Electronic Evidence: Collection, Preservation and Appreciation

Dr.S.Murugan IPS
Joint Director/Inspector General of Police,
Vigilance and Anti Corruption
Chennai.

Outline of My Presentation

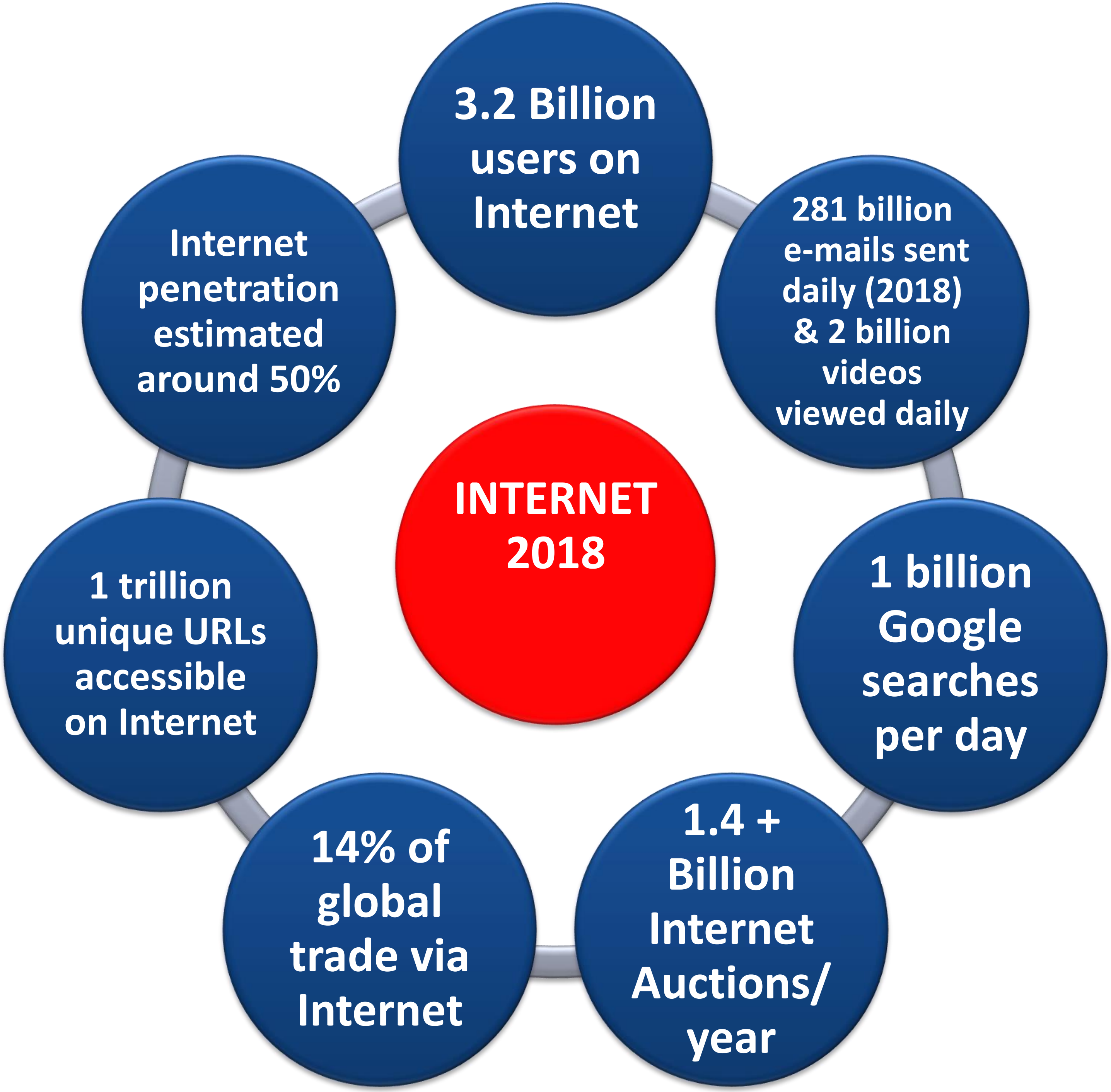
- Cyber Crime
- EE: Acquisition, Authentication, Admissibility
- Chain of Custody : SOP, Hash value
- Cyber Lab : Notifications, Meta data
- Social Media issues, Google,FP
- EE: 2020 Vision
- Recent Cybercrime trends, Dark net issues
- Tips for staying safe online
- Indian Cyber Laws
- Admissibility of EE : Case Laws.

Introduction

- Computers, Mobile phones and Internet are only source? What else?

- Impact of Social Media

- All Stake holders of judicial justice system need to update the use of latest technology and cyber forensic investigation techniques



