A Criminological Psychologybased Digital Forensic Investigative Framework.

Mr. Sameer Dasaka.
Institute of Forensic Science,
Gujarat Forensic Sciences University.
Email: dasaka.sameer@yahoo.com

Abstract: It's been more than 30 years since digital forensics came into existence and started to evolve. With the advancement of technology, criminals started committing crime and started taking leverage of it. Military officials and police officers in the United States first started finding the importance of digital forensics to catch the criminals and started adopting multiple investigative frameworks and strategies to improvise the investigation process. It was necessary for the Government, public and private sectors to take the responsibility to safeguard confidential information from various internal and external threats which were caused due to potential security vulnerabilities that were exploited in software applications. Since then, Digital Forensics played a major role in investigating the attacks occurred and bringing the criminal to justice.

Apart from performing the technical investigations, it is also equally important to understand and address the thought process of the criminal when the crime was committed. Every crime that has been committed is always done with a specific disastrous purpose in mind and to fulfil that purpose, the criminal finds multiple loopholes and builds his/her way to such an extent that the line between right and wrong gets negligible. Understanding what made the criminal think to commit the crime is just as important in producing future preventative measures.

This paper aimsto present and integrate a new existing module/phase titled 'cyber psychology' into the newly designed framework and to present a comprehensive overview of digital forensics, its importance,cyber law, and defineastep-by-step framework that can be used to assess the possibility of the crime by trying to understand the views, thoughts, intentions, actions and reactions of the criminals. Existing forensic frameworks and examples of data breaches and social engineering attacks will be analysed and then a

specific framework is created and elucidated.

Index Terms: Cybercrime, Cyber Law, Cyber Psychology, Digital Forensics, Digital Forensic Investigative Framework, Social Engineering.

1. Introduction

When the term 'Digital Forensics' comes into picture, one should understand that digital forensics is quite different from traditional forensic science and its investigations. 'Forensics' relates to the usage of scientific methods and techniques in investigating and extracting artefacts from the crime scene which can then be produced in the court of law as evidences to solve the crime. Digital Forensics is the art of using methods/techniques that are derived scientifically using advanced investigative methodologies and strategies.

According to DFRWS- 'Digital Forensic Research Workshop, USA-2001', *"The use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorised actions shown to be disruptive to planned operations"*.

According to Wikipedia- *"Digital Forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime"*.

The major aim or goal of digital forensic science and investigation is to find facts and events to recreate the crime scene. These are said to be known as 'remnants.' These remnants are then discovered and exposed which reveals the truth of an event.

Whenever we think about the Internet, we think about evolving technology; both hardware and software but we do not think about the psychological aspects of the human being which usually marks an impression and impacts our social interactions.

2. What is Criminological Psychology.

According to Wikipedia, "*Criminal Psychology, also referred to as criminological psychology, is the study of the views, thoughts, intentions, actions and so reactions of criminals and all that partakes in the criminal behaviour*". Criminology can be considered as a branch of sociology. It is the combination of both psychology and sociology.

3. Background

Since the last two decades, computer forensics has started playing an important role in identifying and prosecuting cyber criminals. Before researchers and computer scientists came up with a scientifically solid/sound digital forensic investigative framework, majority of the computer related crimes were left unsolved.One of the main reasons for having such cases unsolved are lack of maintaining a proper chain-of-custody, lack of quality based digital forensic tools, lack of proper financial resources, lack of proper evidence acquisitions and transmission, lack of proper training and hands-on and more.

Computer researchers and scholars have come up with multiple methodologies and frameworks which will help maintain maximum accuracy of the evidence analysed and output generated. One such process is where a legal duplicate copy of the device which contains the potential evidence is been made and then forensic analysis is performed on the copy of the original so as to ensure that the evidence integrity is not lost. Since then, many investigative frameworks have been designed and developed and most of them are following a definite set of instructions and guidelines to perform the forensic investigation on computers or any other electronic device.

