Summer 2023

Unveiling the Digital Shadows: Cybersecurity and the Art of Digital Forensics

Derek Beardall
Boise State University

Unveiling the Digital Shadows: Cybersecurity and the Art of Digital Forensics

by

Derek Beardall

A project completed in fulfillment

of the CORe 591 requirements for the degree of

Master of Science in Cyber Operations and Resilience

Boise State University

August 2023

Abstract— **This paper navigates the symbiotic relationship between cybersecurity and digital forensics, exploring the profound role of digital forensic methodologies in addressing cyber incidents. Beginning with foundational definitions and historical evolution, this study delves into diverse types of methodologies and their applications across law enforcement and cybersecurity domains. The mechanics of cyber incident response illuminates the strategic orchestration of digital forensic methodologies. Amidst triumphs, challenges emerge from the shadows: swift threat evolution, digital ecosystem complexity, standardization gaps, resource limitations, and legal intricacies. Best practices guide experts through this intricate terrain, culminating in an enhanced understanding of the inseparable bond between cybersecurity and digital forensics. Through this synthesis, cyber threats' shadows are unveiled and mitigated, fortifying the digital landscape.**

Keywords— Cybersecurity, Digital Forensics, Cyber Incident Response, Methodologies, Challenges.

I. Introduction

Since the advent of the internet, innovation, and collaboration have been the new frontier. In the internet's adolescence, systems were constructed with availability and integrity in mind, not security. As advanced technology entered the scene, it played a vital role in facilitating many advancements in a multitude of fields including medicine, health, and employment. However, the lack of integrated security measures has been a catalyst for exploitation by people with malicious intent.

In an era characterized by the unprecedented reliance on digital connectivity, cybercrimes and advanced persistent threats have been on the rise, requiring the domains of cybersecurity, law enforcement, and legal proceedings to undergo reforming shifts toward digital forensics, and the preservation of digital evidence. The pervasive integration of digital systems in everyday activities has presented both opportunities and challenges for the field of digital forensics. As the need to investigate cybercrimes and secure digital evidence escalates, two distinct yet interconnected branches of digital forensics have emerged: digital forensics for criminal prosecution and computer forensics for cybersecurity.

This paper investigates the differences and similarities between digital forensics for criminal prosecution and Digital Forensics Incidents Response (DFIR). Additionally, this paper aims to identify the challenges of digital forensics in incident response and suggest best practices for forward improvement.

A. History of Digital Forensics

Digital forensics has endured an evolutionary change since the inception of computers, despite the establishment of modern era forensic investigative practices occurring gradually. From the 1960s to the 1970s, mainframe computers became more prevalent. It was during this time that government agencies acknowledged the computers' potential as a tool for criminal activities [1].

During the transformative era from the 1980s to the 1990s, the field of digital forensics observed substantial historical landmarks. The debut of the personal computer (PC) played a pivotal role that ignited a widespread fascination with computer systems and networking, thus creating new possibilities and avenues for people to explore [1]. This exploration led to the utilization of computers as criminal instruments and devices to store data related to criminal enterprises. Law enforcement agencies, government entities, and corporations embarked on a journey of collaboration for data retrieval and comprehension, which harnessed the potential of digital forensics, effectively laying the foundation for the field's subsequent evolution.

In 1984, The Federal Bureau of Investigation (FBI) established the National Center for the Analysis of Violent Crime (NCAVC) in Quantico, Virginia. The program's primary goal was to use behavioral science methodologies with advanced computer systems, offering vital support to state and local law enforcement agencies engaged in the investigation of violent crimes [2]. During the latter part of the 1980s, the High Technology Crime Investigation Association (HTCIA) was developed and played a significant role in providing training and resources for law enforcement technological investigations [3]. Recognition of the growing importance of digital evidence led to the inauguration of the FBI's Computer Analysis and Response Team (CART) in 1991. CART's sole purpose was to provide timely and accurate examinations of computers for criminal prosecution [2].

By the early 1990s, staggering statistics emerged, linking criminals to the employment of computers as instruments of criminal enterprises. By 1988, 4.7 million personal computers were sold in the United States. In 1990, it was recorded that at least 400 connected networks existed nationally and internationally. Five-hundred million in revenue was lost annually through illegal use of telephone access codes, one trillion in revenue was electronically moved every week, and only 11% of computer crimes were being reported [4]. These statistics presented an urgent call to action that highlighted the dire need to elevate the standards of digital forensics to confront the escalating scope of unmitigated cybercrime.

Since the establishment of the Computer Analysis and Response Team (CART), noteworthy milestones have shaped what is now known as digital forensics. The following events resulted in key advancements in digital forensics:

- 1998: U.S. Digital Millennium Copyright Act (DMCA) [5]. The DMCA introduced critical copyright protections and restraints on digital content, ushering in protocols for managing intellectual property.
- 1999: National Institute of Standards and Technology (NIST) initiated the CFTT Project. The Computer Forensic Tool Testing (CFTT) project developed guidelines and methodologies for evaluating digital forensic tools, leading to standardization [6].
- 2001: USA Patriot Act and Expandable Law Enforcement Powers [7]. In response to the September 11 attacks expanded the powers of law enforcement agencies to investigate and prevent terrorism. The expansion allowed for broader data collection and surveillance methods.
- 2002: International Cybercrime Treaty [8] The treaty fostered international cooperation in combating

cybercrime and defining the legal framework for digital evidence collection and exchange.