INTERNET 2018

3.2 Billion users on Internet

281 billion e-mails sent daily (2018) & 2 billion videos viewed daily

1 billion Google searches per day

1.4 + Billion Internet Auctions/ year

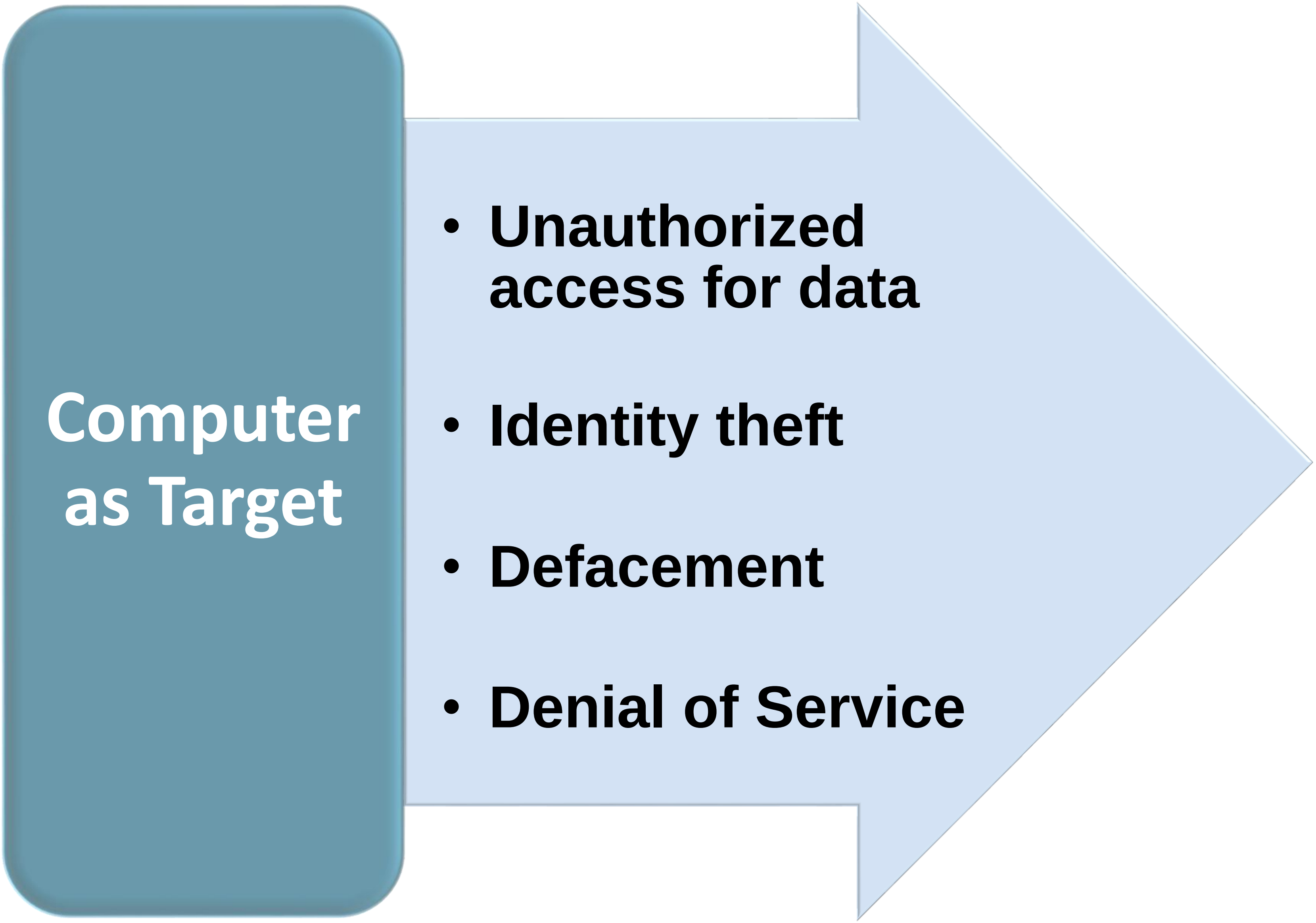
14% of global trade via Internet

1 trillion unique URLs accessible on Internet

Internet penetration estimated around 50%

Cyber Crime

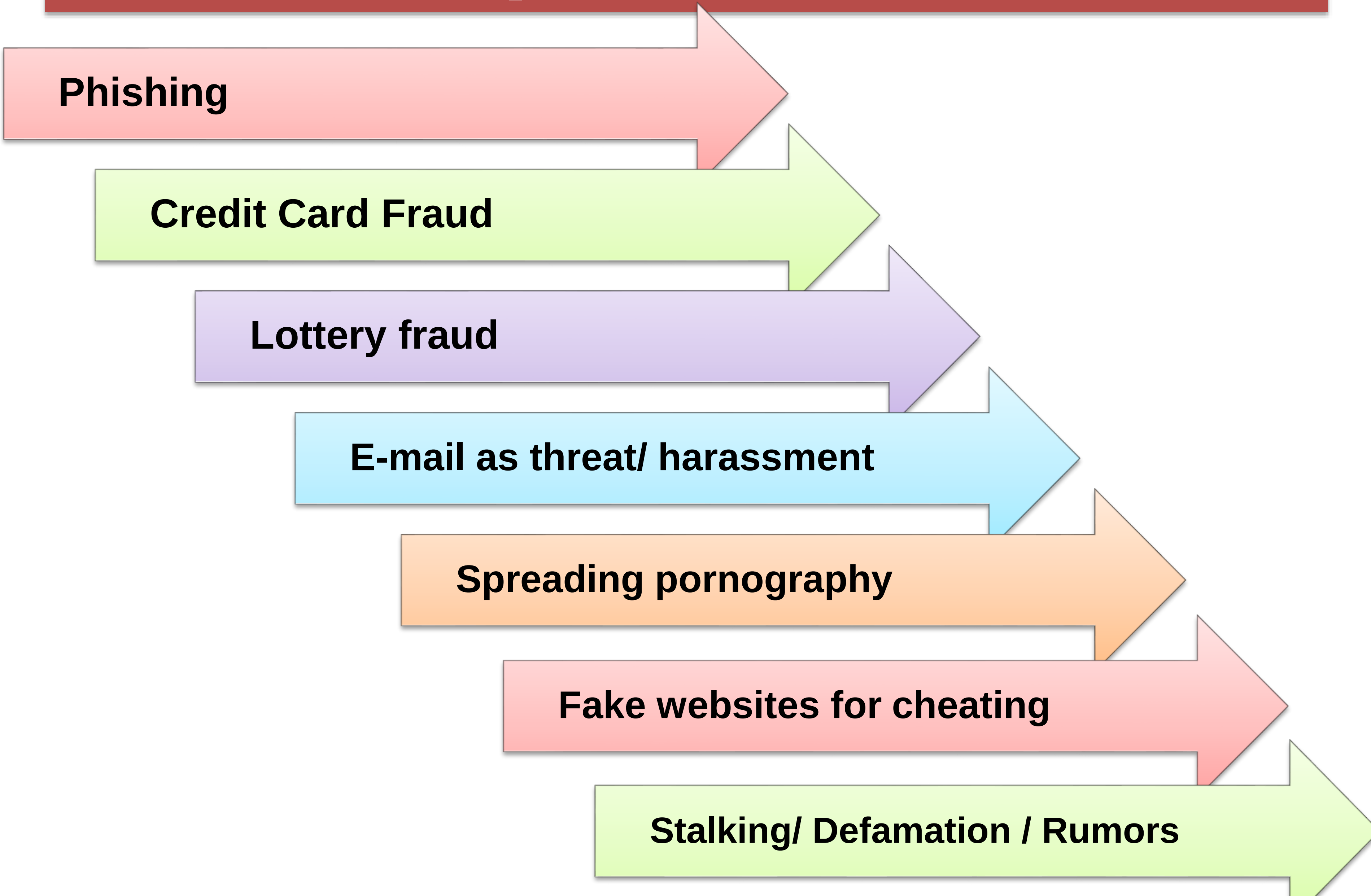
- Cyber crime is defined as a crime in which an electronic communication Device is the object of the crime, or used as a tool / target or used incidental or as a witness to commit an offence.
- Cybercriminals may use Information technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes.



