Information Technology Act 2008 & Cyber crime

Umapathi Sattaru IPS
Inspector General of Police rtd
Mail: umapathi_sattaru@yahoo,com
Ph 9440700900.

Revised AP Police Manual in 2017 circulated to all 1100 Police Stations

What is cyber crime?

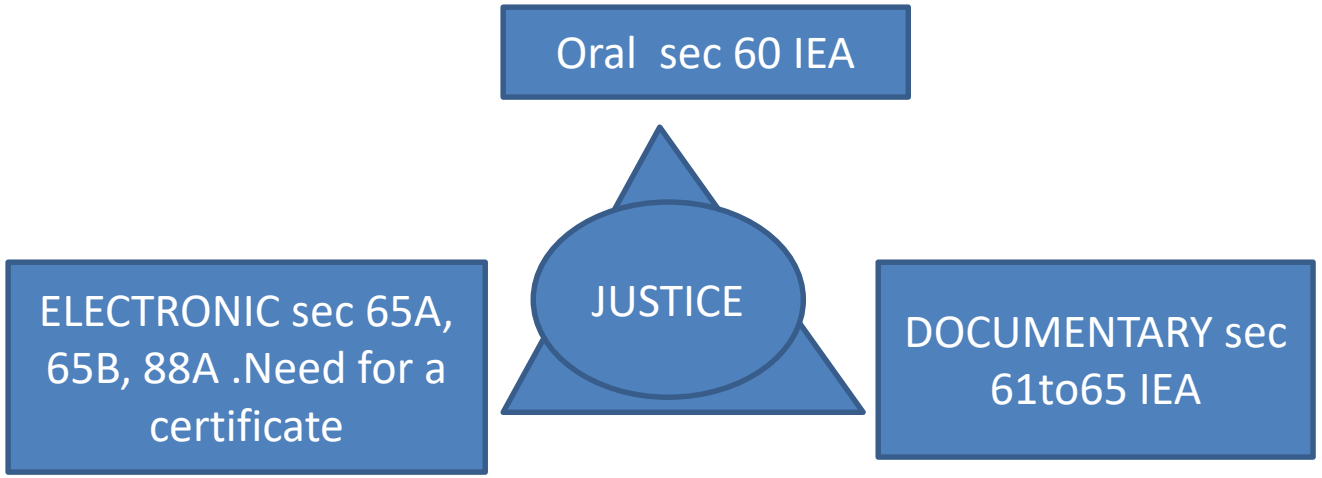
- Cybercrime is: any criminal activity that uses a computer either as an instrument, target, or a means for perpetuating further crimes comes within the ambit of cybercrime, i.e., unlawful acts wherein the computer is either a tool/medium or a target or both.

Definition of computer as per IT Act

- “Computer” means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical,
- arithmetic, and memory functions by manipulations of electronic,
- magnetic or optical impulses, and includes all input, output, processing,
- storage, computer software, or communication facilities which are
- connected or related to the computer in a computer system or computer network;

Courts convict offenders .. Need evidence . Admissible & relevant

- The Link for the I.O.(states to set up Forensic Labs to analyze electronic evidence dt 18th Feb 2019 of Supreme court in Subhendernath vs state of W.B)



Sec 45 opinion of experts, Sec 45A –Opinion of Examiner of Electronic Evi, sec 47 opinion as to Handwriting, 65A Spl provisions regd electronic record, 65B admissibility of Electronic record , 67A Proof of electronic signature, sec 29 A IPC –ELECTRONIC RECORD

Digital India Mission

- **Various Schemes of Digital India programme: Diksha**: It stands for Digital Infrastructure for Knowledge Sharing. It serves as **National Digital Infrastructure for Teachers.** All teachers across the nation will be equipped with advanced digital technology.
- **eNAM**: It was launched on 14th April 2016 as a **pan-India electronic trade portal linking Agricultural Produce Market Committees (APMCs)** across the States.
- **eSanjeevani: ** It is a **telemedicine service** platform of the Ministry of Health & Family Welfare.
- **DigiBunai**: DigiBunai **aids the weavers** to create digital artwork and translate the saree design to be loaded to the looms. DigiBunai™ is a first of its kind Open Source software for Jacquard and dobby weaving.
- **PM SVANidhi scheme: ** The Ministry of Housing and Urban Affairs (MoHUA) has launched **Pradhan Mantri Street Vendor's AtmaNirbhar Nidhi (PM SVANidhi)**, for providing affordable loans to street vendors. It **incentivises digital transactions by the street vendors.**
- **Digital solutions during Covid-19: ** Contact tracing app, **Aarogya Setu.**
- For being transformative that is to realize IT (Indian Talent) + IT (Information Technology) = IT (India Tomorrow).