- 2006: U.S. Federal Rules of Civil Procedure (FRCP) Amendments [9]. FRCP addressed electronic discovery in civil cases that established guidelines for handling digital evidence in court proceedings.
- 2013: U.S. President, Barack Obama Cybersecurity Executive Order [10]. This executive order pushed for standardization in cybersecurity with cybersecurity for improving Critical Infrastructures.
- 2014: Cybersecurity Enhancement Act [11] and NIST Cybersecurity Framework [12]. Two pivotal milestones occurred in 2014 to include (1) the Cybersecurity Enhancement Act that strengthened cybersecurity research and development to include related technology in digital forensics, and (2) The NIST cybersecurity framework that provided guidelines for managing and securing digital information and evidence.
- 2021: U.S. Executive Order on Cybersecurity [13]. This order outlined measures to enhance cybersecurity across government agencies.

These milestones provide a glimpse into the dynamic evolution of digital forensics. While not exhaustive, they exemplify the convergence of technological advancements, evolving legal frameworks, and the mounting significance of cybersecurity and digital forensics in modern society.

B. Digital Forensics

Digital Forensics encompasses the meticulous process of identification, preservation, collection, examination, analysis, documentation, and presentation of computer systems, mobile devices, and network devices. It is often employed to facilitate inquiries conducted within organizations and regulatory bodies, criminal behavior, criminal prosecution, and an assortment of investigative proceedings. The progression of challenges arising from digital connectivity caused a convergence in the field of digital forensics and cybersecurity. This convergence is noticeable when examining the two distinct, yet interconnected fields: digital forensics for criminal prosecution and Digital Forensics Incident Response (DFIR).

C. Illicit Utilization of Digital Evidence for Unlawful Purposes

A digital device or system can include but not be limited to desktop computers, laptop computers, tablets, peripherals, servers, mobile telephones, smart phones, smart watched, and any storage devices. Devices can serve as (1) a focal point for criminal activities, (2) tools involved in criminal acts, and (3) repositories containing evidence that documents the criminal act(s) [14].

A device can be used as a focal point for criminal activity, encompassing offenses like child exploitation, corporate espionage, cyber terrorism, identity theft, internet fraud, intrusion, and phishing [15].

Devices used as instruments in criminal endeavors are common in activities like child exploitation, child solicitation, corporate espionage, counterfeiting, credit card fraud, cyber terrorism, identity theft, internet fraud, intrusion (hacking), social engineering, and theft of intellectual property [15].

Furthermore, repositories of evidence that support criminal cases include instances such as fraud and embezzlement, child sexual abuse material, child solicitation, narcotics trafficking, intrusion, or hacking storage platforms for tools and programs, e-mail, or chat with accomplices in traditional crimes such as homicide, robbery, or burglary [15].

Repositories of data are a treasure trove for digital evidence. There are two types of evidence pertaining to devices: universal and case specific [15].

Universal evidence is a type of application that saves data through everyday use. This includes chat logs, emails, financial records/programs, photographs, and movies, saved documents, registry information, and internet browsing to include favorites/bookmarks, temporary files, history, and active logs.

Crime specific pertains to internet crimes, and investigations that may be centered around child exploitation or child sexual abuse material, financial fraud, or counterfeiting, as well as cyber terrorism or network intrusion. When pertaining to child exploitation or child sexual abuse material, an investigator will examine different artifacts that will eventually prove a suspect's intent, motive, and digital footprint.

In the crime of financial fraud/counterfeiting, investigators will examine template graphics for false IDs, financial records, photo editing software, digital photos and false IDs, customer databases, credit card numbers, and check-making software.

In the crime of cyber terrorism or network intrusion, investigators examine internet protocols (IP) addresses and connection logs, proprietary programs, source code, system configuration logs, internet links or programs that make the user anonymous, and encryption software.

Repository data for crimes that relate to digital connectivity as well as a physical presence include homicides, identity theft, and narcotics investigations.

In a homicide investigation, digital forensic examiners inspect digital artifacts, intent, and motives related to the evidence found on the physical crime scene. Examiners will also collect artifacts pertaining to the suspects' daily activities that could aid in prosecution.

In an identity theft crime, investigators are interested in backdrops, scanners and software, stolen mail, and ID templates and blank IDs.

D. Digital Forensic Methodologies

To comprehend the significance of digital forensics in incident response, it is essential to understand its methodologies. The multitude of crimes, criminal tactics, and the sheer amount of data that can prove these crimes occurred demonstrate how digital forensic examiners must be highly specialized technicians with investigative experience. Hence, digital forensics involves the integration of scientific principles and legal processes. Adherence to specific methodologies and

techniques are essential for discovery in a legal context. In cases where legal prosecution is not the primary objective (i.e., a corporate security breach), the possibility of future legal proceedings may emerge. Therefore, it is vital to manage all prospective digital evidence with forensic thoroughness for the effective presentation in a legal framework.

Digital forensic methodologies follow a scientific workflow for investigations that include several consecutive progressive steps. Step one: the preservation of evidence, step two: pre-examination, step three: catalog, step four: search, find, and extract (SFE), step five: post-examination verification, and step six: package, review, and distribute results.

During the preliminary investigation, it is vital to protect and preserve the device that could contain digital evidence. Preserving evidence includes (1) the proper identification of common devices: computers, cell phones, cameras, optical media, etc., (2) identifying obscured devices: non-traditional devices such as printers with smart technology, digital video recorders (DVR), answering machines, GPS receivers, gaming consoles, and digital voice recorders, (3) protected devices: biometric and mechanically protected devices such as access cards and dongles, (4) concealed devices: devices disguised as other items such as computers disguised as boxes or bottles and embedded USB devices within watches, pens, earrings, credit cards, and toys.