Computer as Target

- Unauthorized access for data
- Identity theft
- Defacement
- Denial of Service

Computer as Tool



Phishing

Credit Card Fraud

Lottery fraud

E-mail as threat/ harassment

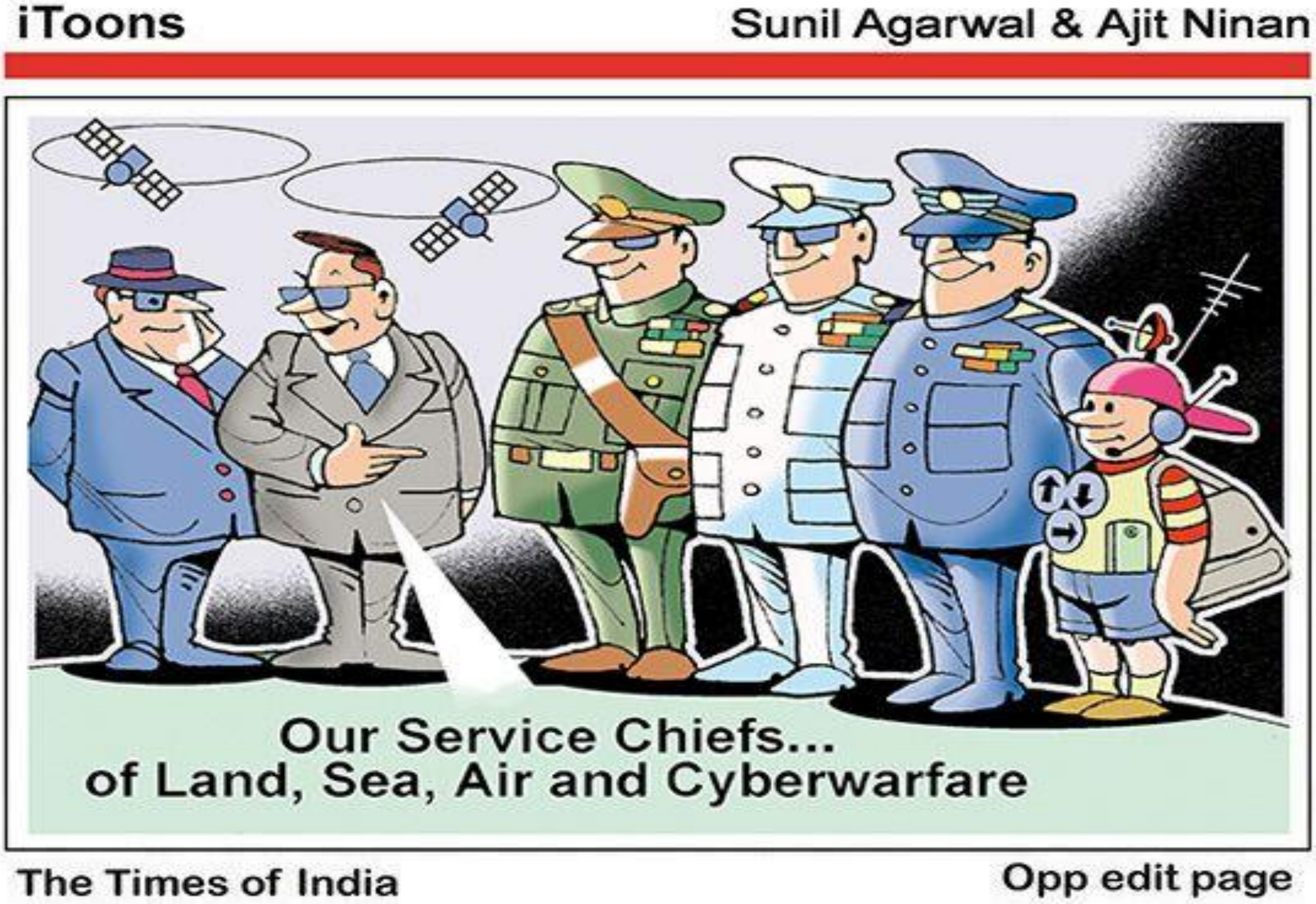
Spreading pornography

Fake websites for cheating

Stalking/ Defamation / Rumors

Cyber Crime Trend

- Cyber crime in to New emerging field of Technology
- Robotics,
- Artificial Intelligence
- Genetics
- Synthetic Biology
- Nanotechnology
- 3D Manufacturing
- Brain Science
- Virtual reality
- Neither LEA nor Forensics researcher not aware of this changes


iToons
Sunil Agarwal & Ajit Ninan
Our Service Chiefs...
of Land, Sea, Air and Cyberwarfare
The Times of India
Opp edit page

Edmond Locard (1877–1966)

Locard's theory

“ Anyone, or anything, entering a crime scene takes something of the crime scene with them. They also leave behind something of themselves when they depart”

Conventional Crime
vs
Cyber Crime

Traditional Criminal Technique

Burglary

Breaking into a building with the intent to steal.

Deceptive Callers

Criminals who telephone their victims and ask for their financial and/or personal identity information.

Extortion

Illegal use of force or one's official position or powers to obtain property, funds or patronage.

Fraud

Deceit, trickery, sharp practice, or breach of confidence. Perpetrated for profit or to gain some unfair or dishonest advantage.

Identify Theft

Impersonating or presenting oneself as another. In order to gain access, information, or reward.

Attempted ID Theft
Your IDENTIFICATION - has been compromised. Your attention is required.
Action
Ignore
Help
Robert Mizerek via Getty Images

Child Exploitation

Criminal victimization of minors for indecent purposes such as pornography and sexual abuse.

Cyber Crime

Hacking

Computer or network intrusion providing unauthorized access.

Phishing

A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.

Internet Extortion

Hacking into and controlling various industry databases (or the treat of). Promising to release control back to the company if funds are received or some other demand satisfied.

