International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Use of Digital Forensics in Cybersecurity and Criminal Cases, How Can it be Leveraged, Challenges

Pranith Shetty

Information Security and Risk Officer, Morgan Stanley, New York

Abstract: ***Digital forensics is a very important string in Cybersecurity defense, since it helps understand the root cause of incidents, attacks in the private sector. Using this data, organizations can generate threat intel to protect them from future attacks. This could save firms a lot of capital expense. Digital forensics or sometimes alternatively referred as Cyber Forensics is a very good defensive tactic that alongside fields like incident management can be very useful strategically. On the other hand in the public sector, especially law enforcement, Digital Forensics has played a pivotal role for more than a couple of decades now, techniques and tools have evolved but the strategies have remained more or less the same. This article aims at understanding, firstly, the connection between Digital forensics and Cybersecurity, secondly the role played by digital forensics in Cybercrime, also delves a little bit into the recent history of digital forensics, how is it relevant today, the benefits of using forensic techniques. There are challenges in the field of forensics but there are ways to overcome those challenges. This paper provides a comprehensive view point of forensics and aims to educate the readers on the nuances in this field and its usefulness in particularly two areas namely Cybersecurity and Cybercrime.***

Keywords: Digital forensics, Computer forensics, Cybercrime, Risk, Criminal cases, Cybersecurity

1. Introduction

[1] Digital forensics and Cybersecurity are concepts used in the same vein, Cybersecurity is about being proactive in protecting your business's infrastructure, controls and measures are taken to ensure the organization safe from threats.

Forensics is reactive as per its operational concept, it's more of an investigation after the attack, trying to recover information from the devices, it comes into the picture usually when the threat actors or attackers are in court of law or during the interrogation processes.

Forensics branches out in a way to form threat intel that provides information for more cybersecurity controls, thus they are related in the world of information assurance and both are important for each other.

Cyber security deals with using software or tactics to protect a device or network from hackers and hijackers [2] Digital forensics describes a scientific investigation process in which the investigator collects computer artifacts, data points, and information about a cyberattack. It's the first step towards closure of ransomware and cyberattacks. When a cybersecurity incident is uncovered, an investigation is usually carried out to find out the root cause of attacks, Digital forensics by definition involves the court of law however, digital forensic specialists operate both in public and private sectors.

[4] Digital forensics in the public domain is typically associated with criminal law since it involves gathering evidence from digital sources that implicate an individual in a crime. Digital forensics plays a key role in preventing and investigating various crimes, such as fraud, identity theft, hacking, and even terrorism.

2. Digital Forensics

[3] By definition, "the identification, preservation, examination, and analysis of digital evidence, using scientifically accepted and validated process, and the ultimate presentation of that evidence in a court of law to answer some legal question.

Its sometimes referred to as Computer forensics, also as Cyber forensics; if the investigation is meant to find evidence around cyber - crime.

[2] Literally, by definition, computer forensics is a branch of digital forensics that focuses on extracting information from computers, but over the course of investigations, Digital and computer forensics are alternatively used and that is ok.

History:
[3] The adoption of digital forensic techniques to computers and high tech equipment was comparatively slow since the general assumption was confidential data was in physical format like the usual files and folders stored in cabinet storage, the idea that information could be stored in digital format in data storage had not caught the attention of law enforcement. In around 1984, FBI launched the Magnet Media program to divert their attention towards digital records, the first official digital forensics program at law enforcement agency.

Many of the other techniques used to track down and identify hackers were discovered accidentally later in 1986 by Cliff Stoll, a UNIX sysadmin who had figured out discrepancy in the accounting log and ended up tempting a German attacker and thus the term Honeypot trap was conceptualized.

The development of this space furthered over the 90s and 2000s in reaction to two major criminal themes, first one around the spread of child pornography online which led to

DOI: https://dx.doi.org/10.21275/SR24213025946

capture of large volumes of digital evidence and secondly around the wars in Afghanistan & Iraq where the US troops ended up capturing a lot of evidence and now information had to be extracted,

Year 2006 also paved the way for United States Rules for Civil Procedure which implemented mandatory policies for electronic discovery.

Tools:

[3] Use of varied tools is key in the forensic profession, there are basic tools, free versions of packet capture tools like Wireshark, and on the other end, we can find enterprise versions of tools like Encase. There are tools catering to various storage mediums, for example you can have dedicated tools to extract information from your cell phones, something called an iPhone Analyzer could be used to extract information from iPhone, similar to encase there are tools like Pro - discover that can scan storage mediums and recover even deleted information.