After surveying previously developed frameworks, this paper will propose a nine-phase digital forensic investigative framework that can be followed scientifically and systematicallyto generate forensically sound evidence while also trying to understand the psychological aspects of the crime and the attacker. The framework is generated by combining existing forensic models and adding a new concept/phase into the existing framework and a new framework is designed and developed.

4. Branches of Digital Forensics

- Computer Forensics.
- Network Forensics.
- Embedded Forensics.
- Web Forensics.
- Social Networking Forensics.
- Satellite Forensics.
- Cyber Psychology and Forensics.
- Anti-Forensics etc.

5. Cyberpsychology

According to Wikipedia, “Cyberpsychology is the study of the human mind and behaviour and how the culture of technology, specifically, virtual reality, and social media affect them” The effect of the Internet and Cyberspace on the individuals and their mindsets is

dealt with cyberpsychology techniques.

6. **Locard's Exchange Principle and Forensic Psychology.**

According to the Police and Scientific Methods (1934), Locard's law states that "*Any action of an individual, and obviously the violent action constituting a crime, cannot occur without leaving a trace*".

Whenever a crime takes place, the criminals will always leave footprints behind which can be used by the investigator to solve the case. This, in terms of technology can be defined as the '*digital footprint*' left behind after a computer crime takes place.

The digital footprint that had been left behind by the intruder/attacker can possibly his/her sense the state of mind which can possibly lead to more pathways that can be explored in the crime scene and understand the crime better by the digital forensic investigator with the help of Forensic Psychologist.

Case Study -1:

Title: Ubiquiti Networks, 2015.

Description: The manufacturer of technology for networking has lost close to $40 million dollars in the year 2015 due to a 'phishing attack'. The hackers compromised an employee's email account and then used the technique of 'employee impersonation' to request fraudulent payments.

Case Study -2:

Title: TARGET, 2013

Description: In 2013, hackers gained access to almost 40 million customers payment information of TARGET. Hackers had been successful in installing a malware on a TARGET partnering company with the help of social engineering attack technique called 'phishing' which allowed them to access the network of the TARGET departmental store. Once after gaining the access, the hackers installed another malware on the TARGET systems to gain access to the credit and debit card information.

Case Study -3:

Title: RSA, 2011.

Description: A backdoor was made available to the hackers to enter into the systems of RSA by sending a fake email which contained a malicious program that gets executed when the attachment is opened.

Psychological Analysis & Breakdown:

According to the NetworkWorld, the psychological analysis behind

majority of the social engineering attacks are due to *'Fear'*, *'Obedience'*, *'Greed'* and '*helpfulness*'.

When we talk about **'Fear'**, it is important to understand that it is one of the unpleasant emotions that are caused by the belief that someone is going to do wrong or something is going to be wrong or is dangerous which will likely cause pain or threat. It is one of the most commonly manipulated emotion when it comes down to social engineering attacks and other cyber psychological entities.

Fake emails impersonating any financial entities or any important individuals, make a targeted recipient or a group to act quickly to avoid or rectify a threatening or painful situation.

For an example, a fake email impersonating a famous bank asking you to change your account password to 'ABCxyz1234' for security reasons or asking you to click on a link to safeguard the compromised account will force the individual to immediately act on it without a second thought.

'**Obedience'** can be defined as accepting an order, request from their respective superior at work or at other professional or personal acquaintance's.

Example, fake instant message, fake phone call or fake email from a person or group of superior authority might make an individual complete the task without verifying the authenticity of the mail.

'Greed' can be defined as an intense and selfish desire for something, especially wealth or power.

'**Helpfulness**' is defined as the willingness to help other individuals.

Case Study -4:

Title: Investigation and Analysis of a Reported Incident Resulting in an Actual Airline Hijacking due to Fanatical and Engrossed VR State.

Case Study -5:

Title: RTI Campaigner imprisoned for 6-years in Puri Cyber Pornography case.

Source: The Times of India.