Digital India

- Ministry of Electronics and Information Technology takes care of the mission
- Digital India is a Government of India (2015) initiative aiming at improving the online infrastructure and enhancing internet connectivity. The motto of Digital India is “Power to Empower”.
- Digital India is a campaign launched by the Government of India in order to ensure the Government's services are made available to citizens electronically by improved online infrastructure and
- by increasing Internet connectivity or making the country digitally empowered in the field of technology.
- For being transformative that is to realize IT (Indian Talent) + IT (Information Technology) = IT (India Tomorrow).

Digital investigation ..

- Why Digital Investigation Lab in Cyber Crime PS? During the traditional crime investigation, forensic process comes at a later stage in the course of investigation whereas in case of Cyber Crimes / Cyber related crimes,
- investigation starts with the forensic process, such as Network Forensics,
- Onsite Forensics, Disk Forensics and
- Video Forensics.
- Thus need for Digital Investigation Lab for identifying the criminal, based on technical clues.

Artificial Intelligence

- AI is the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.
- Scientists are developing artificial intelligence so that we can use machines to improve the quality of life for humans. It lets machines do repetitive tasks which might injure or be dangerous for humans.
- Artificial intelligence can improve the safety of cars and airplanes.
- Ultimately, their purpose is to supplement humans with insights from vast amounts of data only computers can process.

Fake profiles

- By creating fake profile in the popular matrimonial web sites who are searching for the second marriage make them as situational victims and cheat them with money or personal privacy to black mail them.

On line JOB PORTALS

- Viewing the online job portals criminal understands the need of the job to the female victim and start sending the fake job opportunities and make them believe it to be genuine and defraud them for money. Some time they even conduct physical interview with fake offices of reputed name.

FACE BOOK , INSTAGRAM, WHATS APP

- Using Social Media such as Face Book, Instagram, whatsapp, telegram etc., the criminals are contacting the female victim as unknown persons or as known persons similar to victims friends name and make the victim believe the online person and start sharing the personal and private material.
- later the criminal cheats the victim for physical relationship or fraudulent money transactions.
- Accounts of servants or poor people are used to siphon the money in seconds.

ON LINE DOMESTIC HELP

- In the name of online domestic help advts, related to plumbing, carpenter, electrician, beautician etc., physically they visit houses and robs the inmates.
- These people come around noon time in the absence of male members.

Fake call centers

- There are several fake call centers existing who will keep their phone number as the contact number in the google search engine of the popular banks and collects the security credentials of individuals when they call them thinking that the number is genuine and do the online fraudulent transactions and cheat them.

You need experts..

- Why Experts?
- For activities such as online information gathering,
- Network Forensics,
- Mobile tracking, e-mail tracking,
- Social media analysis and link analysis, regular police officers do not possess the required expertise.
- specialists with the latest technology know-how, are handy for complex investigation.

Cyber crimes ..

- Cracker Is a cyber-burglar or vandal, an individual or group intent on causing malicious harm to a network or computer ?
- Data did-ling Involves altering the raw data just before a computer processes it and then changing it back after processing is completed.
- Malware : A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim.

Cyber crimes ..

- Phishing : Using spoof e-mails or directing the people to fake web sites to fool them into divulging personal financial details so that criminals can access their accounts.

- Root kit : A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means

- Salam Attack : This attack involves making alteration so insignificant that in a single case it would go completely unnoticed. These attacks are used for commission of financial crimes.

Cyber crimes

- Sniffer : A program and/or device that monitors data travelling over a network.
- Sniffers can be used both for legitimate network management functions and for stealing information off a network.
- Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere.
- Pen drives are dangerous .. Transfer of data & receipt of data with secret sniffing code.
- Mails can be sniffed. Even official mails can be unless classified like the codes used by consulates..

Cyber crimes..

- Social engineering : A hacker term for deceiving or manipulating unwitting people into giving out information about a network or how to access it.
- Spoofing : Refers to sending information that appears to come from a source other than its actual source.
- Spyware : Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organisations without their knowledge; a type of malicious code.
- Steganography : The art and science of communicating in a way that hides the existence of the communication.
- An image file may contain hidden messages between terror groups, which will be known only to the intended recipient and the sender.