Generally, tools can be divided into the following categories:

1) Disk and data capture tools
2) File viewers
3) File and registry analysis tools
4) Internet analysis tools
5) Email analysis tools
6) Mobile devices analysis tools
7) Network forensic tools
8) Database forensic tools

Benefits of digital forensics:

The main advantage of digital forensics is the ability to identify the attacker through intel collected, this was a very challenging objective for law enforcement prior to 1980s especially around the sophisticated usage of computers. Investigating officers had a tough time catching or trying to identify cybercriminals

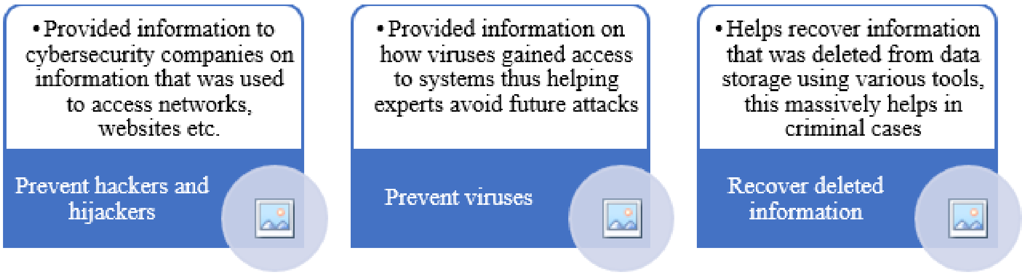
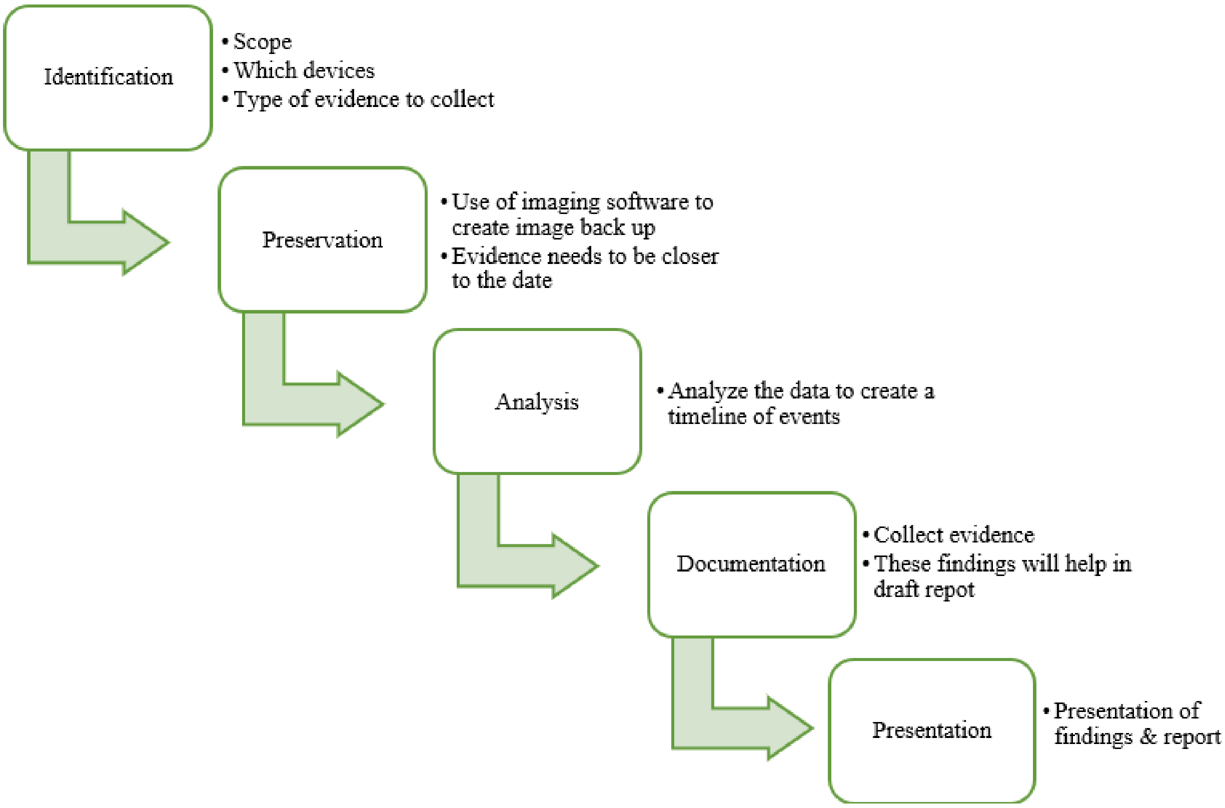

• Provided information to cybersecurity companies on information that was used to access networks, websites etc.
Prevent hackers and hijackers
• Provided information on how viruses gained access to systems thus helping experts avoid future attacks
Prevent viruses
• Helps recover information that was deleted from data storage using various tools, this massively helps in criminal cases
Recover deleted information

Figure 1: Benefits [1]

Steps in Digital forensics [2]:

Digital forensic experts while performing their investigation, follow a series of steps since its absolutely essential to provide a draft report of Investigation, along with steps followed, chain of evidence that helps both in private sector and criminal cases in the public sector.