Internet Fraud

A broad category of fraud schemes that uses one or more components of the internet to defraud prospective victim, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.

Identity Theft

The wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.

Child Exploitation

Using computers and networks to facilitate the criminal victimization of minors.

Evidence…

- Evidence is evidence is evidence!
- Regardless of whether the evidence is physical evidence, trace evidence, biological matter, or electronic evidence residing on a specialized device, all evidence must be treated the same
- Integrity must be protected at all times.

Evolution of Electronic Evidence

- **1984, the FBI began to use computer evidence**
- **In 1991, a new term; "Computer Forensics" was coined**
- **In India IT Act 2000.**

  On 17th October 2000, ITA 2000 was notified and along with it the Indian Evidence Act 1872 got amended with several new sections being added to address the issue of Electronic Evidence

Characteristics of Electronic Evidence

- **Is invisible, can be altered or and destroyed easily.**
- **Is latent like FP or DNA**
- **Crosses jurisdiction borders**
- **Can be time sensitive**
- **Requires special tools equipment and specialized training**
- **Requires expert testimony**

Electronic evidence

- Electronic evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an Electronic device!

Why Digital?

- ‘Digital’ because it has been broken down into digits; binary units of ones (1) and zeros (0), that are saved and retrieved using a set of instructions called software or code.

- Any kind of information—photographs, words, spreadsheets—can be created and saved using these types of instructions.

Where is Electronic Evidence?

- Any kind of storage device
  - Computers, CD’s, DVD’s, floppy disks, hard drives, thumb drives
  - Electronic cameras, memory sticks and memory/ SIM cards, PDA’s, cell phones
  - Fax machines, answering machines, cordless phones, pagers, caller-ID, scanners, printers and copiers
  - CCTV

Type of Files

- Audio
- Video
- Text

“EVIDENCE” TERM : STATUTORY PROVISIONS

- **Section 3 of Indian Evidence Act, 1872 defines**
  - ✓ **“Evidence” means and includes:**
    - **All documents including electronic records for the inspection of the court.**

- **Electronic Records**
  - – **As per Sec 2(1)(t) of IT Act, 2000, it means:**
    - **- Data record or data generated**
    - **- Image or sound stored**
    - **- Received or sent in electronic form or microfilm or computer generated microfiche**

- **Electronic Form**
  - – **As per Sec 2(1)(r) of IT Act, 2000 with reference to information means**
    - **- Any information generated, sent, received or stored**
    - **- in media, magnetic, optical, computer memory, microfilm, computer generated microfiche or similar device.**

STATUTORY PROVISIONS(contd…)

- Information
  - As per Sec 2(1)(v) of IT Act, 2000 it includes:
    - Data
    - text
    - images
    - sound
    - voice
    - codes
    - computer programmes
    - software
    - database
    - microfilm
    - computer generated
    - microfiches

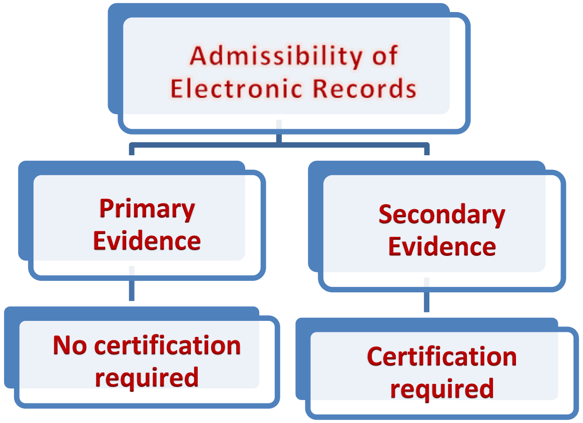
- Section 4 of IT Act, 2000 gives legal recognition

  to the Electronic records on two conditions
  - Rendered or made available in an electronic form.
  - Accessible so as to be usable for a subsequent reference.

Oral Evidence Vs Documentary Evidence

Oral Evidence:

- **Section 22A** declares Oral Evidence as to the contents of electronic records are not relevant unless the sanctity of electronic record produced is in the question.
- The foremost / primary requirement is to prove the sanctity of the document to make it admissible in the court of law.


Admissibility of Electronic Records
Primary Evidence
Secondary Evidence
No certification required
Certification required

Documentary Evidence - Evidence can be of two types:

- **Primary evidence: Sec 62 and Sec 64** Primary evidence means the document itself produced for the inspection of the Court.
- **Secondary evidence: Sec 63 and Sec 65** Secondary evidence means Copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy.

Types of Evidence

- **Primary Evidence**

- **Secondary Evidence**

Electronic evidence is Primary or Secondary?

- Input: **CBI COURT**
- **Binary Equivalent:**
- **01000011 01000010 01001001 00100000 01000011 01001111 01010101 01010010 01010100**