Highlights: Person named 'Jayant Kumar Das' was arrested by the Baselisahi police in the year 2012 for uploading obscene remarks against a journalist's wife on a porn site.

Das wanted to take revenge on journalist for exposing his illegal money lending business and hence defamed the journalist's wife and also posted her personal mobile number on the porn websites.

Crime branch indicted Das under the following sections:

- Section 292 (Obscenity)
- Section 465 (Forgery)
- Section 469 (Forgery for the purpose of harming reputation)
- Section 500 (Punishment for defamation) of IPC and 66C/67/67A of the Information Technology Act.

Psychological Analysis &Breakdown:

In the police investigation, it was confirmed that Jayant had created a forged e-mail account and a fake profile in the name of the journalist's wife and linked it to a porn website. The digital footprint Jayant left behind was the IP address through which the fake email account was created, and the police was able to nab him.

The same IP address was also used by the Jayant to possess an illegal firearm that was registered at one of the police stations in Puri. Here, the digital footprint that was left behind was the original IP address of the individual.

Jayant has taken a step out of anger, pain and humiliation when his illegal business was exposed by the journalist and hence decided to defame and expose the journalist wife without having a second thought of committing another mistake.
(Having accepted this in the court of law)

Pain alone is usually not enough to cause anger in a person. Anger occurs when the pain is combined with a thought that provokes and triggers anger in an individual. These thoughts usually include evaluations, interpretations of situations, self-assumptions, personal assessments and more.

Being angry feels better than being in pain. One of the primary factors that makes it easy for the attacker or the intruder is that changing their mindset from pain to anger consciously or unconsciously, helps them distract themselves and helps them focus on doing harm to the other person.

7. **The Relationship between Psychology and LAW**

According to Prof Craig Haney of University of California, Santa Cruz suggested that there are three primary ways in which psychology and law can be related to each other. They are as follows:

- Psychology and the law
- Psychology in the law
- Psychology of the law.

Psychology and the law:

As per Bartol & Bartol, 1994, p.2, psychology and law are viewed as two separate disciplines. ***The model here which we follow is examination and analysis of the legal system or different components of the law in a psychological perspective.***

Usually, assumptions that are made by the law and psychology are examined. Questions/doubts such as:

- Will the interrogation process or any of its techniques make the eyewitness or any other individual to give false confessions?
  Example: *The offender might make a false confession saying that some other person has forced him/her to commit the crime.*
- Will the offender be violent when released from the prison?
- Is eyewitness accurate at the first place? And more.

Answers to such questions are usually elucidated to the court of law or the judge by the forensic psychologists.

Psychology in the Law

As the title indicates, *'psychology in the law' involves the usage of psychological theories/knowledge in the lawful structure/organization.*

Example: Consider police have nabbed the offender who hacked into highly confidential server and downloaded information without authentication. But, the offender claims that he/she is innocent and pleads guilty. Based on a forensic psychologist knowledge, understanding of psychological research and experience, the investigator can be able to conclude that the offender is saying the truth or not.

With the help of forensic psychology in digital forensics and while investigating cyber related crimes, the forensic psychologist can be able to extract confessions based on various psychological principles and techniques.

8. **Psychological Theories of Crime and Digital Forensics.**

According to *Eysenck's (1964) biosocial theory of crime*,it is believed that some individuals are born with cortical and autonomic nervous systems which influence their ability to learn from their consequences of their behaviour, especially, the negative consequences that are experienced in their childhood. At times, such individuals exhibit strong antisocial inclinations that may give them patience and ability to carry out long term cyber-attacks such as advanced persistent threat attacks (APT's).

While interrogating an individual, after the digital forensic investigation and analysis is complete, it is necessary and important to know if that individual is exhibiting such high levels of extraversion and neuroticism so as to understand if there is any possibility that the offender might again try to target and attack another individual/organisation or entity once he/she gets out of the prison.

