ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

THE CURRENT HURDLES WHICH DIGITAL FORENSICS HAS TO CROSS

Sanjit Muralikrishnan
BK Gadia A levels Junior college
Email Address-sanjitmuralikrishnan@gmail.com

Abstract

Digital forensics is becoming a very important piece in solving many criminal investigations. However this technique is still in its infancy stage. There is a plethora of problems and short comings which effectively reduce its success rate. This research paper try's to explore the current shortcomings of this method such as lack of popularity in countries such as India and other problems such as data overload and potential solutions to these problems such as integrating AI and using better marketing methods to raise its popularity. Whilst the topic itself has been discussed before this research paper tries to integrate its own ideas and opinions on this topic.

Keywords: Anti-forensics, Internet Of things, Disk Degaussing

INTRODUCTION

The earth is about four and a half billion years old. And in this colossal amount of time humans never stopped evolving. Starting from ancient primates and then evolving into a sophisticated species. Many discoveries came along the way like the lightbulb etc. However it is an indisputable fact that the 21st century is the era where the most evolutions occurred due to advancements in technology. Similarly digital forensics also evolved, many cases have been solved with digital forensics. A few cases that come to mind are –

- The Matt Baker case where he was convicted for murdering his wife by overdosing her with sleeping pills, Investigations using digital forensics found out he searched "Overdosing on sleeping pills" and he also used multiple pharmaceutical websites just before her death.
- Krenar Lusha who was arrested based on his searches on the internet, he was found to have downloaded a researchmanual on how to make explosives. He also was found to have 71.8 liters of petrol.
- Larry Jo Thomas was arrested with the help of his Facebookposts; he was convicted of the murder of Rito Llamas Jaurez who was shot with a gun. Larry Jo Thomas was found to be the murderer .as he had taken a phot with the same model of gun with which Rito Llamas Jaurez was shot. He was also seen wearing a bracelet in one of his posts, the exact same bracelet was found near Rito Llamas Jauerez's body.

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA Global Partnership
MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

Digital forensics has also branched out into many categories such as- Disk forensics, network forensics, wireless forensics, database forensics, malware forensics, Email forensics, memory forensics, mobile phone forensics etc.However the evolution of digital forensics has proven to be insufficient. Compared to other forms of more established forensics methods, digital forensics fails to meet their high standards of accuracy. Though there have been cases where digital forensics has succeeded like the ones mentioned above, there have also been times where it failed or wasn't accepted in the court. One such famous exampleis the Griffith V.state case[7] where photos from a social network company called "Myspace" was used to prove that the girlfriend of the defendant had tried to threaten others to not give a testimony in court. Evidence showed that a Myspace account with a matching profile picture had sent threats to other people; however investigators couldn't prove that it was sent from her Mac or IP address due to insufficient amount of available data. It was very possible that it could have in fact been a fake account trying to stage her and so it could not be used as evidence.Digital forensics needs something more to become truly successful. With the number of crimes going up like crazy, digital forensics is becoming more and more needed. Unfortunately, numerous GB's of data needs to be analyzed, stored, reported etc. It also doesn't help that a lot of technical knowledge is required. This creates a huge backlog of cases which are still yet to be solved. In 2014, Darren Quick and Kim-Kwang Raymond Choo stated 3 things which could be leading to this backlog of cases.[1]

1) The sheer amount of devices which are being taken in for analysis has been increasing for every single case
2) There has also been a significant inflation in the number of cases where digital evidence is being accepted
3) There is also more evidence nowadays on any devices being seized for analysis.

The above 3 points should give a basic idea as to why backlogs occur. This situation is very serious as sometimes long delays lead to prosecutions being missed in court. This paper will review the current problems with digital forensics and will suggest potential solution to problems like using AI technology more frequently, better marketing to attract more youngsters and so on.

Theory

Improvements of digital forensics in the recent past-

Before going into the problems, the evolution of digital forensics should be acknowledged. During digital forensics early infancy, it was a small industry only used to support the investigation and was primarily used only at the end of a case to verify small details. It was nothing much of note. However, times have changed and now digital forensics can be considered as the left arm of crime investigators. It is immediately used at the beginning of investigations to clarify details and collect evidence. Many famous TV shows such as CSI: Crime Scene Investigation incorporates such aspects into the show. One of these fields' biggest achievements is hosting the DFRWS (Digital Forensic Research Workshop)[2] every year since 2001 to help educateyoung and aspiring future investigators and young people who are interested in Computer forensics.