After the device has been identified, the preservation process continues with the proper handling of the evidence to preserve the data contained within. This idea can include maintaining power or shutting it off in a certain fashion, packaging the device with caution since evidence is volatile data, and proper documentation to include the chain of custody.

The device continues to be preserved through the beginning stages of the digital forensic examiner's investigation. As previously stated, data on devices are volatile and altering or causing any damage to the original evidence could have costly results in an investigation. Forensic examiners will preserve the evidence via forensically preparing media (completely wiped media), write blocking the device to ensure no inputs can change the data, and completing pre-examination verifications. A pre-examination verification is performed through hash-based verification. Hashes, also referred to as digital fingerprints, are outcomes generated by cryptographic algorithms crafted to create a sequence of characters [16]. After the pre-verification portion is completed, the forensic examiner will create a working copy of the evidence. This action is performed by creating an exact, bit-for-bit copy of the evidence that is placed on the forensically prepared media. Once the image is created, examiners will verify that the digital fingerprint (hash algorithm) matches to show the evidence has not changed. This is done to preserve the original evidence while the examiner investigates the device.

In the catalog section of the workflow, the examiner identifies all the devices, applications, and contents of the device. This response is obtained through the identification of drive Geometry and File listing. Next, the examiner will search, find, and extract (SFE). This is the section of the workflow where the investigator will adhere to their legal authority in delving into the devices and repositories for evidence congruent to the crime. After the evidence is found and the examiner's actions are documented, the examiner will perform a post-exam verification. The verification results will fall into two different categories: a match or a mismatch with the original pre-exam hash derived from the initial evidence. When the verification matches, it signifies the evidence remained unaltered throughout the investigation workflow. Conversely, if the verification is mismatched, the examiner will delve into the irregularities, potentially necessitating a restart of the examination of the working copy. Often, the error stems from issues with the tools used, hence, the importance of structured guidelines of tool audits and functioning verifications.

At the end of the workflow, an examiner will produce derivative evidence consisting of reports documenting the investigations and backups of the process. In addition, the investigator will prepare the forensically discovered evidence for evidential discovery in the legal system and presentation for trial.

II. Digital Forensics for Criminal Prosecution and Digital forensics Incident Response (DFIR)

Digital forensic examiners, possessing specialized expertise, play a pivotal role in the realm of forensic science. Grasping the essence of digital forensics and its methodologies underscores the complexities in countering malevolent activities prevalent in the digital landscape. Instances of crime have endured over time, and as both time and technology have progressed, the gravity of these cyber-attacks has amplified, consequently leading to the bifurcation of digital forensics into two distinct fields. This section will explain these branches, exploring their commonalities, differences, and points of convergence in the field of digital forensics.

A. Law Enforcement Digital Forensics

Digital forensics for criminal prosecution primarily involves the examination and analysis of digital evidence for use in legal proceedings and criminal investigation following strict legal framework and regulations. This branch of digital forensics plays a pivotal role in the pursuit of justice by recovering and preserving digital evidence, ensuring its integrity, and presenting it effectively in a court of law.

The goal of digital forensics in criminal prosecution revolves around the extraction of information in electronic devices, transforming the data into actionable intelligence, and delivering their findings for legal proceedings [17].

B. Digital Forensics Incident Response (DFIR)

Digital Forensics Incident Response (DFIR) is centered on the investigation of cyber incidents and protecting digital systems from security breaches. This branch plays a pivotal role in identifying the source of cyber-attacks, analyzing threat actor tactics, and facilitating the recovery and remediation of compromised systems.

The goals of DFIR are to identify, preserve, analyze, and document digital evidence congruent to cyber-crime [18]. Additionally, the main objectives include identifying network

vulnerabilities and deploying mitigative techniques [19], uncovering the "who, what, and how" behind security incidents to retrace the hacker's actions to restore functionality, and to build a more robust system [20].

C. Live vs. Dead Analysis

The separation between these two branches is identified by two distinct techniques: traditional (commonly called "dead analysis" or "static analysis") and live analysis. Dead analysis is deployed by examiners in criminal prosecution capacities. Live analysis is deployed by DFIR.

Dead or static analysis is performed by digital forensic examiners in the criminal prosecution branch. Dead forensics is conducted on inert media, typically involving devices that are powered off. An example of a powered-off, inert media device would be a hard drive. Hard drives are removed from potentially compromised systems before analysis begins [21]. This approach stands as the most exhaustive means of preparing evidence, offering the advantage of complete preservation and examination of physical volumes [21]. Dead analysis methods come into play once the system's power is turned off and the forensically prepared bit-for-bit replica of the hard drive is created. The exact copy of the evidence is then scrutinized in a controlled environment using trusted operating systems and approved applications [22]. In the field of digital forensics for criminal prosecution, opting to use dead analysis techniques holds precedence over live analysis due to its non-interference with the original state of the system under investigation, and the ability to recover data from severely damaged devices [23].

Live analysis is the technique of analyzing a system while it is still powered on and actively performing. There is a preference in Digital Forensic Incident Response (DFIR) for live analysis, since examiners have the potential to yield more precise outcomes. This approach allows examiners to observe real-time system activities, which prove invaluable in the detection of malware and monitoring networks, logs, and other malicious actions [24]. However, it is vital to note that live analysis can pose greater challenges compared to dead analysis due to the requirement of specialized tools, expertise, and funding, which fluctuates from one organization to another [25].