9. 'Social Engineering is Psychology'

With emerging technology, there is also exceptional growth of security vulnerabilities and loopholes. With many potential things available to exploit, hackers chose social engineering attacks as the root of hacking. This is important because, the attacker not only needs to understand how we work as individual's but also how we work as individuals within a society and social environment. With the understanding of such, attackers plan advanced persistent threats to commit the crime which is usually successful.

Usually when cyberattacks (social engineering attacks) take place, the attacker is often trying to get the something important and valuable or is trying to put the user away from accessing that important source of information, returning it in exchange for money.

For an example: Ransomware. The attacker will lock all the users essential and important files and will demand a ransom to unlock them or might threaten to delete the information resulting in a psychological trigger to pay the amount without a second thought.

10. Psychology behind Insider Attacks.

It is always important to know how a technologically sound individual is looking forward to malicious activities. Basically, it would be necessary for the forensic psychologies or the clinical psychologist to understand the childhood of the offender. Typically, scary and hurtful childhood experiences, dominations, opportunity to steal confidential information, thrill when not being caught, and many other factors lead to an employee turning against his/her employer. Such an exposure in people's childhood might trigger and lead to a stress spiral which might ultimately cause an individual to feel underprivileged and open to such malicious opportunities.

At times, depending upon the offender's mindset, such malicious intent can lead to insider attacks to damage a company's asset, gain financial access, cover an error, to prove a point, damage reputation and more.

Kevin Mitnick stated that ***"Cyber-security is about people, processes and technology, and organisations need to bolster the weakest link - which invariably is the human element. It does not matter what security software you have installed, because it just takes one person in the targeted organisation to make a bad business decision, and "it's game over"***

11. The Hacker's Mind

According to a study conducted by the psychologists at Danube University suggests that the hacker's mind is quite similar or identical to a burglar whose main intentions are identity theft and unauthorised information access. It is typically hard to access and cyberprofile the psychological state of a hacker as there are many different types of hackers with various motivations behind their actions.

12. Proposed Framework

In this section, a new digital forensic framework will be proposed. The aim of this section is to add a new module/investigation process into the existing framework to make it a complete framework ideally designed to investigate potentially important phase of criminal psychology in cybercrimes which would make the investigation processsimpler and more efficient.

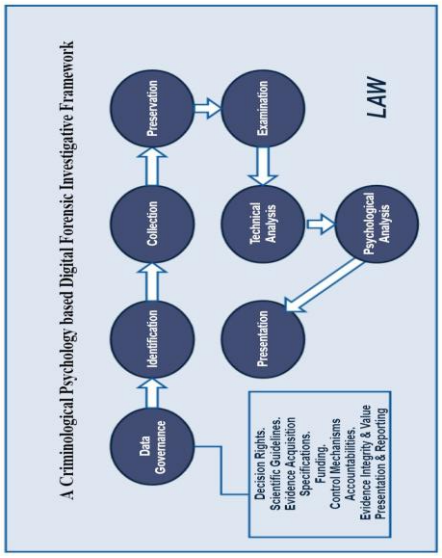

Figure 1- A criminological psychology based Digital Forensic Investigative Framework

13. Data Governance in Digital Evidence Acquisition.

Data Governance in digital forensics can be referred to as a data management concept which enables the ability to ensure that high quality of data exists throughout the data acquisition life cycle which ensures that when processed, the integrity of the evidence is nowhere tampered or manipulated in any of the digital forensic investigation phases like identification, collection, preservation, examination, technical analysis, psychological analysis and presentation.

In Data Governance, the following requirements are to be addressed.

- Why is it required to conduct the digital forensic investigation in the first place?