Cyber crimes..

- Trojan : A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.

- A **computer virus** (self-replicating) is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code.
- If this replication succeeds, the affected areas are then said to be "infected" with a computer virus. Ex: large net works of Banks , gas pipe line, power supply, electricity grid.

- Worm : A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

- Zombie : A program that is installed on a system to cause it to attack other systems.

Hacking

- Hacking is gaining entry into a computer system without the permission, withan intention to cause loss, steal, or destroy the data contained in it.
- Done by persons well versed with computer tech, by exploiting some of the vulnerabilities that are present in the computer system.
- This involves various methods of acquiring sensitive information like user names, pass words, internet protocol addresses and use them to gain access
- They penetrate into defence mechanisms employed by target computer systems in the form of Trojans, malware, worms, and viruses which will get embedded
- in the target computer system compromising its security

Cyber crime..

- Sec.**66 E: Punishment for violation of privacy.** Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both
- **Explanation.- For the purposes of this section—**
- (a) “Transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;
- (b) “Capture”, with respect to an image, means to videotape, photograph, film or record by any means;
- (c) “Private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;
- (d) “Publishes” means reproduction in the printed or electronic form and making it available for public;
- “Under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that—
- (i) He or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

Types of cyber crimes

- **Online lottery frauds / online job frauds** In this type of offence, innocent people are contacted by the fraudster through both SMS and e-mail communication stating that they have won huge amount in lottery or got lucrative job offer.
- Slowly, in the name of customs, anti-terrorism, conversion, NOC, VISA processing, etc., incremental money will be asked to be deposited in bank accounts which are created with fake credentials.(mostly in remote areas of NE States & other places). *Banks fail to notice the illegal transfers and with drawls as there is no on line computer vigilance system*)
- Mostly people from foreign origin (like Nigerians) are indulging in such offences. The money lost by the victims is runs into crores of rupees. We have no MLAT with Nigeria.
- On the same analogy people are being targeted and cheated in the names of jobs abroad (ex case study CFSL Scientist)

Case study of matrimonial fraud

- Cr no .. /2001 u/s 417 (punishment for cheating), 419 (cheating by personation) , 420 (cheating) IPC , 66 C, 66 D IT Act of Cyber PS :
- One Reddy posted his sons' bio data in Telugu matrimony site with ID no ....
- On 19th Jan 2021 one woman purportedly from USA but n/o Bangalore accepted the ID, came in contact with boys parents using male voice (ADCOM software), spoke with the boy , requested to deposit Rs 1,16,262/ - for an engagement ring to KVB AC. . One of Complainants' son in USA transferred the money from his CITI bank in USA to KVB AC.
- After receiving money the woman stopped answering her cell phone & Mr Reddy felt he was cheated , hence FIR

Case study contd..

1. SHO Cyber PS registered FIR . Inspector of police is IO (Investigation Officer)
2. Sent notice to KVB Manager u/s 91 CrPC to produce Bank AC details. Ascertained the AC holders names. AC pertains to a watchman of an Apt in Bachupally , Cyberabad.
3. Through watchman ascertained name of the woman who opened the accounts and kept their Bank ac books with her.
4. SHO obtained the Login /Logout IPs , contact phone , recovery e-mail address of profile ID ....
5. Sent requisition to DCP Crimes for CDR of accused woman phone numbers and secured from nodal officer of cell phone companies.
6. SHO arrested the accused married woman MBA (finace) , mother of a child on 26 th Feb 2021 (case reported on 19th Jan) with all link evidence . She was also involved in 5 other case earlier , arrested, released on bail, continue same M.O (MODUS OPERANDI)

case study... Investigation.

- Modus operandi: accused woman has 8 alias names. She lures poor people , opens bank accounts in different banks , collects pass books, debit cards with 4 digit PIN numb, withdraws money when un suspecting bride grooms deposit money and close the cell phone or account .
- She installed “Second line “ application in her mobile phone for generating virtual number of USA . Facade to make people believe she is H1B visa holder & in USA
- Why? She had to repay a loan of 10 lakhs & found this fraud is easy.
- How? she will post good looking girls photos from Bharat Matrimony.com, Telugu matrimony . Com and post them as her photos to lure .
- When the prospective bride grooms want to meet her she will block their phones or switch off.

Cyber crime..