D. Overlap of the two domains

The difficulty in comparing the two realms of digital forensics lies within conflicts of interest. Digital forensics for criminal prosecution adhere to laws regarding convicting or exonerating a suspect of a crime. Conversely, DFIR concerns do not revolve around criminal prosecution. Their concern centers around private company interests, using frameworks and various regulations, such as CCPA, HIPPA, and GDPR, in mitigating attacks, restoring lost data to preserve the company brand, customers, and monetary interests [20].

The overlapping similarities consist of the utilization of digital evidence to probe criminal efforts and cyber assaults. Both domains have the objective to scientifically prove the who, what, where, when, and how for security incidents and criminal activities. The criminal prosecution perspective focuses their efforts on retracing the suspects and victim's steps to comprehend the methodologies and motives behind the crimes. The cybersecurity perspective focuses their efforts in retracing the steps of a hacker to comprehend the methodologies behind intrusion attacks.

Digital forensics for criminal prosecution specialize in reactive forensics and highly effective means for preserving evidence for legal discovery. DFIR specializes in proactive forensics to avert attacks before they materialize. Despite the distinct goals, these two branches share common functionalities tailored for their respective objectives. Nevertheless, when cybersecurity incidents reach a critical juncture demanding responses that are ethically ambivalent or necessitate legal intervention, these two branches seamlessly cooperate toward a shared objective. The collaboration of the two branches ensure that response actions adhere to ethical, regulatory, and legal frameworks, allowing for a comprehensive approach to managing intricate cyber incidents.

III. Cybersecurity incident response (CSIR)

Cybersecurity Incident Response (CSIR) involves evaluating, countering, and providing valuable insight to building a robust system within an organization [26]. This idea relates to the methods and technologies in an organization that detect and counteract cyber threats, breaches in security, or cyber-attacks that plague modern day organizations [27]. In the event where malicious cyber catastrophes exist, support is extended to the potential affected organization by the government. The federal agency that is accountable for assistance, and the preservation to avoid repercussions on critical infrastructures lies with Homeland Security. In a serious rapid expanding incident, Homeland Security collaborates with federal agencies with similar cyber objective, local law enforcement, and the private sector to identify the individuals responsible for the attacks and orchestrates the national approach to cyber occurrences [28].

A. Incident Response

An incident response plan consists of projected procedures that organizations employ to recognize and address cybersecurity occurrences. When an incident occurs, it is important that highly skilled practitioners respond to the threat for containment and recovery. Incident response consists of many frameworks that private and public sectors can choose from. These frameworks include the National Institute of Standards and Technology (NIST) framework, SysAdmin, Audit, Network, and Security (SANS) framework, the Cyber Incident Response (CERT) Resilience Management Model (CERT-RMM) framework, OCTAVE Allegro framework, International Organization for Standardization, the International Electronical Commission (ISO/IEC) framework, and the Cybersecurity Framework (CSF). Of these, the most widely used, and the framework this paper focuses on, is the National Institute of Standard Technology (NIST) framework [29].

The NIST incident response plan encompasses four main processes. These steps, shown in figure 1, are designed to provide an organization with a comprehensive framework for effectively handling cybersecurity incident responses. As organizations implement the following steps, it is crucial to

recognize that the framework is a fluid program, adapting to the evolving threat landscape.

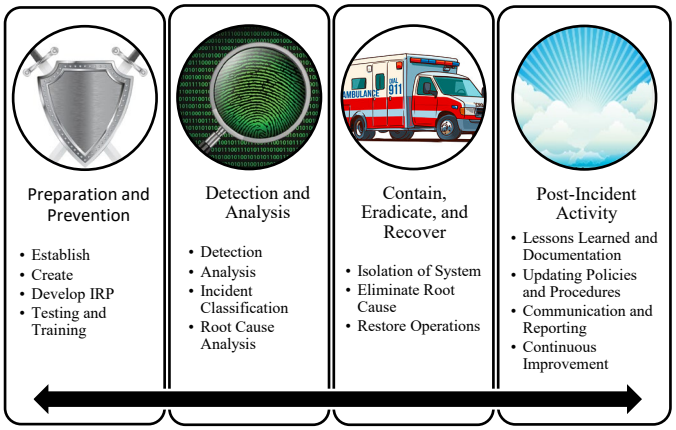

Fig. 1. *National Institute Of Standards Technology Incident Response Framework*

B. Steps Involved in Cyber Incident Response

In the Preparation and Prevention stage of the NIST Incident Response Framework [30], organizations set up a robust response capability by creating dedicated teams, defining roles, and training their team members to create a formulated and comprehensive incident response policy aligned with business objectives, compliance requirements, and criteria for escalations. These plans need to be tailored to the organizations Information Technology (IT) environment, covering communication strategies, resource allocation, evidence preservation, and legal aspects. In addition, the organization needs to perform regular testing to validate plan effectiveness and give team members an advantage in defense by knowing their systems.

In the Detection and Analysis stage of the NIST Incident Response Framework [30] focuses on proactive monitoring and swift identification of potential security breaches or uncommon activities. These actions include establishing a resilient monitoring system to track network traffic and system logs and promptly detecting anomalies that could indicate security incidents. Upon identifying an incident, the event is categorized based on the severity and the potential impact to determine the type of response needed for efficiency. The incident response team then executes rapid and well-defined actions, assigning specific responsibilities for containment and investigation. During the forensic investigative analysis, investigators will meticulously and methodically unearth the root cause of the incident. As the team investigates deeper into the problem, they will detect exploited vulnerabilities and carefully preserve the crucial evidence for potential legal proceedings [30].

