NANOTECHNOLOGY AND CYBER CRIMINALISTICS

Written by Ratnesh Shah

5th Year Student of B.Com LLB, Institute of Law, Nirma University

INTRODUCTION

Cybercrime is also known as a web crime; it is the use of a gadget (such as computer, smartphones, tablets, etc.) as a tool in using illegal acts. Committing fraud actions, Pornography, Child trafficking, stealing other peoples' identity or it may be violating privacy, intellectual property and all other forms of illegal acts.

Cyber criminalistics had developed fast over the months and years primarily through the use of the internet the computer has become the inside knowledge for entertainment. Commerce or even government because of the fast pacing adoption of the equipment and other gadgets of the people has caused so many cybercrimes. Cyber-crime involves a breach of contracts; it may be personal or corporate policies. Assaults on one's integrity and information, blackmailing also falls in cybercrimes. In the midst of lying transaction based acts such as fraud, human/ child trafficking, pornography falls in Cybercrime.

Another type or form is the involvement or attempts or disrupting the actual acts over the internet. Including spam, fraud, service attacks, that is present on the web thus resulting in rapid growth of Cyber Criminalities. Cybercrimes can affect both the real body and the inner self. But it has a different effect on ones' personality. The most common cybercrime anywhere in the world is the identity theft. It is where someone copies the identity of the other. Copying the ID, e.g., Social Identification the most common identification that reproduced because the Social Security has long been identified as legal identification because it represents as tax identification id. Many institutions also use Social Identification to keep them tracked or connected to their employees.

Journal of Legal Studies and Research
Volume 3 Issue 5
ISSN: 2455 2437 (India)
Published by 'The Law Brigade Publishers', A Libertatem Media Group Company

There is also the credit card information of ones' hard earned money most like to pay even if they did not do the purchasing themselves so as the big lending companies handling the credit card accounts are most likely to suffer from a very bulgy loss. Stolen or misplaced credit cards can be used by cybercriminals to steal ones' identity. These are examples of what cybercrime is all about. Nanotechnology is the branch of Technology that deals with dimensions and individual molecules and atoms. Criminalistics is another word for "forensic science," it is the scientific principles of pieces of evidence in criminal cases, it is an experimental technique to the crime. Thus, nanotechnology and cyber criminalistics is the study or detection, analysis, interpretation, identification, to recognize and identify physical evidence especially in criminal cases. Every detail from visible ones to the tiniest details that a one could get.

CRIMES AND ITS PROCESS

- **Identity theft** – is the most common fast pace of cybercrime activity, Social Security Identification has always been the hot target hackers.
- **Internet Fraud** – fraudulent have been using different technique, and different kinds of sweet and too enticing offers that one could hardly ignore. Like an interest of 5x the investment, or gold mines, in a form of an asset to be sold in a small amount. That some people would be caught in their bait. Always remember “If it’s too good to be true, it is probably a fraud”
- **ATM Fraud** – criminals have the ability to set-up machine that looks exactly like an automated teller machine (ATM), the purpose of which is not dispensing money but taking information’s of the ATM owner especially the PIN of the card. ATM fraud has become a worldwide problem.
- **Wire Fraud** – example of wire fraud is a telephone conversation being recorded by the third party. Scammers sometimes introduce themselves as an agent to any business account and mostly seeking for your personal information in terms of telemarketing fraud. Most of

the scammers uses the internet to go "phishing" (an of sending email alerts to many people containing enticing stories and end up by requesting the person's personal identification.