- **Online harassment** : There has been an increase in this type of offences and the victims are mostly females.
- The cyber criminal uses mobiles, emails and social networking sites to harass the victims creating fake identities, posting derogatory, obscene and private content, causing mental agony, and affecting family relations, leading to divorces and break-up of engagements.
- Keep away from face book etc . Literally dangerous

Cyber crime..

- **Online cheatings** : Criminals are using matrimonial sites and other advertisement sites with false content to lure innocent victims again mostly female, thereby cheating them for wrongful gain and blackmailing.
- In another type of offence, profile of divorced women is collected by these habitual offenders who lay a trap and convince them that they will marry them and take undue advantage of their situation through physical exploitation and cheating them financially.
- Again money transfers thro banks…

Cyber crimes..

- **Fake online appointments in reputed multi-national companies :**
- For such offences, cyber criminals access the details of people whose resume is posted on different online job portals with their personal details.
- Using those details, the cyber criminals contact them and offer jobs and collect money in the name of processing fee, etc., for wrongful gain.

- **Phishing frauds :**
- In this line, cyber criminals contacts netizens in the guise of popular banks, Income Tax Department, Webmail service providers, such as Gmail, Yahoo Mail, etc., and send messages asking the targets to part with their security credentials such as Username, password, account information, date of birth, etc., so that they can hack into those accounts for wrongful gain. (ex .. City police cases)

Cyber crimes..

- **ATM, Debit and Credit card frauds :**
- These are all possible both online, by collecting the PIN numbers, CVV numbers, and offline, by cloning the card.

- **Hacking cases :**
- The term Hacking has broad connotation, but in Cyber parlance it means unauthorized access. There are several ways and means used by these fraudsters to compromise computer security, bank accounts, mail accounts, websites and web servers for defamation, wrongful gain, cheating, stealing of personal data. In hacking cases, targets could be individuals, companies, nations or critical infrastructure.

Cyber crimes..

- **Publishing of obscene content :**
- This is also one type of online harassment, wherein victims, share their intimate pictures, videos with people who manage to come very close to them and, at a later time, if some issues arise between them, the victims are targeted by publishing their personal/ private videos, in the net.
- **Cyber terrorism :**
- The most deadly and destructive form of cyber crime is “cyber terrorism”. The traditional concepts and methods of terrorism have acquired new dimension.

Internet of things (IoT) & AI

- The **Internet of things** (**IoT**) describes the network of physical objects, so known as, "things" — that are embedded with sensors, software, and other technologies that is used for the purpose of connecting and exchanging data with other devices and systems over the Internet.
- Things have evolved due to the convergence of multiple technologies,
- real-time analytics,
- machine learning,
- ubiquitous computing,
- commodity sensors, and embedded systems.
- Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things.

Internet of Things (IoT)

- . According to Lewis, "The Internet of Things, or IoT, is the integration of people, processes and technology with connectable devices and sensors to enable remote monitoring, status, manipulation and evaluation of trends of such devices.“
- In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures,
- thermostats,
- home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers.
- The IoT can also be used in healthcare systems.

Some of latest FIRs

- **On line trafficking** : Cr no 965/2020 U/S 370 A(2)IPC (exploitation of a trafficked person above 18 yrs) , Sec 3,4,5 of ITP (Immoral traffic prevention Act) & Cr no 974/2020 of Kukatpally PS of Cyberabad

- **Trafficking to other countries like Gulf** : Cr no 102/ 2017 u/s 376 (2) (i) , 370,420, 468 (forgery for purpose of cheating) , 471 (using as genuine a forged document which is known to be forged) r/ w 34 IPC, Sec 3, 4 of POCSO Act of Kamatipura ps of Old City HYD

Some FIRs of cyber crimes

- Cr No .. . /2020 under section (u/s) 354 D (Stalking) , 509 IPC (word or gesture intended to insult modesty of woman) ; 67 IT Act (Punishment for publishing or transmitting obscene material in electronic form.. cyber stalking) of Cyber crime PS of Rachakonda Commissionrate
- Cr No.. / 2020 u/s 354D, 509 IPC , Sec 12 POCSO Act sexual harassment of child), sec 66 C, 66 D IT Act of Cyber crime PS
- Cr No ../ 2020 u/s 419 (cheating by personation), 509 IPC , 66 C (Punishment for identity theft), 66 D (Punishment for cheating by personating by using computer Resource) IT Act of cyber crime PS