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

Problems with digital forensics-

With advancements in technology, cybercrimes have started to become a common recurrence. However digital/cyber forensics is helping companies to avoid losses in money by identifying the crime occurring finding evidence available on laptops such as emails and files. However all is not well with digital forensics and there are few glaring problems. To summarize them simply before diving deep, we should see the 5 points which Sriram Raghavan stated in his research "Digital forensic research: Current state of the art" –[1]

1. The problem of complexity, this occurs because data is collected in the binary form. With the increasing amounts and complexity of metadata, advanced reduction techniques may be needed before analyzing the data.
2. The problem of diversity which is occurring due to increasing amounts of data coupled with the lack of techniques and to tools to analyze the ever increasing amount of data and different sources.
3. The consistency and correlation problem which arises from the fact that the tools used in digital forensics aid in finding out fragments of evidence but not to aid in investigation otherwise.
4. The volume problem which arises from the increasing number of devices which can store crucial information for an investigation and the lack of tools to analyze all the devices.
5. The unified time-lining problem which occurs due to different sources giving different times due to multiple reasons such as lag or problems with the set device timing.

Another glaring issue is that even though awareness of digital forensics is increasing, this is not affecting cybercrimes at all. In 2020 alone, over 1 trillion dollars (were predicted to be lost in cybercrime (as reported by the McAfee). To give a comparison, in 2018 the losses were about 600 million dollar; this is a jump in more than 50%. For computer forensics to be a success it need to slowly bring these values down even by a little bit.[8]

Antiforensics-

Technological evolution, as we discussed is never stagnant, so it should have been anticipated that something or the other would have been developed as a foil to digital forensics. This foil is called anti-forensics and every analysts dread it. Anti-forensics are techniques used to obstruct analyst. As of this moment, most people believe anti-forensics is purely a malicious practice for people with malicious intent. However, there are those who believe anti-forensics as ways to show the world the defiance's of digital forensics, thereby helping analysts to correct these problems and improve the art. Anti-forensics may also tempt analysts to work harder and collect better evidence which will make digital forensics better. While the points I have mentioned above are all true to some extent, I am certainly of the opinion that it isn't beneficial. This situation can be compared to the situation medical researchers are facing with pathogens. Each timean antibiotic is developed to kill a bacterium, after some time, the bacterium evolves and becomes resistant to it. The medical researchers again have to make an antibiotic and the game goes on like a never ending cat and mouse chase. Digital forensics and anti- forensics methods are following the same route. A never ending battle which will go on for generations to come.

Few techniques which were developed to aid digital forensics and cyber security are now cleverly being used in anti-forensics. The most famous example is encryption. Encryption is the

process by which the user makes a message unintelligible to third party access. It uses an encryption key which is a type of a mathematical algorithm to rearrange or change letters which makes the message make no sense to hackers. It was used to establish secure connection between computers and servers and to protect confidential files. Now people use these encryption techniques to hide files with potential evidence to prove one guilty thereby making it harder for analysts to discover the evidence.

Another currently unpopular anti-forensic technique is steganography. Steganography is a way of concealing messages in within other messages or another physical object as well. Steganography when correctly used can disturb the forensic processes. What's more is that criminal can use it to hide messages from digital forensics analysts making their lives all that much more harder. Currently steganography is not very popular but in due time it can become forensic analysts nightmare.

Another data hiding technique is spoofing. Spoofing disguises communication and makes a unknown and unsafe source seem like an authentic, safe and known source. Spoofing is very versatile technique which can be used in a variety of ways such as emails, websites or even phone calls. Spoofing is commonly used infiltrate a network and infects it with malware so that personal information can be retrieved. How can spoofing be used in antiforensics? Spoofing can be used to infiltrate systems with important digital evidence for a case. Criminals can even hide their IP address making it a whale of a task to track them down.

All of the above mentioned techniques are some form of data hiding. However these aren't the only types of anti forensic techniques. Other such examples include. Artifact wiping, Disk destruction techniques, and trail obfuscation.