- **File Sharing and Piracy**- is an act of duplicating copyrighted materials such as movies, DVD, music, data compression, etc. A scammer burns DVD and make copies for selling, (P2P) person-to-person file sharing over the internet is also considered as cybercrime. anything that is owned by someone and copied from the internet for personal copy or even for selling is not allowed thus it is considered as cybercrime.
- **Counterfeiting and Forgery** – is an act of reproduction and copying of signatures or documents. Plagiarism falls on this category.
- **Child Pornography –** is engaging sexual behavior boy or girl of ages 18 and below and is shown with the use of devices and internet is called child pornography, it has a wide range of market all over the internet and most customers are pedophiles, it's so sad that most victims here are the innocent ones, who could have been playing on the street enjoying childhood rather than being "on-sale" doing sexual acts in exchange of money. This cybercrime is rapidly rising in countries were cybercrime law has not yet been focused by the government, one is in some areas of Southeast Asia. Child pornography believed to be a multibillion-dollar business.
- **Hacking** – is one of the biggest problem the world is facing right now, everybody can be a victim from private person, celebrity, public servant, small businesses to big corporation, or even the whole system of government is possible for hacking. Everybody can become a victim of this type of cybercrime, this is rolled into one as to abovementioned types of cybercrime. Stealing personal identification, cloning ones' personality, video uploads, and so on.
- **Computer Viruses** – it is an act of damaging programs of the computer system. Some of most harmful bugs were produced or programs as diverse location are Philippines, Bulgaria, Pakistan, The United States of America. The intentional release of computer viruses is another form of cybercrime.

Nanotechnology as the forensic tool for a rapidly innovating technology

Criminalistics frequently the puzzle solver of the case. There are lots of field of specialization of forensics, Fingerprint identification/ analysis, identifying of firearms, lie detector, toxicology, examination of documents, DNAs to name a few[1].

Fingerprint reading

A fingerprint is a form of lines or ridge that form a pattern or design on a person's thumb or fingertips. The fingerprint built while being conceived in the womb of the mother about 3-4 months. The composition of the end joints of the fingertips is made up with the papillary ridge. Papillary ridge is sometimes called friction ridge or epidermal ridge. The furrows are the downing of canals between the seams or the gaps.

There are two kinds of fingerprint analysis one is the **real impression**, and the other is a **chance impression**. The actual idea is made with the use of any printing materials, while the **chance impression** is an impression taken of chances which means taken unintentionally to produce the print. There are some ways on how to take real fingerprint analysis. One is rolling of fingertips; it is commonly called as "thumb mark" the way how to print the thumb is you turn your thumb away from the center to the body of the subject.

Another one is clear impression it is the opposite side, meaning printing without rolling the thumb or fingers.

A chance impression is sometimes visible or unclear print. It is visible when the print has no chemical treatment; Latent print impression when t print is invisible, but it became noticeable when some substances have applied.

There are three characteristics of fingerprints:

[1] https://www.britannica.com/topic/cybercrime [Cybercrime]

1. The individuality – there is no lookalike fingerprint, never had it recorded that two individuals have the same fingerprint.
2. Permanency – the uniqueness of every detail of the ridges never change.
3. Infallibility – reliable fingerprint evidence.

The outer part of the skin of the fingers are called "epidermis, " and the inner scarf is called "dermis" in case of temporary impairment the external component reverts to its natural aligning nevertheless the ridge will remain the same. But, if the thin inner skin will be broken or destroyed it will never get back to the way it is before.

1. When I fingerprint a warrant an evidence warrant conviction?

The evidence of the fingerprint must have found at the crime scene which they could acknowledge the time and when the subject did the crime. Otherwise, it would be impossible for a suspect to commit the crime of the subjects' fingerprint haven't recognized in the crime scene.

2. How are latent impressions analyzed?

They are made by human perspiration on the top of the ridge on a thumb or fingers.

3. What was the first Appellate court to submit the admissibility of the fingerprints?

In Illinois Court, the case was People vs. Jennings, the very first Appellate Court to pass the admission of the fingerprint as evidence.

4. Is Fingerprint image sufficient enough for conviction support?

In the case of State vs. Conner's, the court supported the photograph showing the fingerprint upon the judge without producing the post.

5. What are the different patterns of fingerprints?
    a. Arch (5.0%) – the understandable arc is the most common to all fingerprint patterns, it is a form of ridge entering from one side to another side most commonly known as "Thumb-mark."
    b. Loops (65%) – is a type of pattern of ridges are studied whether recurve, imaginary lines, pass, or touch they tend to exit the same ridge entry which is common to three general models and sub-divided into two distinctive groups. The ulnar and the radial.