Sec 482 Cr PC .High courts inherent powers vis a vis police investigation

- *The section is a sort of reminder to the High Courts that they are not merely courts in law, but also courts of justice and possess inherent powers to remove injustice.*

- Accused persons file petitions for a) quashing FIR, b) stay on investigation, c) stay on arrest , d) deleting names from FIR , d) discharge petitions, e) stay on trial

- High courts exercise these powers to secure ends of justice, prevent abuse of the process of any court

Justice delivery-Inter connectivity of IPC, CrPC, IEA- accusatorial system- the players

- The triangle of Substantive law (IPC)+Procedural law+ Evidentiary law
- Players: police station (to set law into motion ..FIR), I.O (investigating officer),
- Forensic clues team including Cyber expert & FSL,
- Special Public Prosecutor, PP (Public prosecutor for sessions trial cases), Addl PP, APP (trial of cases in Asst Sessions / Magistrates courts),
- Sessions Judge, ADJ, Asst sessions judge, Magistrate
- Defense advocate,
- Victim, Witnesses, Accused, prosecution exhibits, documents, medical and FSL reports, electronic evidence etc.

Investigation

- Sec 2 (h) CrPC : Includes all the proceedings under the Code
- For the collection of evidence
- By a police officer or by any person authorised by a Magistrate
- Objective: to bring the offender to justice by adducing admissible and relevant evidence before the Trial court for adjudication.
- To elicit truth..
- To present case without concoction or fabrication or padding up evidence.
- Your Case Diary reflects your process of investigation (court may peruse at any time ..during remand..charge sheet..trial)

Sec.420, IPC :

(1) Deception of any person

(a) fraudulently or dishonestly inducing that person

(i) to deliver any property

(ii) to consent that any person shall retain any property: or

(b) **intentionally inducing** that person shall to do or omit to do anything which he would not do or not omit if he were not so deceived.

which act or and omission causes or is likely to cause damage or harm to that person body, mind, reputation or property.

Sec. 420 IPC contd....

- ✓ Sec 23. “Wrongful gain”.—“Wrongful gain” is gain by unlawful means of property to which the person gaining is not legally entitled.
- ✓ “Wrongful loss”.—“Wrongful loss” is the loss by unlawful means of property to which the person losing it is legally entitled.
- ✓ Sec 24. “Dishonestly”.—Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing “dishonestly”.
- ✓ Sec 25. “Fraudulently”.—A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.
- ✓ Sec 29A. “Electronic record”.—The words “electronic record” shall have the meaning assigned to them in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000 .
- ✓ Direct proof of ‘*mens rea*’ is seldom available and it has often to be inferred from the surrounding circumstances.
- ✓ Mere breach of contract can not give rise to criminal prosecution on for cheating unless fraudulent, dishonest intention us shown at the beginning of the transaction.

Age Verification (Sec. 94 JJ CPC Act)

(Crucial to establish the victim is a child below 18 yrs)

I.O. should immediately obtain date of birth certificate from one of the sources:

- ✓ School Date of Birth / T.C
- ✓ Aadhar/Ration/Voter I.D. Card
- ✓ As entered in Hospital Records
- ✓ Village/Municipal Records
- ✓ Ossification test when no other record is available.
- ✓ I.O. to mention age details in C.D.

Age Certification

Most important criterion in case of ossification test

- ✓ Jayamala Vs Home Secretary of J&K (AIR-1982 SC 1297)
- ✓ The Supreme Court held that when experts opinion is given within an age bracket, the lower age should be the one taken into consideration by the I.O. & Courts, so that benefit of doubt favours the victim.
- ✓ For ex: if age is certified by Doctor as 17 to 19 yrs, it should be presumed to be 17 yrs by the I.O and the Court.
- ✓ Though victim is rescued at the age of 20 yrs, if she states that she was trafficked at the age of 16 / 17 yrs relevant IPC sections will be applicable.

Granting Bails / Acceptance of sureties in Human trafficking and ITP Act cases : contd….

- ✓ Certain conditions like
- ✓ automatic cancelation of bail to the absconding traffickers, on being arrested,
- ✓ not to be released on bail, till completion of trial ,
- ✓ not to grant bail to those who do not have fixed abode etc.

Liability of Prosecutor and Investigating Officer :

- ✓ In *State of Gujarat Vs Kishanbai in Criminal appeal 1485 of 2008*
- ✓ dated : 7th January, 2014, the Hon'ble Supreme Court said that…….
- ✓ "every acquittal should be understood as a failure of Justice delivery system, in serving the cause of justice.