Instead of simply hiding potential evidence from investigators, artifact wiping involves destruction of evidence. Once evidence is destroyed it becomes near impossible to retrieve them. Artifact wiping itself has multiple sub-categories such as disk cleaning utilities, file wiping utilities and disk degaussing/ destruction techniques. Disk cleaning utilities is basically a tool to overwrite existing data on hard disks. There are variety of techniques and tools which can be used in disk wiping. File wiping systems delete files from a operating system of a computer. File wiping utilities are much faster in their jobs than disk wiping and they also leave a much smaller signature than disk wiping utilities. Dis degaussing or destruction is a highly effective method. T generally involves applying a strong magnetic field to a device clearing it of all data. It is a known fact that anything good comes with a cost, this is literally the case with this method as it is very expensive to apply despite being highly effective and is hence not very widely used.

Hyper Formalisation-

However the problems do not stop with antiforensics. Another major problem in this field is that the bar has been set very high with little to no room for improvisation due to the standards and guidelines which are followed to the T. Even though it is often argued that different companies have different standards for digital evidence and so there is no set or defined standard or quality the evidence has to be, while this true the major problem lies elsewhere. The roble is that there are so many situations where the full evidence cannot be retrieved without modifying it slightly. In today's world digital crime uses multiple gigabytes and terabytes of data and critical systems which cant be taken offline for analysis because of which it is unrealistic to expect the digital forensic community to retrieve all of it without modification and it is also unrealistic to expect

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

them to seize all of the available data. Other common problems include the volatility of data and the fact that some digital media has only limited lifespan, limited bandwidth while transferring data during investigations has always been a recurring problem.However the organizational and guidelines often fail to address such situations and end up making wrong choices. This has been termed as hyper-formalisation.[2]

Lack of knowledge on multiple Operating systems and low standards of Research-

It is surely an advantage to the digital forensics community as the ability to deeply analyze digital artifacts has been developed. However this has caused another problem. Almost all of this knowledge is based on the Widows and Linux operating systems. This is due to the insane popularity of both of these operating systems especially Microsoft, to put it into context Microsoft market share is 87.56% of all shares, the mac os is 9.54% of the share and linux has 2.35%. Due to this the digital forensics community only focuses on these systems and forgets that there are a few more less popular ones.All applications on these operating systems such as Mozilla Firefox, Outlook etc. have been thoroughly studied and analyzed but people have forgotten about other systems such as ZFS and UFS along with countless other examples.

Another problem is the need to raise the bar for the standard of research in the digital forensics community. The problem until not so long ago was the fact that digital forensics was new to the world and the knowledge available on the subject was quite limited and many people didn't have much research experience on this topic. Computer science was always very famous like it is now. However real world digital training and cases is quite a bit harder and people writing research on this topic had to overcome huge volumes of learning and information. This lead to low standards of research in the community. Research papers on digital forensics are quite new and don't compare to the number of research papers in other fields. As time goes on journals and papers tend to be of higher quality as the readership and number of people writing it increase exponentially whilst the acceptance rate reduces forcing pepe to write papers of imperious quality, relevance and importance. This is definitely changing and evolving as time goes on but there is still room for significant improvement.

Cloud Computing-

Another thorn to the digital forensics community is cloud computing. 'Cloud' is a very common service used by people in the 21st century. It essentially allows you to backup data and access your data from anywhere as long as you are connected to the internet. Many cloud services have come up in the past decade or so such as google drive, i-cloud etc. Though cloud computing has had a profound benefit on your layman's life it has added a whole other layer of complexity to digital forensics.

Data stored on cloud is usually stored over a number of nodes unlike the common forensic situation where all the important data is stored on one device/system. Due to this distribution, crucial data can potentially exist across multiple places making the digital forensics procedure more time consuming and expensive.

Additionally the problem of CSP's(Cloud Service Providers) also arises. Investigators will start becoming dependent on CSP's for their cooperation in extracting and using their clients data. All CSP's are different from each other, They are different in terms of security levels, service level agreements which both a thorn in digital forensics growth. Cloud accounts are

usually made with very little information which makes identifying criminals and suspects in investigation near impossible. Anti-forensics techniques such as encryption are also very regularly used in cloud based crimes. Commonly used digital forensics tools such as Linux dd have proven to be insufficient in extracting data from cloud services. A research conducted Theti and Keane .shows that most forensics tools took a considerable amount of time to take 30 gigabytes of data from a cloud account.