In the Contain, Eradicate, and Recover stage of the NIST Incident Response Framework [30], immediate action is taken to confine the incident's impact. This response is accomplished through isolating the affected system and deploying intrusion detection mechanisms. The root cause of the incident is identified and eliminated by thoroughly mitigating vulnerabilities, patching, and cleaning the system. Subsequently, recovery procedures are executed, involving data and system restoration from clean backups, followed by rigorous integrity checks. An additional and vital aspect of this stage is using thorough and proper documentation, communication, and execution of individual responsibilities within the team.

In the Post-Incident Activity stage of the NIST Incident Response Framework, the organization engages in a comprehensive review of the incident, documenting both the successful strategies, and the areas that need improving. As with the previous stage, effective communication is key. Communication with the stakeholders, regulatory bodies, and potential affected parties is vital. The incident is formally closed once containment and recovery efforts are completed and verified. The organization will use the information throughout the event to continuously improve, including training, addressing found internal issues, and making necessary changes to policy and standard operating procedures [30].

C. Roles of Digital Forensic Methodologies in each Step of the Response Process

Digital Forensics has an essential role in every step of the NIST Incident Response Framework. Examiners contribute their knowledge and skills to help investigation, analyses, and mitigation of the threat. During the preparation and prevention stage, examiners are identified as a part of the team while being trained to collect, preserve, and analyze digital evidence. Their role, in this stage, is to meticulously define the proper procedures for evidence preservation to ensure accuracy and possible e-discovery for legal proceedings.

During the detection and analysis stage, examiners adhere to the established protocols to collect and preserve digital data as evidence when the proper identification of the threat is known. Examiners will capture volatile data from the live systems to create forensic images or working copies. Examiners will then analyze the artifacts contained in the evidence, to determine the incident's scope, identifying attack vectors, compromised assets, and potential data breaches.

In the containment, eradication, and recovery phase, examiners provide valuable insight for the root cause of the incident, the attackers, methodologies, and how the vulnerability was exploited. This insight allows for an effective eradication of the threat and provides direction for actions to prevent future attacks. Additionally, the information found by the examiners holds legal prosecution weights and regulatory compliance verifications.

With resolution of the incident, examiners analyze the incident's timeline and tactics. Extracting lessons learned, these insights contribute to policy updates and fortifies the organization's security posture, thus enhancing future response efforts.

IV. Digital Forensic Challenges in Incident Response

In response to one of the most compelling challenges of the digital age, Incident Response Frameworks have emerged. Modern society's heavy reliance on digital connectivity and technology for daily functions has contributed to a perpetually shifting threat landscape. This dynamic environment consistently gives rise to an unending barrage of cyberattacks.

However, a meticulous examination of the challenge intertwined with cyber incident response reveals a significant disparity. While digital forensics has demonstrated remarkable success in criminal prosecution, its adaptation to digital forensics incident response has encountered obstacles that hinder comparable achievements. Unlike the relatively linear trajectory of digital forensics in criminal prosecution, the inherently dynamic nature of cyber incident response introduces a multitude of complexities.

A. Statistics

Echoing off news channels, resonating in local law enforcement agencies, and reverberating through political events, a common chorus persists - crime is on the rise. The comprehension of this statement is difficult to fully comprehend without seeing the statistical data.

According to the Federal Bureau of Investigation Internet Crime Report (2022), the scale of victimization and monetary losses is staggering. Table 1 clearly illustrates the growth of cyber-crime since 2018. Over the course of five years, the number of reported complaints that represent instances of cyber-attacks has shown a constant increase. However, the financial toll of these attacks is monumental, with 2022 witnessing a increase of 381% more financial losses than 2018.

TABLE 1, FIVE YEAR STATISTICS

Complaint and Loss Comparison: 2018-2022

Year	**Complaint**	**Monetary Loss**
2018	351,937	$2.7 Billion
2019	467,361	$3.5 Billion
2020	791,790	$4.2 Billion
2021	847,376	$6.9 Billion
2022	800,944	$10.3 Billion
Total:	3.2Million Total Complaints	$27.6 Billion in Total Losses

Table 1 reveals compelling statistics from the past five years, pointing to significant revenue loss attributed to digital technology used in crimes. The persistent accent culminating in a total victim loss of $10.3 billion in 2022 requires further analysis. Over the span of 2016 to 2021, an estimated 651,800 cases were reported. However, in 2022 alone, this number surged drastically to over 7.3 million complaints of individuals and organizations victimized through digital technology. These numbers translate to an average of 2,175 compromisations daily [31].

These statistics not only inform us of the prevailing landscape but also shed light on the profound hurdles that digital forensics confronts. The realm of cyber-crime investigation encompasses a myriad of offenses demanding thorough examination. Table 2 presents a comprehensive breakdown of these crimes by victim count and monetary loss by the Federal Bureau of Investigation's Internet Crime Report.

