The Kolkata
PROTECTOR
JULY - AUGUST 2018 Rs. 50/-
NEW MEDIA
www.theprotector.in
A Magazine for the Kolkata Police
PROMOTING PEACE

MARCHING AHEAD IN UNISON

KOLKATA POLICE - WITH YOU ALWAYS

Name: Ummed Meel
Designation: Cyber Expert (Police and Defence Trainer)
Bio:
Education: B Tech (ECE), CEH (EC-Council), Diploma in Cyber Law, LLB (Pursuing)

Ummed is closely associated with police, Air Force, Army and higher defence authorities in India from 5+ years (India's Youngest Police and IPS trainer).

Ummed has conducted 50+ trainings and workshops for Indian Police of Delhi, Uttar Pradesh, Rajasthan, Haryana and Himachal police etc and trained more than 8,000 police officers and other LEA's officers including Air force and defence ministries.

He has also conducted 70+ seminars for government/ non-government organizations, school, colleges and other law enforcement agencies on Cyber Crime awareness.

He has simultaneously investigated 200+ major cybercrime cases for the Indian police.

Ummed has been interviewed by several news channels, newspapers and magazines for Cyber Crime Safety.

Ummed has 5+ years of experience in Cyber Security, Cybercrime investigation, Digital Evidence seizure Digital Forensics and Vulnerability Assessment.

DIGITAL FORENSICS: COMBATING CYBERCRIMES

Digital Forensics

Digital forensics science is the application of forensic science that is able to generate admissible evidence during the criminal investigation. Digital forensics science includes the collection, preservation and analysis of the digital evidence. Digital evidence is the backbone of the cyber-criminal investigation. Cyber-crime can either be committed by using electronic devices or committed to hack or damage electronic devices.

Before 2000, cyber-crime was investigated by the general law system keeping it under the Economic Offenses Wing. In 2000, the IT Act was created keeping in mind the increasing use of computers and computer crimes. In the IT Act, any crime that is committed by stealing data from computers, computer resources, and computer networks or using these resources, it comes under the category of cyber-crime.

Digital forensics is not only confined to the court but is at times used to solve internal issues in private companies, such as violating corporate policy, which is not necessary to drag into the "crime" category. In our daily life, digital forensics is also used to retrieve accidentally deleted data from mobile phones, computers or any other electronic device.

Digital evidence seizure and preservation

During the seizure of the digital evidence in course of the cyber-crime investigation, the seizure procedure involves several precautions that are required to be taken in addition to the care taken during the seizure of conventional articles. Digital forensics plays an important role in detecting cyber-crimes, investigating and convicting the culprit.

Seizure methods for various electronic devices are also different like mobile phones should be seized in the faraday bag to keep them away from radio waves. As soon as the Incident Response Team goes to the cyber incident site, computer systems and computer resources must first be removed from power and data connectivity since the connection of devices with internet becomes a network hub, the problem for the investigating officer increases. Digital evidence is very sensitive. While seizure of digital evidence; casual or slight negligence is enough to contaminate it. Nobody can actually recover the tampering and that evidence is not even admissible in the court of law.

Investigation of cyber-crime cases

With the help of digital forensics, it has become easy to investigate big crimes such as copyright, privacy, cyber bullying, cyber stalking, child pornography, harassment and online bank fraud and convict the culprit. Cyber hazards approaching the defence department or other government web servers to gather cyber intelligence can be detected in advance with the help of digital forensics. With the help of memory investigation, we can extract the details of recent work done on computers such as incoming and outgoing data, running services, hidden processes, malware, bots, created files, watched videos and movies etc.

Digital forensics has been divided into many parts according to the technical checks system; computer forensics, network forensics, mobile forensics etc. Information such as the name of the sender and recipient of the information, the device connected to the computer system, internet service used and physical location etc. can be precisely detected by the digital evidence.

After the release of evidence, the investigating officer should calculate the value of the evidence at forensic science lab that keeps its integrity and authenticity intact. In the case of cyber-crime Investigation, digital evidence cannot be examined directly. For this, the investigating officer should have to first create a forensic image of the evidence such as a hard disk, pen drive etc. After that, the investigation may be carried out on an image of the evidence.

Hurdles

Today, in the era of technology, use of electronic devices such as mobile phones, computers, etc. are increasing rapidly. Digital devices not only make our life easy but also create a big market for cheaters and criminals. The investigation becomes quite complex when it involves electronic devices.

It is necessary to seize all the digital proofs used in any crime, but if there is a bank, finance, CCTV recorder or email server etc. (which is in the production environment) in cyber-crime, then the police usually do not get them seized. On many occasions, it is very difficult to present the entire computer server as evidence in the court. For example, we cannot bring the entire bank server to the court to discuss any case related to bank frauds. According to the 65 B of IT Act 2000, you can submit only a small part of any digital evidence to the court as evidence. In this case, you need to take that small information along with the form 65 B that should be signed by either network admin or owner of digital infrastructure.

Data encryption is the biggest problem in the cyber-crime investigation. It is also difficult to remove a password from a mobile phone and computer that was built in the form of data security. Many social media websites remove Metadata from the uploaded file so that the forensics team are not able to find information from photos, videos or documents like date of creation, date of modification, device name, and place, etc.

In many cases, nowadays it is found that cybercriminals send the earned capital to any foreign bank account or website, in which case the Indian Law Enforcement Agency faces problems to gather evidence and information. Sometimes foreign banks clearly deny sharing of any information with the Indian police agencies. In that case, the investigating officer should approach it with the LR method via Interpol agencies of the respective countries.

Nowadays the main problem for LEAs is GDPR. As GDPR law states that an organization is required to keep the only limited amount of information of their customer/client. Now, if a person commits a crime using any social media platform, it would be very difficult for LEAs to track down the criminal due to limited or restricted information provided by the social media organization. GDPR acts as both a boon and bane for the community. ■