Improvements of digital forensics in the recent past-

Another hurdle faced by the digital forensics community is IOT(Internet of things).[4] Internet of things refer to as every object or system which have technologies which enable them to connect to the internet. A research by Juniper research in march 2020 showed that there were 35 billion IOT devices in 2020 and this number is expected to increase to 83 billion in 2024[3] which is a increase in about 130% in just four years. IOT has a very good scope of becoming a arrow in the quiver of digital forensic analysts, however for now it remains a thorn. There is always less certainty from where the data came from. These devices also tend to have a limited memory which means the challenges in cloud forensics will also be applied for IOT devices. IOT devices also add to the complexity problem due to differences in operating systems etc.

CONCLUSION

This research paper was made to discuss the current problems with digital forensics and areas which should be improved on such as cloud computing and IOT devices. All these problems are thorns in the path of digital forensics and is making the whole analysis process a lot harder for the digital forensics community. What's more is that even though each of these problems are problematic enough on their own, when all of them are occurring at the same time the difficult compounds by multiple times. The ever increasing amounts of data consumption and usage arenot showing any sign of stopping. A research conducted by the telecom ministry in 2020 showed that Indians used 308 petabytes of data and the data consumption increased by 13% in short amount of time. This sort of increase in data consumption will soon lead ballooning in case volume which will only hamper the progress of this art even more. Unless these issues at hand are tackled with, digital forensics will be in serious trouble.

REFERENCES

- David Lillis, , Brett A. Becker, Tadhg O'Sullivan and Mark Scanlon,"Current Challenges and Future Research for Digital Forensic Investiation", Annual ADFSL Conference on Digital Forensic, Date accesed:May.24 2016[Online], Available:https://commons.erau.edu/cgi/viewcontent.cgi?article=1346&context=adfsl
- Nicole Beebe,Digital Forensic Research: The Good, The Bad, The Unaddressed", in Advances in digital forensics, Glbert Peterson, Sujeet Shenoi, Eds, Fifth IFIP WG 11.9 International Conference on Digital Forensics, Orlando, Florida, January 26-28, 2009, Available: https://link.springer.com/content/pdf/10.1007%2F978-3-642-04155-6_2.pdf
- Sam Smith, "IOT CONNECTIONS TO REACH 83 BILLION BY 2024, DRIVEN BY MATURING INDUSTRIAL USE CASES", Juniper Research,

https://www.juniperresearch.com/press/iot-connections-to-reach-83-bn-by-2024 (Accesed:31 mar 2020)

- "What is IOT?", Oracle India,https://www.oracle.com/in/internet-of-things/what-is-iot/#:~:text=The%20Internet%20of%20Things%20(IoT)%20describes%20the%20network%20of%20physical,and%20systems%20over%20the%20internet.&text=Oracle%20has%20a%20network%20of%20device%20partners.
- N.Theti and A.Keane, "Digital Forensics Investigations in the Cloud", 2014 IEEE International Advance Computing Conference (IACC), Gurgaon, Haryana, India, 21-22 Feb2014, Available:https://www.researchgate.net/publication/271547130_Digital_forensics_investigations_in_the_Cloud
- L.Cameron, "Future of Digital Forensics Faces Six Security Challenges in Fighting Borderless Cybercrime and Dark Web Tools", computer.org, https://www.computer.org/publications/tech-news/research/digital-forensics-security-challenges-cybercrime
- P.Callaghan, "Legal Lessons Learned: 5 Times Digital Evidence Was Denied In Court", Pagefreezer, https://blog.pagefreezer.com/legal-lessons-learned-5-times-digital-evidence-was-denied-in-court
- S.Ramasubramanian,"Cyber Crime Could Cost the World 1 Trillion Dollars in 2020, Says MCafee", The Hindu, https://www.thehindu.com/sci-tech/technology/cybercrime-could-cost-the-world-almost-1-trillion/article33269047.ece (December 07, 2020)