TABLE 2, YEARLY CRIME TREND

Crime Trends		2021	2022
Credit Card/Check Fraud	**Increased**	$172 M	$264 M
Crimes Against Children	**Increased**	$198 T	$577 T
Data Breach	**Increased**	$151 M	$459 M
Extortion	**Decreased**	$60 M	$54 M
Identity Theft	**Decreased**	$278 M	$189 M
Malware	**Increased**	$5.5 M	$9.3 M
Personal Data Breach	**Increased**	$517 M	$742 M
Phishing	**Increased**	$44 M	$52 M
Ransomware	**Decreased**	$49 M	$34.3 M
Spoofing	**Increased**	$82 M	$107 M
Threats of Violence	**N/A**	$4 M	N/A
Harassment/Stalking	**N/A**	$5 M	N/A

The staggering scale of monetary losses incurred by both individuals and organizations is a distress signal for attention. Although Table 2 is not an exhaustive inventory of all reported crimes, it provides a striking illustration of the exponentially increasing rates. Among the twenty-seven crimes listed in the report, eighteen experienced an increase from 2021 to 2022, with three new additional crimes introduced as statistical data. In addition, fifteen of the twenty-three reported crimes demonstrated escalation from 2020-2021. This consistent upward trajectory of escalating losses urgently emphasizes the need for improvement.

In pursuit of improvement, the critical first step entails identification of roadblocks and challenges. Numerous areas in digital forensics incident response have already documented challenges. These encompass a rapidly evolving landscape, the intricate nature of digital ecosystems, a lack of standardization, constraints in resources, and complex legal and regulatory challenges.

B. Challenges to Overcome

The domain of cybersecurity that exists is often referred to as the cyber threat landscape. Consequently, the first challenge to overcome is the rapidly evolving nature of the threat landscape [32], while encompassing a wide array of existing threats that impact specific regions, industries, or communities. The arena where attackers and defenders are in perpetual flux gives rise to fresh challenges each year, broadening the scope in which cybersecurity professionals operate. This challenge is a major concern due to the swift proliferation of the internet, which has outpaced the advancements of cybersecurity measures, leaving both business and casual internet users vulnerable to threats.

The expanding and evolving threat landscape segways into the next challenge: the complexity of digital ecosystems. The

digital ecosystem is a complex network involving people, enterprises, and systems that use technology to interact with one another. Digital ecosystems capitalize on physical layers (devices), information layers (data), and application layers (apps) [33]. A complex ecosystem utilizes technology to gather customer data for innovating new products, offering services, and crafting customized customer experiences. The use of this data empowers companies to harness all three layers at once, facilitating seamless interactions between customers. However, this complexity poses a challenge for incident response. The intricate interplay of these layers and components demands a comprehensive and adaptable approach to managing cyber incidents effectively.

The third challenge to digital evidence incident response includes the lack of standardization. This challenge can result in confusion and operational inefficiencies for an effective response. Unlike the standardized procedures prevalent in digital forensics for criminal prosecution, the landscape of the incident response often lacks uniformity. This absence of standardization protocols allows different organizations to adopt diverse procedures and tools to address cyber incidents. Consequently, the absence of consistent standards makes it challenging to coordinate collective efforts and share crucial information among various entities engaged in incident response. This glaring disparity stresses the importance of establishing a comprehensive standardization in cyber incident response procedures, to ensure a coherent and effective response to evolving cyber threats.

Resource constraints represent another formidable challenge, stemming from organizations' insufficient personnel and expertise [34] to mount effective responses to cyber incidents. Furthermore, many organizations may lack the necessary tools and technologies, or simply cannot afford to implement such measures, which hampers their ability to promptly detect and respond to incidents. This scarcity of resources underscores the critical need for both human expertise and appropriate technological investments in building a robust incident response management system.

The final challenge this paper addresses is legal and regulatory hurdles. In cyberspace and incident response, ensuring accuracy and integrity of cyber evidence becomes a serious concern. Intertwined with the growing threat landscape brought on by legal and regulatory challenges, digital forensic examiners stand as crucial sentinels in this domain, wielding their specialized skillset to guarantee that evidence collection, preservation, and analysis align with exacting legal standards. As examiners navigate through the complexities of modern cyber threats, they use advanced procedures, technologies, and tools to meticulously extract digital evidence. The demanding nature of this field engages multifaceted challenges like jurisdictional ambiguities, data privacy regulations, cross-border, data transfers, and the delicate balance of cooperating with law enforcement. In an environment where oversight can lead to severe legal consequences, the role of examiners has become not only indispensable, but also highly exacting. An examiner's expertise in navigating intricate digital landscapes is vital in providing reliable evidence that can withstand legal scrutiny, ultimately contributing to the resolution of cyber incidents.

V. Case Studies

The challenges in digital forensics incident response carry the potential for severe repercussions, as illuminated by the statistics presented in this paper. It is imperative to address these challenges through a multifaceted approach that encompasses the cultivation of highly skilled professionals, the provision of requisite tools for the organizations, the enhancement of communication within the cyber community for ethical implementation of digital forensics principles, and the strategic progression to counter the ever-evolving landscape of cyber-crime.

The efficiency of digital forensic science is maximized when executed through stringent procedures and utilization of appropriate tools. Addressing the issues arising from live forensics mandates a consistent surveillance approach, affording examiners the opportunity to shift from a reactive stance to a proactive one. Demonstrating the efficiency of digital forensics, the following case studies spotlight the prowess of dead analysis, underscoring the limitations inherent to live analysis in similar scenarios.

A. BTK Killer

The BTK Killer committed a series of ten murders spanning seventeen years. The case turned cold in 1991 after his last confirmed murder, but resurfaced in 2004. The serial killer sought dialogue with a news reporter, divulging his perspective of the crimes. Through notes, poems, and packages containing the victim's belongings, the killer maintained an unsettling correspondence. In 2005, a pivotal turn occurred as the killer sent a floppy disk, along with a BTK letter, to a local television station. The information was promptly transferred to law enforcement to undergo analysis by digital forensic examiners.