Electronic FORENSIC KIT

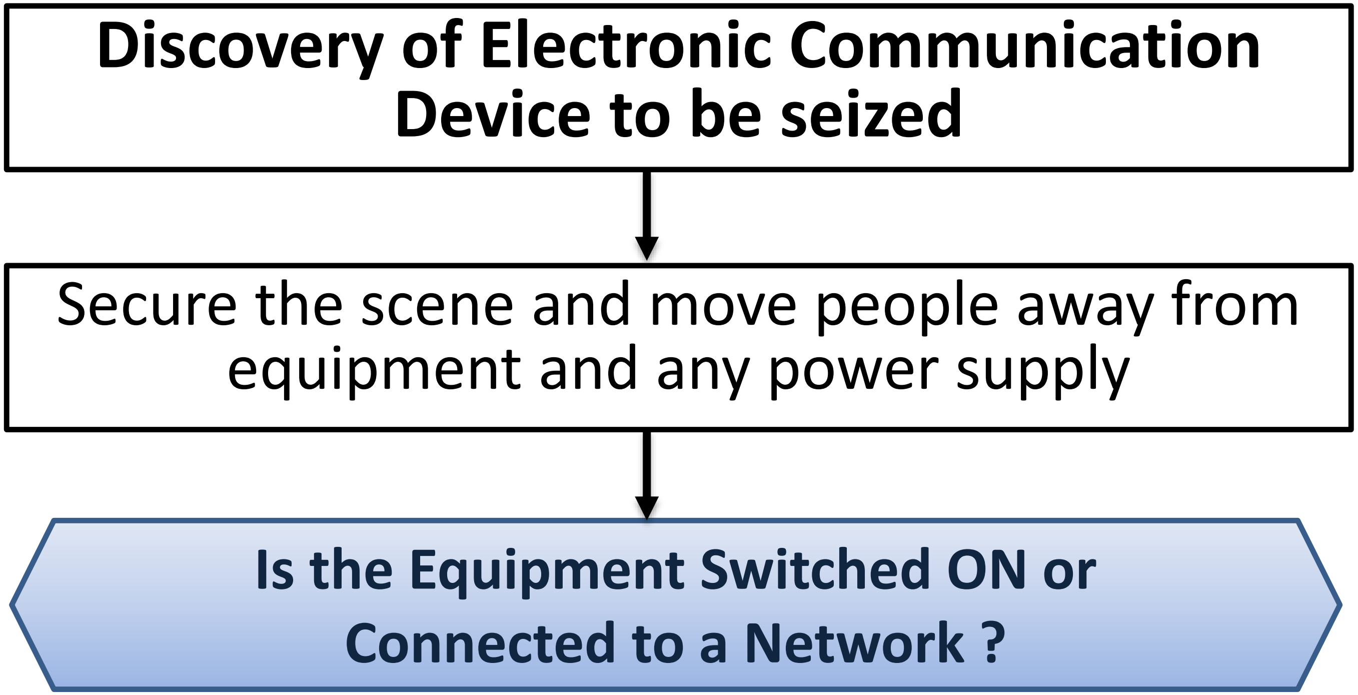
A Electronic forensics field response kit may contain some of the following:

- 1. Electronic camera
- 2. Sterilized removable media
- 3. Forensic computer
- 4. Hardware write-blocking devices
- 5. Forensically sound boot disks
- 6. Mobile device acquisition tools
- 7. Tool kit (screw drivers, etc.)
- 8. Evidence packaging materials

Seizure of Electronic Equipment

Discovery of Electronic Communication Device to be seized

Seizure of Electronic Equipment



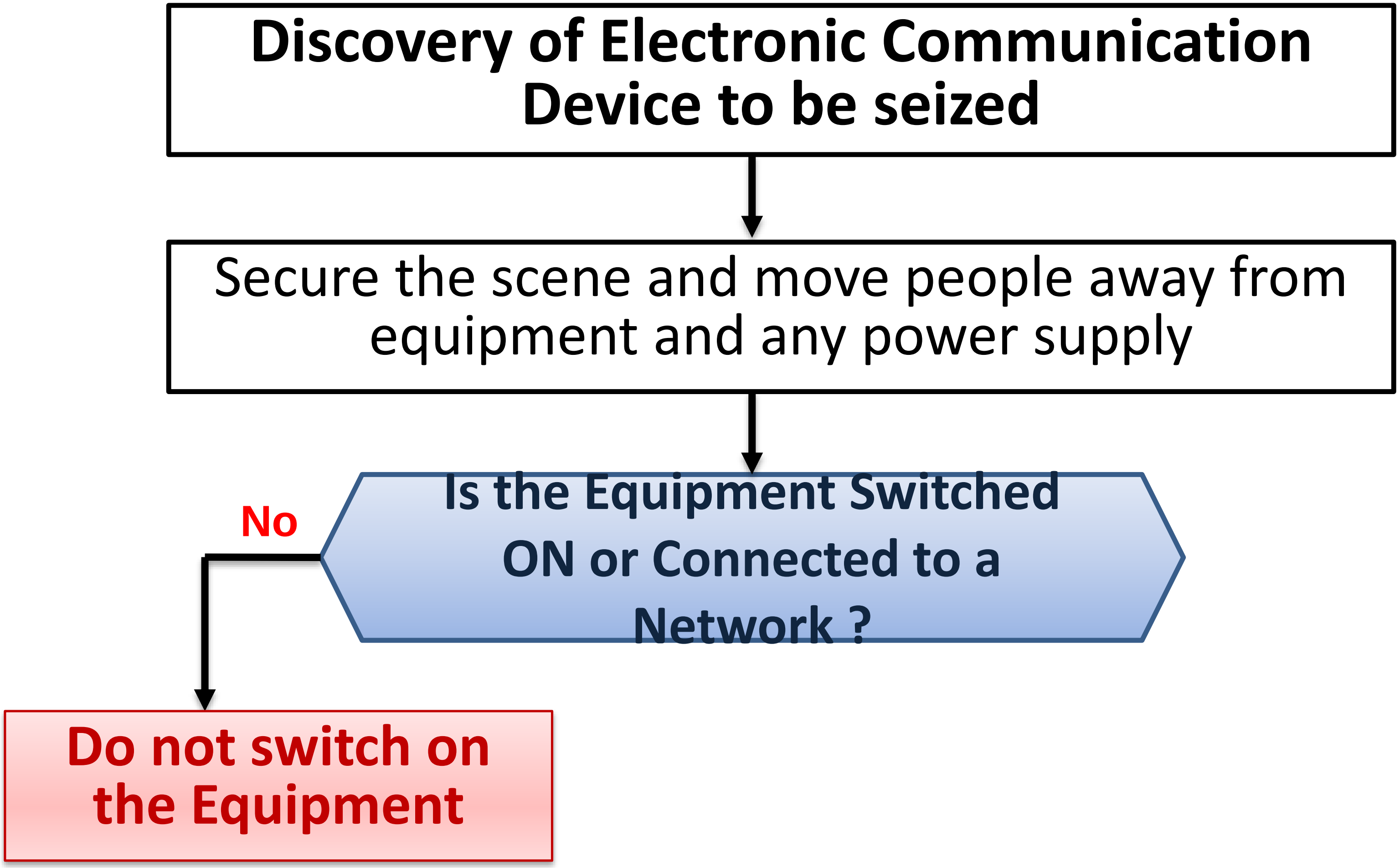
Discovery of Electronic Communication Device to be seized

Secure the scene and move people away from equipment and any power supply

Is the Equipment Switched ON or Connected to a Network ?