Identification
• Scope
• Which devices
• Type of evidence to collect
Preservation
• Use of imaging software to create image back up
• Evidence needs to be closer to the date
Analysis
• Analyze the data to create a timeline of events
Documentation
• Collect evidence
• These findings will help in draft repot
Presentation
• Presentation of findings & report

3. Digital forensics in Cybercrime

Forensic experts play a key role in catching cyber criminals, primarily by investigating the scene of crime, if the criminal activity involves computers or use of technology, that's hwne Digital forensic experts take a lead in the case since the key piece of evidence might be tied with the use of technology by the criminal.

In the event of a cybercrime, forensic investigators must carefully preserve evidence at the scene of crime without corrupting data and following proper protocol,

While transferring or moving data from scene of crime, "chain of custody" is absolutely crucial, basically a log of events, who handled this data, when and all those details.

Improper handling of data might result in the report and findings not admissible in court so chain of custody is crucial. [4] By maintaining the chain of custody, authenticity and reliability of evidence can be established. Understanding file systems and encryption is also key in cybercrime investigations. Forensic examiners or investigators for law departments help catch criminals by using the varied tools at their disposal.

[6] Performing such an analysis could take anything from a day to a few months, depending on what was required, the state and security of the storage medium, or more importantly, the magnitude of the case. Increase in dark web activity has resulted in some challenges in the cybercrime area since traffic data and history are masked in dark web, trace route tools don't work, especially of browsers like TOR (onion routing protocol-based browser) are used.

4. Challenges and Discussion

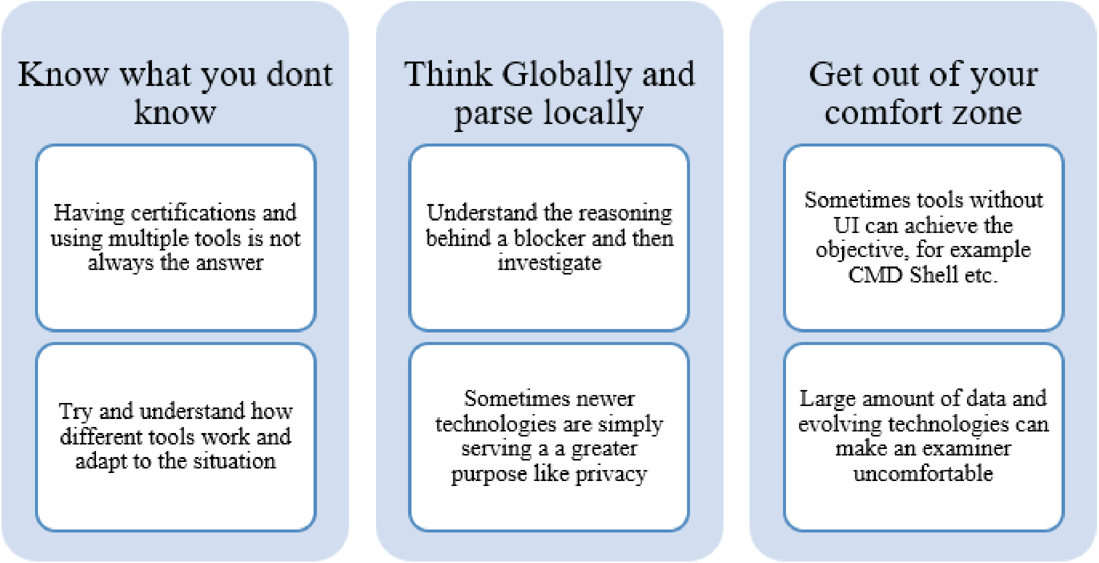
Digital forensics also like other technology domains needs to constantly evolve and keep pace with the threats, attacks and cybercrimes. There are 2 main types of challenges observed in this domain

Technical challenges [5] [8]:
1) Use of advanced encryption techniques – The tools at the forensic examiner's disposal should have the ability and capacity to crack advanced encryption mechanisms. Microsoft drives are encrypted by default using bit locker without user awareness, in such cases search warrants need to be issued and only then the examiners can proceed
2) Large volumes of data – Storing, processing and analyzing large data sets can be every problematic for the examiners since time, resources and effort spend are also key in these cases
3) Anti - forensic techniques – Methods like information hiding, cloaking and encryption all of these measures make it really hard for the forensic examiners and the "anti - forensic" mindset is on the rise amongst attackers.