In the digital evidence, the examiners uncovered metadata offering valuable insights. These digital breadcrumbs contained details about the author of the documents and a particular church. By delving into this data, investigators unveiled the trail leading to the identification and arrest of Dennis Radar, conclusively linking him to the BTK killings [35].

B. The Boston Marathon Bombing

The 2013 Boston Marathon bombing marked a tragic event that brought digital forensics to the forefront of the investigation. The attack involved two homemade pressure cooker bombs detonated near the finish line of the marathon, resulting in casualties and widespread chaos. Digital forensics examiners played a crucial role in piecing together the events by meticulously analyzing a vast array of digital evidence. The digital traces left by the perpetrators, including their online activities, communications, and facial recognition technology, were instrumental in identifying and apprehension of Tamerlan Tsarnaev and Dzhokhar Tsarnaev.

C. Sony Pictures Hack

Digital forensics emerged as a crucial force in unveiling the intricacies of Sony Pictures hack by meticulously examining the malware integral to the attack. Through forensic analysis, examiners identified striking similarities in the code employed,

drawing parallels with code utilized in previous cyber intrusions unequivocally attributed to North Korea. The investigative efforts extended further, as the Federal Bureau of Investigation scrutinized the origins of the attackers' IP addresses. This intensive examination unearthed compelling evidence linking some of these IP addresses to North Korea, further solidifying the cause against the responsible parties. The collaboration of the two digital forensic branches, incident response and criminal prosecution, unveiled hidden insight within the digital landscape and the attacker's origin, highlighting the profound impact of digital evidence in navigating the complexities of cyber incidents [37].

VI. Digital Forensics Best Practices

As digital forensics has become increasingly vital in the modern era, it continues to necessitate a structures and synchronous role in criminal justice investigations, litigation, and cybersecurity incidents. Ensuring the integrity and reliability of digital evidence demands the application of rigorous best practices. As stipulated by the National Institute of Standards and Technology (NIST), the bedrock of digital evidence examination resides in the principles of computer science. The efficient use of these computational techniques emphasizes the credibility of digital investigations. Amongst the basic best practices are data duplication, text string searches, timestamp analysis, and the examination of call logs in mobile devices. These techniques are fundamental components of a digital inquiry, utilizing widely applied and comprehensively understood basic computer operations [38].

Additional best practices encompass discerning the root cause of digital issues, accurate identification and localization of all available data and evidence, and the provision of continuous support to fortify an organization's security posture [39]. When dealing with digital evidence, it is imperative to adhere to overreaching forensic and procedural tenets. The meticulous processes of collecting, securing, and transporting digital evidence should be orchestrated in a manner that preserves the integrity of the evidence itself. Crucially, the examination of digital evidence must be exclusively entrusted to experts with specialized training in this domain, mitigating the risk of inadvertent contamination or compromise [14].

VII. Conclusion

In conclusion, there is fundamental significance of digital forensics methodologies in the realm of cyber incident response. The complex challenges faced by digital forensic experts in countering evolving cyber threats highlight the critical need for ongoing advancements in the field. Embracing a comprehensive array of best practices, coupled with the cultivation of adaptive methodologies, organizations can elevate the effectiveness of their incident response strategies, ending in the adept safeguarding of their digital assets.

As the dynamic cyber landscape continuously evolves, it remains paramount for both governmental bodies and private enterprises to proactively prioritize the domains of cybersecurity and digital forensics. This unwavering commitment is instrumental in fortifying the protective layers of digital ecosystems, and preserving the untarnished integrity of sensitive data. Through conscientious integration of these best practices, organizations manifest their dedication not only to respond to cyber threats but also to anticipate, prevent, and mitigate them in an agile and proactive manner. These deliberate efforts position organizations to forge resilient incident response architectures, well-prepared to navigate the multifaceted challenges posed by the evolving cyber threat landscape.

References

[1] SACHOWSKI, J. (2021). Introduction to Digital Forensics. In Digital Forensics and investigations: People, process, and technologies to defend the Enterprise (pp. 3–17). essay, CRC PRESS.

[2] FBI.(2016, June 17). Timeline. FBI. https://www.fbi.gov/history/timeline

[3] About. High Technology Crime Investigation Association. (2023, July 27). https://www.htcia.org/about/#history

[4] Crime Laboratory Digest. (1992). Computer Analysis and Response Team(CART):The Microcompter as Evidence https://www.ojp.gov/pdffiles1/Digitization/137561NCJRS.pdf

[5] Digital Millennium Copyright Act. (n.d.-b). https://www.govinfo.gov/content/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf

[6] Federated Testing Project. NIST. (2023, April 26). https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/federated-testing

[7] USA PATRIOT Act. USA PATRIOT Act | FinCEN.gov. (n.d.). https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

[8] projects, C. to W. (2023, April 16). Convention on cybercrime. AtoZ Wiki - A to Z Information at your tips. https://atozwiki.com/Convention_on_Cybercrime

[9] 2006 amendments to the Federal Rules of Civil procedure. (n.d.-a). https://www.maglaw.com/media/publications/articles/2006-10-05-2006-amendments-to-the-federal-rules-of-civil-procedure/_res/id=Attachments/index=0/07010060004Morvillo.pdf