The ulnar is the point where the flow is in the direction of the little finger while the radial is where it flows towards the course of the thumb.

c. Whorl (50%) – is the 2nd most common fingerprint pattern used for investigative reports, they are sub-divided into four parts into 4. The Distinct Group; the Accidental Group; the Double loop; and the Central/ Plain Pocket Loop.

DNA on forensics

DNA is the process of determining individuality of DNA characteristics. Fingerprinting, testing and DNA typing falls under the individuality training of DNA profiling. As mention earlier fingerprinting is one of the best uniqueness of individuals, thus no one has precisely the same ridge as the other.

DNA profiling is the most common process applied by forensic experts, the four nitrogen base found are Guanine, Thymine, Adenine and Cytosine each of these components represents the beginning capitalized the letter. I.e., "A" for **adenine**, "T" for **thymine** and so **on**. Two **mixe**d components are namely:

adenine + *guanine* = **purines**

thymine + *cytosine* = **pyrimidines**

The interactions with proteins can be unspecified; it can bind to a single specific DNA sequence. Proteins can bind to DNA and enzymes, the polymerases that copy the DNA base sequence transcription and DNA replication are both extremely important. Forensic DNA examination was in 1984[2].

[2] https://en.wikipedia.org/wiki/DNA

CYBERCRIME AND NANOTECHNOLOGY

Nanotechnology will increasingly impact cyberspace by the late teen years, and in trying to gain the most advantage possible from its use, new security gaps (which could turn into nightmares i f not handled carefully) will emerge. For example, as data nano bots are implanted in the brain of users (later organic bots will become an integral part of the individual), special attention will have to be paid to providing advanced firewalls to keep intruders from cracking into the bots and terrorizing the recipient. Could there be a more frightening crime than having your brain - stored knowledge erased or scrambled, or hearing voices threatening to destroy your memory unless you pay extravagant blackmail — mind stalking?[3] Nanotechnology is beginning of an impact of handling of evidence at crime scenes, its study in the laboratory and its demonstration in the courtroom. Application of nanotechnology is likely to develop the capacity of materials and soil, forensic evidence in tissue, toxic substances and more.

Nanotechnology plays a valuable and powerful tool in most of the areas including forensics. It is a rapidly growing region of research with a huge potential in a forensic filed of expertise, running from forensic laboratories and production and forensic science. Nanotechnology has a vital role in making significantly positive contribution in forensic science in Crime detection. In forensic nanotechnology, minute chip tools are used instead of volume instruments, that reduces the method of examination to make investigation firm and precise, accurate, appropriate, and timely. This topic aims to focus on some of the applications of Nanotechnology in Forensic Science.

Nano-forensics is an entirely new area of criminalistics associated with the development of Nanosensors, the Nanotechnical procedure for actual crime scene investigation and terrorist activity investigations, resolving the presence of explosive gases, biological agents, and residues. Forensic Science is a wide range in the field of subspecialties which use expertise adapted from the natural sciences to acquire criminal or other legal evidence.[4]

[3] http://sciences.ucf.edu/fwg/wp-content/uploads/sites/157/2016/11/FWGV5-11-04-2010.pdf
[4] https://www.rroij.com/open-access/nanotechnology-in-forensics-and-its-application-in-forensic-investigation-.php?aid=82204_[nanotechnology in Forensics and its application in Forensic Investigation]