Legal challenges:
Privacy preservation – Privacy is also important to a firm and victim; it becomes very challenging when the examiner stumbles accidentally across a lot of key information related to the case but cannot use it due to privacy issues brought up by the opposition.

Resource and time constraints:
Forensic examiners have an immense backlog of cases that requires their inputs, every case is deemed important by law enforcement, and clients want examiners to focus on their cases. Often times examiners have to scrape through large amount of data that might or might not end fruitful for the overall case, there might be times where they are stuck with certain encryption method or may be a new tool that's needed to uncover hidden data, all of the measures required need time and resources which sometimes can be very challenging

How to get ahead of these challenges [12]:



Know what you dont know

Having certifications and using multiple tools is not always the answer

Try and understand how different tools work and adapt to the situation

Think Globally and parse locally

Understand the reasoning behind a blocker and then investigate

Sometimes newer technologies are simply serving a a greater purpose like privacy

Get out of your comfort zone

Sometimes tools without UI can achieve the objective, for example CMD Shell etc.

Large amount of data and evolving technologies can make an examiner uncomfortable

5. Conclusion

Cybersecurity threat landscape is constantly evolving, it's very difficult to build a proactive defense and expect that there won't be any attacks, threat attackers are constantly on the lookout for gaps and vulnerabilities, it's almost impossible for organizations to remediate all vulnerabilities. Additionally, there will always be incidents to deal with for businesses, digital forensics is a space that can provide good quality intel to avoid these incidents and the risks that come alongside. There are various benefits of having forensic experts as part of our staff, with tools at their disposal, the defensive arsenal would gain a boost by having a dedicated forensics team.

In the field of Cybercrime and law enforcement, forensic experts have been a part of the investigation team for a long time, Digital forensics, however, is a branch that took shape a couple of decades back and is now a very strong and reliant wing of various police staff, with criminals constantly using modern techniques, computers, cellphones to attack victims, mobile forensics, network forensics have picked up steam and attention of the experts.

There are challenges that come with the use of forensics and for forensic examiners in general but these challenges can be overcome using certain strategies as highlighted in this paper.

References

[1] G. Blogger, "How Digital Forensics Is Important To Cyber Security, " *www.yoh. com*, Jun.11, 2020. [Online]. Available: https: //www.yoh. com/blog/how - digital - forensics - is - important - to - cybersecurity

[2] P. D. Team, "What is Digital Forensics and Why Is It Important?, " *Proven Data*, Jul.20, 2020. [Online]. Available: https: //www.provendata. com/blog/what - is - digital - forensics/

[3] "What is digital forensics? And how to land a job in this hot field, " *CSO Online*. [Online]. Available: https: //www.csoonline. com/article/566787

[4] P. Keheley, "Digital Forensics - Here's What Lawyers Need To Know, " *www.digitalwarroom. com*. [Online]. Available: https: //www.digitalwarroom. com/blog/digital - forensics

[5] B. Hartwig, "AI & Cyber Forensics: How Does AI Contribute to Digital Forensics? - IT Supply Chain, " *itsupplychain. com*, Sep.07, 2020. [Online]. Available: https: //itsupplychain. com/ai - cyber - forensics - how - does - ai - contribute - to - digital - forensics/

[6] "Digital forensics: How to catch a cybercriminal, " *WeLiveSecurity*, Feb.05, 2020. [Online. Available: https: //www.welivesecurity. com/2020/02/05/how - catch - cybercriminal - tales - digital - forensics - lab/

[7] L. Cameron, "Future of digital forensics faces six security challenges in fighting borderless cybercrime and dark web tools | IEEE Computer Society, " *Computer. org*, 2015. [Online]. Available: https: //www.computer. org/publications/tech - news/research/digital - forensics - security - challenges - cybercrime

[8] F. Focus, "An Introduction To Challenges In Digital Forensics, " *Forensic Focus*, Jun.29, 2017. [Online]. Available: https: //www.forensicfocus. com/articles/an - introduction - to - challenges - in - digital - forensics/

[9] "Forensic Challenges, " *DFRWS*. [Online]. Available: https: //dfrws. org/forensic - challenges/

[10] R. Boddington, "The challenges of digital forensics, " *Phys. org*, Mar.17, 2015. [Online]. Available: https: //phys. org/news/2015 - 03 - digital - forensics. html

[11] O. Carroll, "Challenges in Modern Digital Investigative Analysis, " *www.crime - scene - investigator. net*, Apr.26, 2019. [Online]. Available: https: //www.crime - scene - investigator. net/challenges - in - modern - digital - investigative - analysis. html

[12] S. Deyarmond, "How to Solve Digital Forensics Challenges? Be Curious, " *Magnet Forensics*, Mar.20, 2017. [Online]. Available: https: //www.magnetforensics. com/blog/solve - digital - forensics - challenges - curious/