- What is the list of areas that are to be focused? Is it for standalone systems & entry-point forensics, mobile forensics, network forensics, embedded forensics, social networking forensics, web forensics, malware forensics and research, anti-forensics andmore.
- Is proper financial support and technical resources available to perform the digital forensic investigation?
- List of scientific guidelines, rules and regulations to be followed.
- Who will be taking informed decisions and establishing decision rights?
- Integrating data governance into technology and forensics.
- What are the accountabilities?
- A systematic process for control mechanisms.
- Specifying evidence acquisition requirements, scientific methods and processes.
- Collaborating technical analysis and psychological aspects of forensic investigation.
- Measuring and reporting evidence value.
-

14. **Digital Evidences**.

Each and every bit of data/information that is being stored or transmitted is in the form of 0's and 1's i.e Binary format. It can be found on a computer hard drive, smart phones, pagers, camera and lot more. This kind of format is what the court relies upon. Digital evidence is usually associated with electronic crime such as credit card frauds, hacking, child pornography and more.

15. **Investigative framework by Altheide and Carvey**

Altheide and Carvey mentioned in their book named "Digital Forensics with Open Source Tools" that the process of Digital Forensics can be broken down into three categories. They are as follows:

• Acquisition.

• Analysis.

• Presentation.

Acquisition:

The process of collecting digital media/evidence (while relating to digital forensics) from digital devices which has to be later examined is said to be known as Acquisition.

Different types of devices from where evidence can be gathered are:

• Physical hard drives.

• Pen drives.

• Storage cards.

• Digital cameras.

• Optical media.

• Embedded devices and chip sets.

• Document files and more.

It is important for the digital forensic investigator to understand that evidence collected is very sensitive and delicate in nature and has to be preserved. It is always important to maintain a duplicate copy of the original which is also called as the working copy.

16. **Technical Analysis:**

This part of analysis refers to the process of examining the acquired data where identification and interpretation of the evidence is carried out. First, the area of interest such as a file, document, image, video, logs, statistical analysis etc is identified in the data and then filters them. Next, interpretation is done of the extracted artefacts and are subjected to further scientific analysis.

17. **Psychological Analysis:**

Psychological Analysis in digital forensics plays a very important role. There are many questions that needs to be addressed in order to give accurate judgement by the court of law while taking into the behavioural and psychological conditions of the offender into consideration.

Few sample psychological situations that need to be addressed are:

- ***Victim being hypnotized by the influencer to do the crime.***
- ***Victim might have been forced to commit the crime else leading to life threatening consequences by the criminal.***
- ***Victim might have been under the influence of the influencer to commit the crime.***
- ***Victim might have been under emotional influence by the influencer to commit the crime.***
- ***Victim might have been under the 'belief influence' by the influencer to commit the crime.***
- ***Victim might have been influenced by 'something' to commit the crime.***
- ***Self-hypnotization leading to criminal activity.***

18. **Presentation**

Presentation refers to the process by which the digital forensic investigator will share the outcome

of their investigations and analysis to the court of law or other legally interested parties. This process consists of important actions and initiatives taken by the investigator such as artefacts discovered, analysis on the extracted artefacts, meaning of the artefacts and more.

19. **Cyber Laws- I.T Act 2008 Amendment.**

- Section 43(a)- Unauthorised Access.
- Section 43(b)- Unauthorised downloading, copying or extraction.
- Section 43(c)- Spread of computer virus, worm or contaminant.
- Section 43(d)- Damaging a computer.
- Section 43(e)- Disruption of a computer.
- Section 43(f)- Denial of Service.
- Section 43(g)- Facilitating unauthorised access.
- Section 43(i)- Destruction, deletion or alteration.
- Section 43(j)- Source code theft.

For all the above listed sections penalty or compensation is done and no arrests are usually made.

Criminal Offences under the I.T Act

- Section 65- Tampering with computer source documents.
- Section 66- computer related offences.
- Section 66A- Sending offensive messages.
- Section 66B- Dishonestly receiving a stolen system.
- Section 66C- Identity theft.
- Section 66D- Cheating by personation.
- Section 66E- Violation of Privacy.
- Section 66F- Cyber Terrorism.
- Section 67- Transmitting obscene electronic material.
- Section 67A- Electronic material with Sexually explicit act.
- Section 67B- Child Pornography.
- Section 67C- Preserving or retention of information by intermediaries.
- Section 72- Breach of confidentiality or privacy.