CERTIFIED FORENSIC COMPUTER EXAMINER IACIS

Seizure of Electronic Equipment



Discovery of Electronic Communication Device to be seized

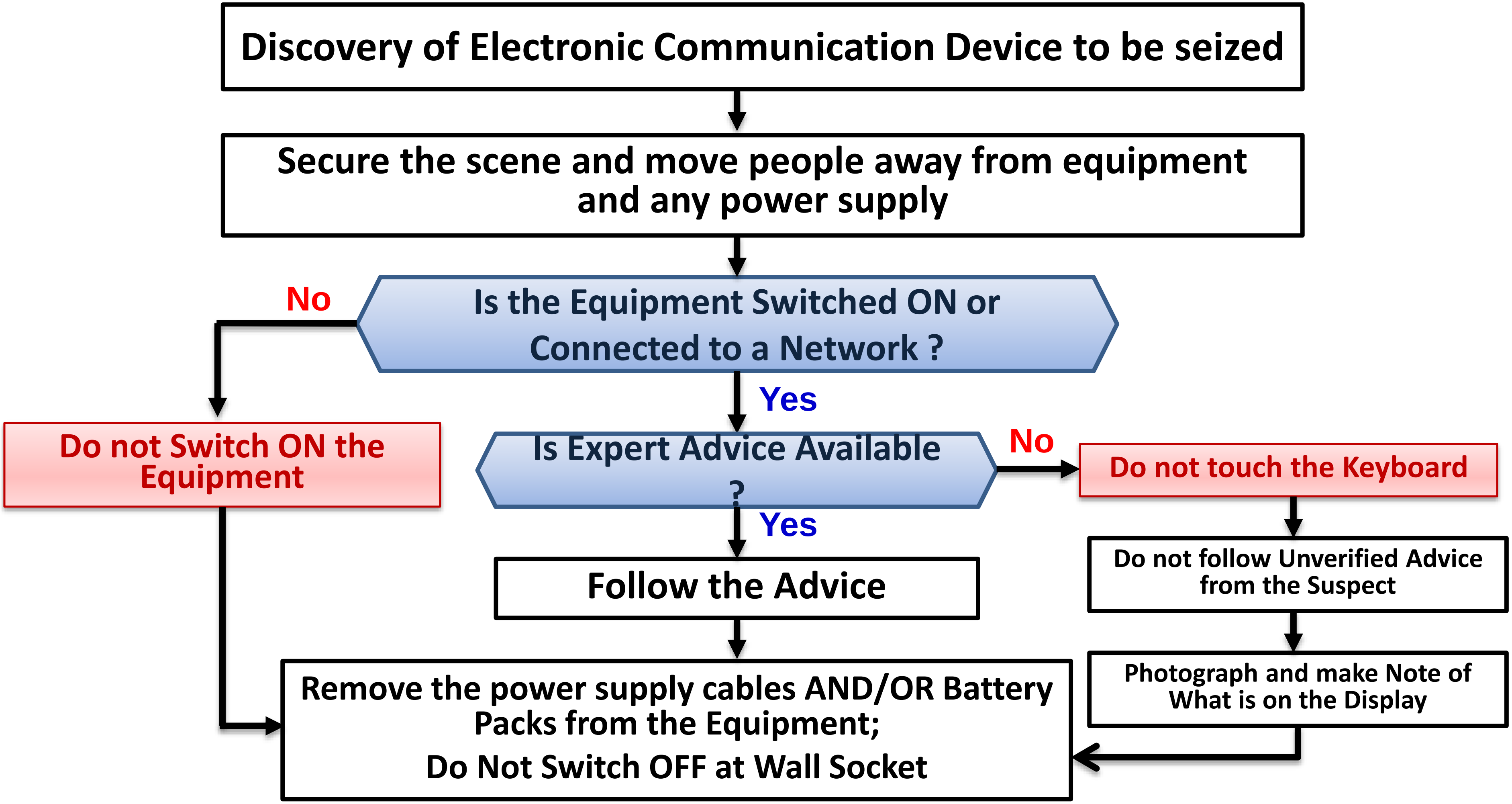
Secure the scene and move people away from equipment and any power supply

Is the Equipment Switched ON or Connected to a Network ?

No

Do not switch on the Equipment

Seizure of Electronic Equipment



Discovery of Electronic Communication Device to be seized

Secure the scene and move people away from equipment and any power supply

Is the Equipment Switched ON or Connected to a Network ?

No

Do not Switch ON the Equipment

Yes

Is Expert Advice Available ?