Important punishable sections of IT Act

- Sec.65:Tampering with Computer Source Documents
- Sec.66: Computer Related Offences : If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
- Sec.66A : Punishment for sending offensive messages through communication service, etc**.** Hon'ble Supreme Court of India struck down Sec 66A of IT Act in WP 167/2012 dt. 24-3-2015 (Shreya Singhal vs. State of Maharashtra).
- Sec.66B: Punishment for dishonestly receiving stolen computer resource or communication device.

Cyber crimes ..

- **Sec.66C: Punishment for identity theft.**
- Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment for a term which may extend to three years and fine which may extend to rupees one lakh.
- **Sec.66D: Punishment for cheating by personation by using computer resource.**
- Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment for a term which may extend to three years and fine which may extend to one lakh rupees

Cyber crimes contd...

- Sec.**66 F: Punishment for cyber terrorism**
- (1) Whoever,-(A) With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –
- (i) Denying or cause the denial of access to any person authorised to access computer resource; or
- (ii) Attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
- (iii) Introducing or causing to introduce any Computer Contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70,

Most common cyber crime..

- Sec.**67 :Punishment for publishing or transmitting obscene material in**
- **electronic form :** Whoever, publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either
- description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Most common offence..

- Sec.**67 A: Punishment for publishing or transmitting of material containing sexually explicit act etc. in electronic form:** Whoever, publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Child porn & related matters

- Sec.**67 B: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form. :** Whoever,- (a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or (c) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or (d) Facilitates abusing children online or

Child porn & related matters. Sec 67B contd..

- Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:
- POCSO Act (Protection of Children from Sexual Offences) sections like sec 3 r/w 4 (PSA.. Penetrative Sexual Assault) & Sec 5 r/w 6 (APSA .. Aggravated Penetrative Sexual Assault) , sec 13 r/w 14 (use of children for pornographic purposes) are also applicable ..
- In case of trafficking sec 370 IPC is applicable

Provision for blocking internet etc

- **Sec.69 A : Power to issue directions for blocking for public access of any information through any computer resource** (1) Where the Central Government or any of its officer specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence
- by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

Finalising the case..

- Police seized a laptop , 5 cell phones, 8 SIM cards, 4 ATM cards, 3 ADCOM mobile phones
- Remanded to Judicial custody after medical examination and covid 19 report ..
- Learning points:
- When we don’t meet persons how do we believe ?
- Without meeting parents why do people cinch the marriage proposal?
- ?????

Case study .. Extortion thro' instagram

- Cr no ../ 2020 u/s 417, 419, 420, 384 (extortion) IPC , 66-C, 66-D IT Act of Cyber PS dt 31st Jan 2020
- One unmarried woman 26yrs was harassed by a suspct male on her Instagram & demanded payment @ Rs 50,000/- four times on the threat of posting her nude pictures in U tube and extorted Rs 2 lakhs in toto.
- Some one in june 2019 sent her a message saying that he has her nude photos and unless paid Rs 50, 000/- he will upload in YOU tube. Though she has no such occasions she feared and paid
- Four months later same demand and she paid after she saw a morphed nude picture with her face. It continued till Jan 2020 with severe abusive language in night times..
- Police registered a case on 31st jan 2020
-

Extortion thro’ Instagram

- The accused created four different Ids of Instagram while sending the abusive messages.
- IO obtained the IP address from Face Book inc, California USA & came to know the cell phone & address .
- Surprisingly the accused is a married woman?? Resident of same locality. Since the complainant is unmarried she thought of extorting money from her .
- All digital evidence pin pointed the commission of cheating, extortion, by impersonation thro electronic media .
- Accused was arrested on 20th Feb 2020 and remanded to judicial custody.
- Learning points....???