[10] Obama's Cybersecurity Executive Order: What you need to know. ZDNET. (n.d.). https://www.zdnet.com/article/obamas-cybersecurity-executive-order-what-you-need-to-know/

[11] Computer Security Division, I. T. L. (n.d.). CSRC topic: Cybersecurity Enhancement Act. CSRC. https://csrc.nist.gov/Topics/Laws-and-Regulations/laws/Cybersecurity-Enhancement-Act

[12] The five functions. NIST. (2023b, March 16). https://www.nist.gov/cyberframework/online-learning/five-functions

[13] The United States Government. (2021, May 12). Executive order on improving the nation's cybersecurity. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[14] Investigative uses of technology: Devices, tools, and Techniques. National Institute of Justice. (n.d.). https://nij.ojp.gov/library/publications/investigative-uses-technology-devices-tools-and-techniques

[15] Digital Evidence Field Guide. Regional Computer Forensics Laboratory. (2018, July 9). https://www.rcfl.gov/file-repository/fieldguide_sc.pdf/view#:~:text=Digital%20Evidence%20Field%20Guide%20Properly%20handling%20digital%20evidence,pre-%20serve%2C%20and%20transport%20this%20type%20of%20evidence.

[16] Hoffman, C. (2017, February 17). What are MD5, SHA-1, and SHA-256 hashes, and how do I check them?. How. https://www.howtogeek.com/67241/htg-explains-what-are-md5-sha-1-hashes-and-how-do-i-check-them/

[17] Digital Forensics. INTERPOL. (n.d.). https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics

[18] What is Digital Forensics: Phases of Digital Forensics: EC-Council. EC. (2023, July 24). https://www.eccouncil.org/cybersecurity/what-is-digital-forensics/

[19] What is Digital Forensics in cyber security?. What is Digital Forensics in Cyber Security: Is This a Good Career for Me? (n.d.). https://www.ecpi.edu/blog/what-is-digital-forensics-in-cybersecurity-is-this-a-good-career-for-me

[20] Mehta, M. (2022, March 3). Cyber security and digital forensics: What's the difference? InfoSec Insights. https://sectigostore.com/blog/cyber-security-and-digital-forensics-whats-the-difference/

[21] Johansen, G. (n.d.). Digital Forensics and incident response. O'Reilly Online Learning. https://www.oreilly.com/library/view/digital-forensics-and/9781787288683/2925d222-5f43-4e05-9309-0ecfa17b95cf.xhtml

[22] Carrier, B. D. (2006, February 1). Risks of live digital forensic analysis. ACM. https://cacm.acm.org/magazines/2006/2/5996-risks-of-live-digital-forensic-analysis/abstract

[23] IPL. (n.d.). Advantages And Disadvantages Of Digital Forensics. Advantages and disadvantages of Digital Forensics. https://www.ipl.org/essay/Advantages-And-Disadvantages-Of-Digital-Forensics-PK8RF5HEACFR

[24] Google. (n.d.). How to use live forensics to analyze a cyberattack | google cloud blog. Google. https://cloud.google.com/blog/products/identity-security/how-to-use-live-forensics-to-analyze-a-cyberattack

[25] Combining static and live digital forensic analysis in ... - IEEE xplore. (n.d.). https://ieeexplore.ieee.org/document/5348415

[26] *Security Qradar*. IBM. (n.d.). https://www.ibm.com/qradar

[27] *What is incident response?*. IBM. (n.d.-b). https://www.ibm.com/topics/incident-response

[28] *Cybersecurity Incident Response: CISA*. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response

[29] Mutune, G. (2022, August 13). *23 top cybersecurity frameworks*. CyberExperts.com. https://cyberexperts.com/cybersecurity-frameworks/

[30] Salfati, E., & Pease, M. (2022, November 29). *Digital Forensics and Incident Response (DFIR) framework for Operational Technology (OT)*. NIST. https://www.nist.gov/publications/digital-forensics-and-incident-response-dfir-framework-operational-technology-ot

[31] 2022 1INTERNET Crime report - internet crime complaint center. (n.d.-b). https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[32] *What is the cyber threat landscape?: Upguard*. RSS. (n.d.). https://www.upguard.com/blog/cyber-threat-landscape

[33] *Everything you need to know about digital ecosystems*. IMD business school for management and leadership courses. (2023, January 31). https://www.imd.org/reflections/digital-ecosystems/

[34] Forensic Focus. (2020, May 12). *An introduction to challenges in digital forensics*. Forensic Focus. https://www.forensicfocus.com/articles/an-introduction-to-challenges-in-digital-forensics/

[35] A&E Television Networks. (n.d.). *BTK Killer Sends message*. History.com. https://www.history.com/this-day-in-history/btk-killer-sends-message

[36] Staff, M. N. (2023, August 12). *1 dead, 6 injured after mass shooting at Minneapolis Punk Show*. MPR News. https://www.mprnews.org/story/2023/08/12/1-dead-6-injured-after-mass-shooting-at-minneapolis-punk-show

[37] Lee, T. B. (2014, December 14). *The Sony hack: How it happened, who is responsible, and what we've learned*. Vox. https://www.vox.com/2014/12/14/7387945/sony-hack-explained

[38] *Digital Forensics*. BU MET Landing Pages. (2023a, February 8). https://bumetprograms.bu.edu/digitalforensics/

[39] *Digital Forensics and Incident Response (DFIR)*. Palo Alto Networks. (n.d.). https://www.paloaltonetworks.com/cyberpedia/digital-forensics-and-incident-response