No

Do not touch the Keyboard

Do not follow Unverified Advice from the Suspect

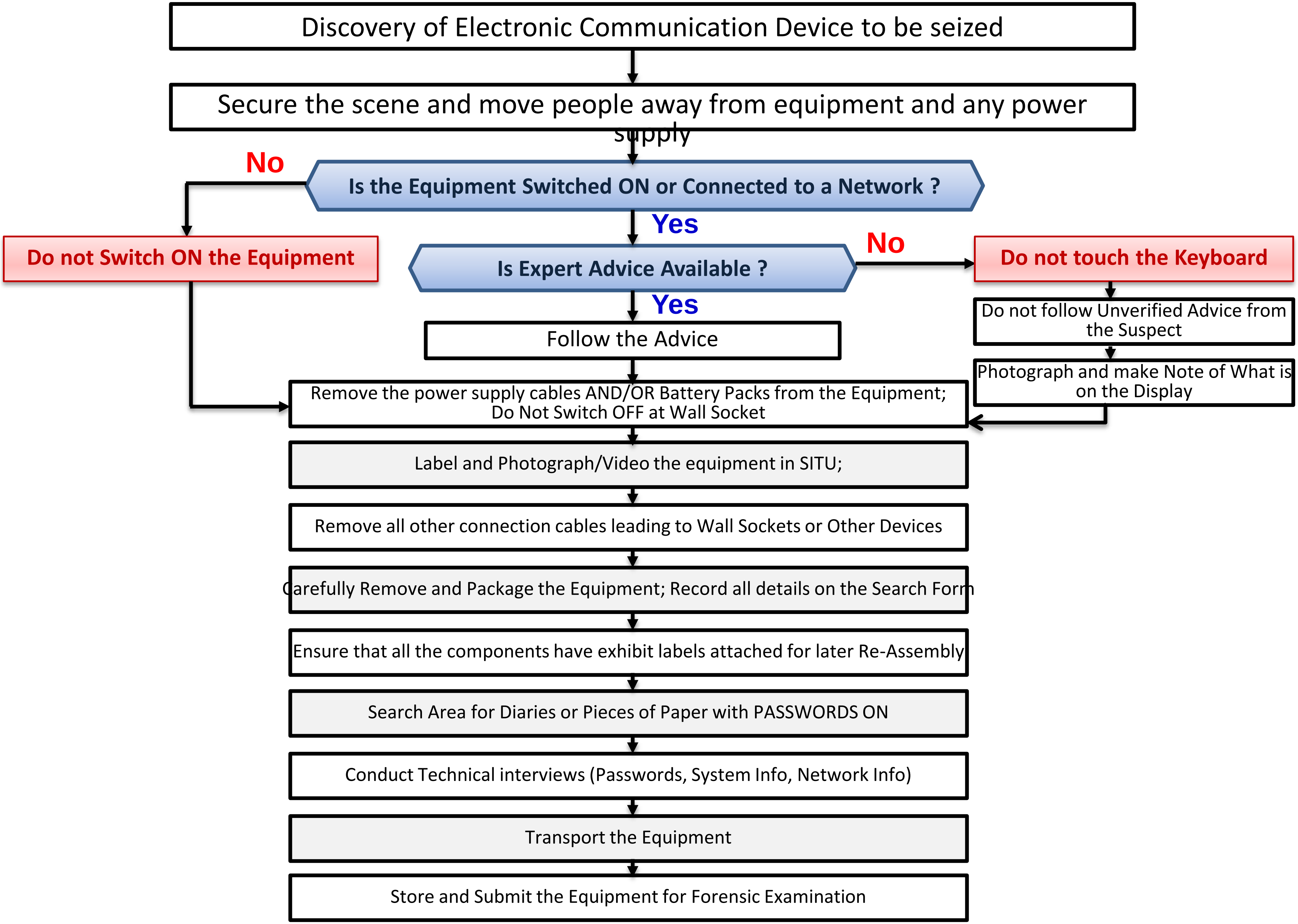
Photograph and make Note of What is on the Display

Yes

Follow the Advice

Remove the power supply cables AND/OR Battery Packs from the Equipment;
Do Not Switch OFF at Wall Socket

Seizure of Electronic Equipment



Discovery of Electronic Communication Device to be seized

Secure the scene and move people away from equipment and any power supply

Is the Equipment Switched ON or Connected to a Network ?

No

Do not Switch ON the Equipment

Yes

Is Expert Advice Available ?

No

Do not touch the Keyboard

Do not follow Unverified Advice from the Suspect

Photograph and make Note of What is on the Display

Yes

Follow the Advice

Remove the power supply cables AND/OR Battery Packs from the Equipment; Do Not Switch OFF at Wall Socket

Label and Photograph/Video the equipment in SITU;

Remove all other connection cables leading to Wall Sockets or Other Devices

Carefully Remove and Package the Equipment; Record all details on the Search Form

Ensure that all the components have exhibit labels attached for later Re-Assembly

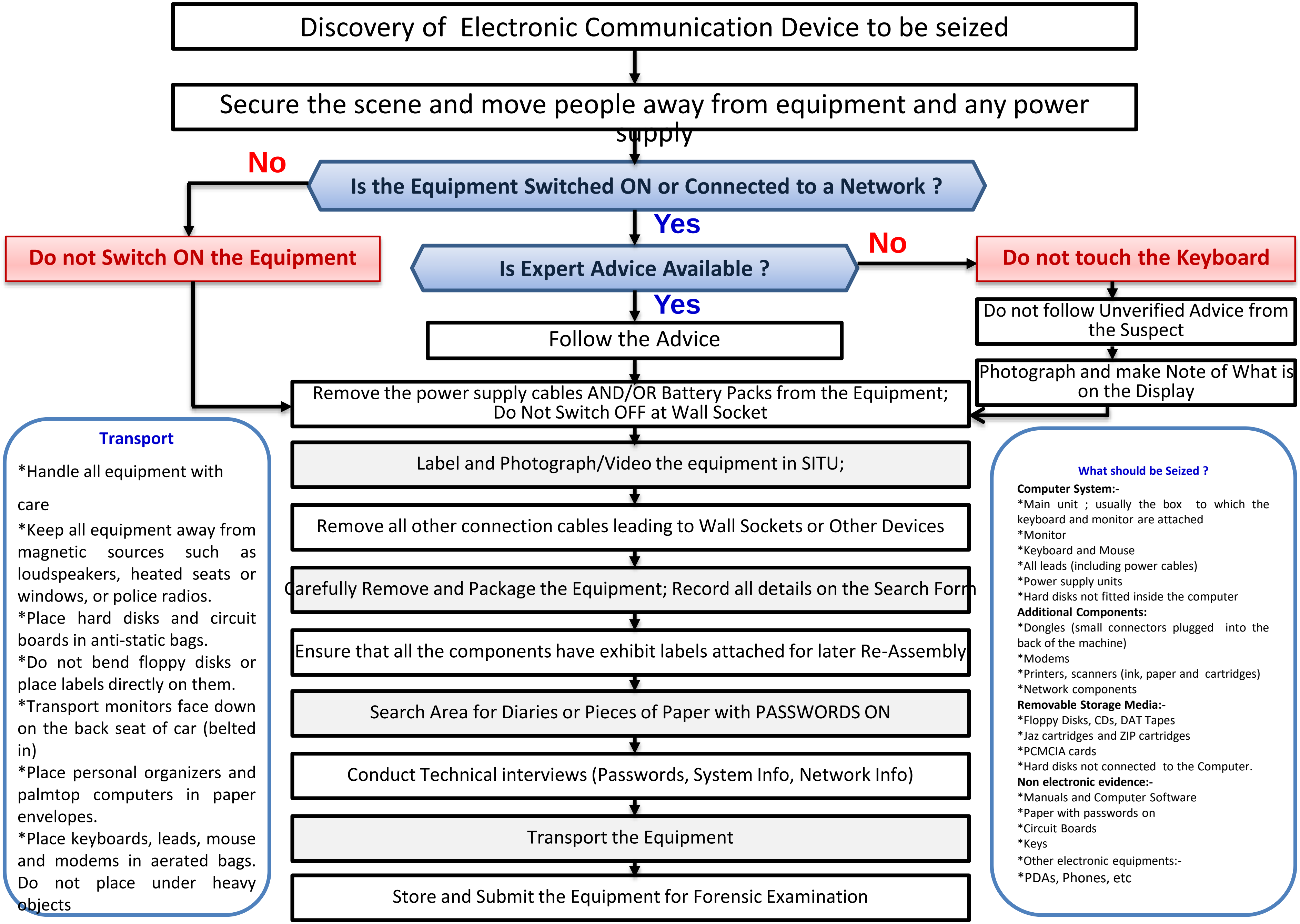
Search Area for Diaries or Pieces of Paper with PASSWORDS ON