Gift fraud case

- FIR No: ... /2020.U/S 417, 419, 420 IPC, section 66 (C) 66 (D) of IT Act of Cyber PS : THE ACCUSED DEFRAUDED A 26 YEAR OLD TO PART WITH 29LAKHS PROMISING 4 CRORES and Gold Jewellery

- A1) Adjel GIFT osas s/o Adjel, age: 27 years, N/o Liberia.
- A2) Akpalu Godstine S/o Ghaakpalu, ahe: 27 years, N/o Agror of Nigeria
- A3) P.EhigiatornDaniel S/o Ehigiator, Age: 29 years, N/o: Federal Republic of Nigeria
- A4) P.Kromah Oyibo S/o Kromah, age: 24 years, N/o Bellayala of Liberia. (Arrested).
- A5) Nkeki Congidence david, S/o Nkeki Confidence, age: 26 years, N/o Republiuc of Ghanna.
- All are R/o. 3rd Floor of HNo-E23, RanjithVihar Colony, Nilothi extension, Nilothi, West District, New Delhi (The accused A1 to A5 were arrested on 05- 01-2021 at Nihal Vihar PS, New Delhi, produced before Hon'ble Duty Metropolitan Magistrate at Tihar Jail, West District, New Delhi; 'Transit Remand' was obtained and produced herewith.)

M/s Satyam Computer Services and Ltd.-Fraud Case-case study 05

- ✓ Causing loss to the investors to the tune of Rs 14,162 crores.
- ✓ Company secured illegal gains to the tune of about Rs. 2743 crores.
- ✓ C.No.2/2009 u/s 406, 420, 467, 471, 477A IPC of CID PS dt: 09.01.2009, Andhra Pradesh.
- ✓ First 40 days CID AP laid foundation for offences mentioned above
- ✓ CID constituted MDIT (Multi Disciplinary Investigation Team) with officials from IT, Forensic Auditing etc

u/s 406 IPC (Criminal Breach of Trust (CBT)

(i) There should be an entrustment by one person to another of the property (or) with any dominion over property

(ii) Such entrustment must be in trust

(iii) There must have been misappropriation (or) conversion to his own use by the person who received the property in trust.

(iv) Such conversion or retention of the property must be against or in violations of any direction of Law. (or) of any legal contract made touching the discharge d of such trust.

" **Being in any manner entrusted with property** "

Sec. 467 IPC: Forgery of Valuable Security (up to 10 yrs and fine

(i) Fraudulently signing a document with an intention (*mens rea)* of causing it to be believed that such document was signed by another or **under his authority.**

(ii) Making of such a document or electronic record ***intention*** to commit fraud or that fraud may be committed.

Sec. 471 IPC: Using as genuine a forged document or electronic record.

(i) fraudulent or dishonest use of a document as genuine.

(ii) The person using it must have knowledge or reason to believe that the document is a forged one.

Sec. 477: IPC (7 years and fine)

Falsifications of accounts :

1. Person coming within the purview must be a clerk, an officer, or a servant or **acting** in that capacity.

2. He/she must wilfully with intent to defraud

   i. destroy, alter, mutilate, or falsify any **book, paper, writing valuable security** or account which belongs to or is in the possession of his employer or

   which has been received by him for or on behalf of his employer or

   ii. Make or abet the making of any false entry in or omit or alter or abet the omission or

   alteration of any material particular from or in any such book, paper, writing valuable security or account

Perpetration of the fraud (Satyams Case)

1. By inflating the revenue of the company through false sales invoices and

2. Showing corresponding gains by forging the bank statements **with** the **connivance** of the statutory and Internal Auditors of the company.

3. The annual financial statements of the company with **inflated** **revenue** were Published for several years leading to higher price of the script in the market.

4. Innocent investors were lured to invest in the company.

5. Attempts were made to conceal the fraud by acquiring the companies of the ***Kith and Kin***

2009 January FIR , 7th April 2009 charge sheet filed against 10 accused - A fraud of 7123 crores

Feb 17, 2011: USA class action suits settled for 125 million US dollars.

July , 15 2014 : SEBI slaps Rs. 1,850 crore fine on chairman and bars him from market for 14 yrs.

April, 2015 : special CBI Court sentenced the chairman and 9 others to 7 years in jail and fined Rs. 5 crores each.

Chairman and others served 31 months jail term during trial.

Satyam case contd..

Motive : wanted to be among the top 4 firms in IT industry

High court said :“They rode a tiger, not knowing how to get off without being eaten” :

Our role

- Launch delete/ block campaign
- Educate students / youth of the traps
- Educate your own family members
- Demonstrate your grit in taking case to logical conclusion
- When you visit schools/ colleges do educate students and parents.
- Keep upgrading your knowledge and skills

ROAD MAP

- ✓ Educate
- ✓ Empower
- ✓ Entrust
- ✓ Engage
- ✓ Ensure
- ✓ Establish
- ✓ Evaluate

Young hearts like you can change the Social Fabric of Indian Society

Thank You for your kind attention