In its look for speed and potency on the online, networks can grow in size and scope. for instance, a network together with all branches of an outsized bank becomes a bigger net once many banks merge and bigger still once all banks in a very region be part of to cut back prices and speed service delivery. Then a national banking web emerges and is before long replaced by a international and eventually a worldwide web. Whereas information superhighway becomes additional powerful as it grows, it additionally becomes additional prone to attack. A closure of a regional web would produce disturbance, however the slack may well be picked up by different nets. However, if the worldwide web is closed, true chaos ensues, leaving banks/customers at the mercy of blackmailers/extortionists/terrorists. Thus, the larger the networks (e.g., energy, medical, education; regional, international, worldwide), the additional essential security becomes. On the opposite hand, several might even see a bigger threat evolving from the powerful technology obtainable to thwart crime and, indeed, all criminal activity. Authorities have long same, ―If you have got nothing to cover, you've got nothing to fear‖ once talking regarding authoritarianism police investigation capabilities. it'd appear that theory are well tested by the evolving technology of consecutive few years, as all activity are seen and recorded and prepared for retrieval and prosecution and so development of preventive ways. will we actually need to measure in a very society wherever law is supreme, while not recourse, and mistakes don't seem to be allowed, wherever ―the record‖ is case in point and there's no place for bargaining or mediation/arbitration. Have we tend to evolved to the present level of ―perfection[5].

CONCLUSION

Nanotechnology is beginning of an impact of handling of evidence at crime scenes, its study in the laboratory and its demonstration in the courtroom. Application of nanotechnology is likely to develop the capacity of materials and soil, forensic evidence in tissue, toxic substances and more.

[55] http://sciences.ucf.edu/fwg/wp-content/uploads/sites/157/2016/11/FWGV5-11-04-2010.pdf

Nanotechnology plays a valuable and powerful tool in most of the areas including forensics. It is a rapidly growing region of research with a huge potential in a forensic filed of expertise, running from forensic laboratories and production and forensic science. Nanotechnology has a vital role in making significantly positive contribution in forensic science in Crime detection. In forensic nanotechnology, minute chip tools are used instead of volume instruments, that reduces the method of examination to make investigation firm and precise, accurate, appropriate, and timely. This topic aims to focus on some of the applications of Nanotechnology in Forensic Science.

Nano-forensics is an entirely new area of criminalistics associated with the development of Nanosensors, the Nanotechnical procedure for actual crime scene investigation and terrorist activity investigations, resolving the presence of explosive gases, biological agents, and residues. Forensic Science is a wide range in the field of subspecialties which use expertise adapted from the natural sciences to acquire criminal or other legal evidence.

The future path through Internet is full of threats and opportunities, most of that cannot even be fanciful at now. With 5,000 years of technological progress expected between 2100 and 2125, it‘s troublesome to forecast the dilemmas that lie ahead, however due to the creative thinking and genius of William Gibson, Ray Kurzweil, et al like them, some predictions are created and might be used as a base for AN examination of future crime and crime fighting. the web as we all know it—computers, websites, email, blogs, commerce, etc.—may be obsolete as presently as the early years of following decade once a seamless, wireless network of mobile signals received directly by transmitters within the possession of people and nano bots planted within the bodies of people handle all communication. At this time, cyber offenses can become terribly personal, as AN attack on the net may be a direct attack on the user—possibly even incursive his brain and memory keep in neural networks. As nanoscience advances to the purpose that bots within the atmosphere capture and record all spoken and physical activity, the selection can evolve: tightly management all human interaction by holding people liable for each deed and action (each of that is supported by for good keep evidence) during a with efficiency networked worldwide net or enable creative thinking and individualism to emerge by refusing to line boundaries and jurisdictions on the

web, deed it very much like it's today—without management or social control. the previous would curtail crime and create the net a secure vehicle for communication, socialization, commerce, etc., however at a considerable price to privacy, freedom of speech, and alternative civil liberties. The latter would enable a free flow of data and exchange of products and services while not government interference, however with a considerable threat to the economic and social lives of peopleand society itself posed by cyber offenders. By 2025, it's probably the entire thought of the web and crime is also passé—part of the trash barrel of history. the best threat then could be the acute problem of separating virtual (cyber) reality from physical reality. Already psychologists warn that perception is additional vital than truth; so, if cyber reality is additional convincing than physical reality, will the virtual world become the ―reall world?