. https://doi.org/10.1109/mitp.2009.46

Ben Fredj, O., Mihoub, A., Krichen, M., Cheikhrouhou, O., & Derhab, A. (2020). Cybersecurity attack prediction: A deep learning approach. *13th International Conference on Security of Information and Networks*. https://doi.org/10.1145/3433174.3433614

Wang, Y., Cannady, J., & Rosenbluth, J. (2005). Foundations of Computer Forensics: A technology for the fight against computer crime. *Computer Law & Security Review*, *21*(2), 119–127. https://doi.org/10.1016/j.clsr.2005.02.007

Fernando, V. (2021). Cyber forensics tools: A review on mechanism and emerging challenges. *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. https://doi.org/10.1109/ntms49979.2021.9432641

Wang, Y., & Lee, H. C. (2013). Research on some relevant problems in computer forensics. *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)*. https://doi.org/10.2991/iccsee.2013.393

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access*, *10*, 11065–11089. https://doi.org/10.1109/access.2022.3142508