Now, it is necessary to conduct more research and add more sections to the I.T Act 2008 where computer crime and behaviour Analysis can integrate together to give a better judgement.

20. **Conclusion**

Behavioural Analysis and assessment of the psychological state of the offender will help understand the root cause of the crime and will help the court of law to make important decisions. Such

analysis will help identify individuals who are innocent, individuals who are forced or threatened to commit the crime and lot more. Such information will always help identify the main culprit instead of some innocent victim being punished by the court. More research scope is included in this paper in the domain of Cyber laws.

This paper has designed and developed an initial version of psychological analysis based digital forensic framework that will help establish important links, connections and solve the case more efficiently.

21. References

- A Synopsis on Digital Forensics and its Investigative Strategies by Mr. Sameer Dasaka, International Journal of Advanced Research in Computer Engineering and Technology. http://ijarcet.org/?page_id=6029

- Investigation and Analysis of a Reported Incident Resulting in an Actual Airline Hijacking due to a fanatical and engrossed VR State by Atsushi Ichimura[1], Isao nakajima[2], Muhammed Athar Sadiq[3], Hiroshi Juzoji[4]. https://cyberpsychology.eu/article/view/4202/3243

- https://searchdatamanagement.techtarget.com/definition/data-governance

- https://www.mentalhelp.net/articles/psychology-of-anger/

- Altheide, Cory; Carvey, Harlan (2011-04-28). Digital Forensics with Open Source Tools: Cory Altheide, Harlan Carvey: 9781597495868: Amazon.com: Books. ISBN 978-1597495868

- CERIAS: Digital Forensics Resources. http://www.cerias.purdue.edu/research/forensics/resources.php?output=printable

- Lillis, D., Becker, B., O'Sullivan, T. and Scanlon, M., 2016. Current Challenges and Future Research Areas for Digital Forensic Investigation. In Proceedings of 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Daytona Beach, Florida, USA, pp. 9-20.

- Robbins, Judd. An Explanation of Computer

Forensics. http://www.computerforensics.net/forensics.htm

- Nolan, Richard, et. al. Forensics Guide to Incident Response for Technical Staff.http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf

- Ghosh, Ajoy. Guidelines for the Management of IT Evidence. http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

- https://www.us-cert.gov/sites/default/files/publications/forensics.pdf

- Computer-Forensik Hacks: Amazon.de: Lorenz Kuhlee, Victor Völzow: Bücher. 2009-09-09. ASIN 3868991212

- Vömel, Stefan; Freiling, Felix C. (2011-07-31). "A survey of main memory acquisition and analysis techniques for the windows operating system" (PDF). Digital Investigation. 8:322.doi:10.1016/j.diin.2011.06.002

- https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1777&context=jclc

- https://en.wikipedia.org/wiki/Data_governance
- http://www.datagovernance.com/the-dgi-framework/

- https://timesofindia.indiatimes.com/city/bhubaneswar/rti-campaigner-gets-6-year-imprisonment-in-puri-cyber-pornography-case/articleshow/59917436.cms

- https://catalogue.pearsoned.co.uk/assets/hip/gb/hip_gb_pearsonhighered/samplechapter/0205949932.pdf

- https://securereading.com/digital-forensics/

- http://blog.wallix.com/the-psychology-of-the-cyber-criminal

- http://mo.co.za/open/dfframe.pdf

- https://www.digitalforensics.com/blog/the-basic-of-social-engineering/

- https://gatefy.com/posts/7-real-and-famous-cases-social-

engineering-attacks/

- https://www.networkworld.com/article/3070455/cloud security/hacker-psychology-understanding-the-4-emotions-of-social-engineering.html
- https://blog.avast.com/psychology-of-cybercrime.
- http://www.cyberlawsindia.net