Conduct Technical interviews (Passwords, System Info, Network Info)

Transport the Equipment

Store and Submit the Equipment for Forensic Examination

Seizure of Electronic Equipment



Discovery of Electronic Communication Device to be seized

Secure the scene and move people away from equipment and any power supply

Is the Equipment Switched ON or Connected to a Network ?

No

Do not Switch ON the Equipment

Yes

Is Expert Advice Available ?

No

Do not touch the Keyboard

Do not follow Unverified Advice from the Suspect

Photograph and make Note of What is on the Display

Yes

Follow the Advice

Remove the power supply cables AND/OR Battery Packs from the Equipment; Do Not Switch OFF at Wall Socket

Label and Photograph/Video the equipment in SITU;

Remove all other connection cables leading to Wall Sockets or Other Devices

Carefully Remove and Package the Equipment; Record all details on the Search Form

Ensure that all the components have exhibit labels attached for later Re-Assembly

Search Area for Diaries or Pieces of Paper with PASSWORDS ON

Conduct Technical interviews (Passwords, System Info, Network Info)

Transport the Equipment

Store and Submit the Equipment for Forensic Examination

Transport

*Handle all equipment with care

*Keep all equipment away from magnetic sources such as loudspeakers, heated seats or windows, or police radios.

*Place hard disks and circuit boards in anti-static bags.

*Do not bend floppy disks or place labels directly on them.

*Transport monitors face down on the back seat of car (belted in)

*Place personal organizers and palmtop computers in paper envelopes.

*Place keyboards, leads, mouse and modems in aerated bags. Do not place under heavy objects

What should be Seized ?

Computer System:-

*Main unit ; usually the box to which the keyboard and monitor are attached

*Monitor

*Keyboard and Mouse

*All leads (including power cables)

*Power supply units

*Hard disks not fitted inside the computer

Additional Components:

*Dongles (small connectors plugged into the back of the machine)

*Modems

*Printers, scanners (ink, paper and cartridges)

*Network components

Removable Storage Media:-

*Floppy Disks, CDs, DAT Tapes

*Jaz cartridges and ZIP cartridges

*PCMCIA cards

*Hard disks not connected to the Computer.

Non electronic evidence:-

*Manuals and Computer Software

*Paper with passwords on

*Circuit Boards

*Keys

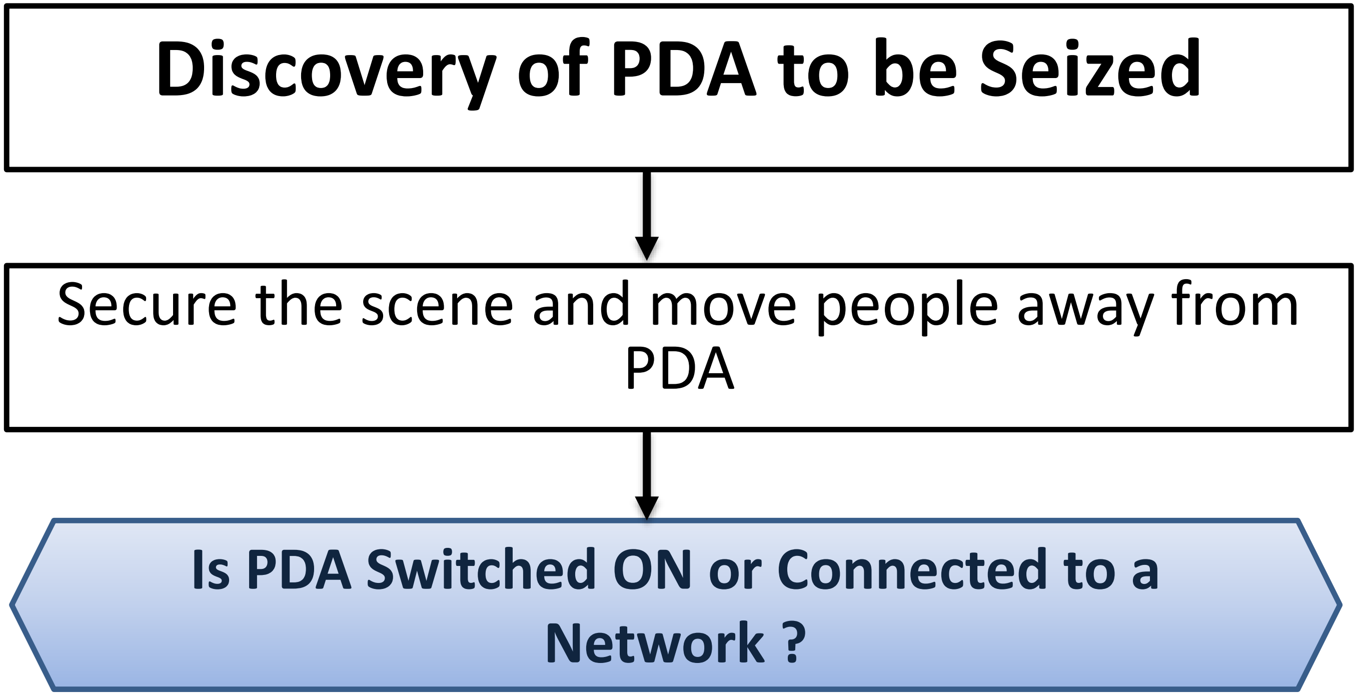
*Other electronic equipments:-

*PDAs, Phones, etc

Flowchart/Pocket guide : Handheld devices (PDAs)

Discovery of PDA to be Seized

Flowchart/Pocket guide : Handheld devices (PDAs)

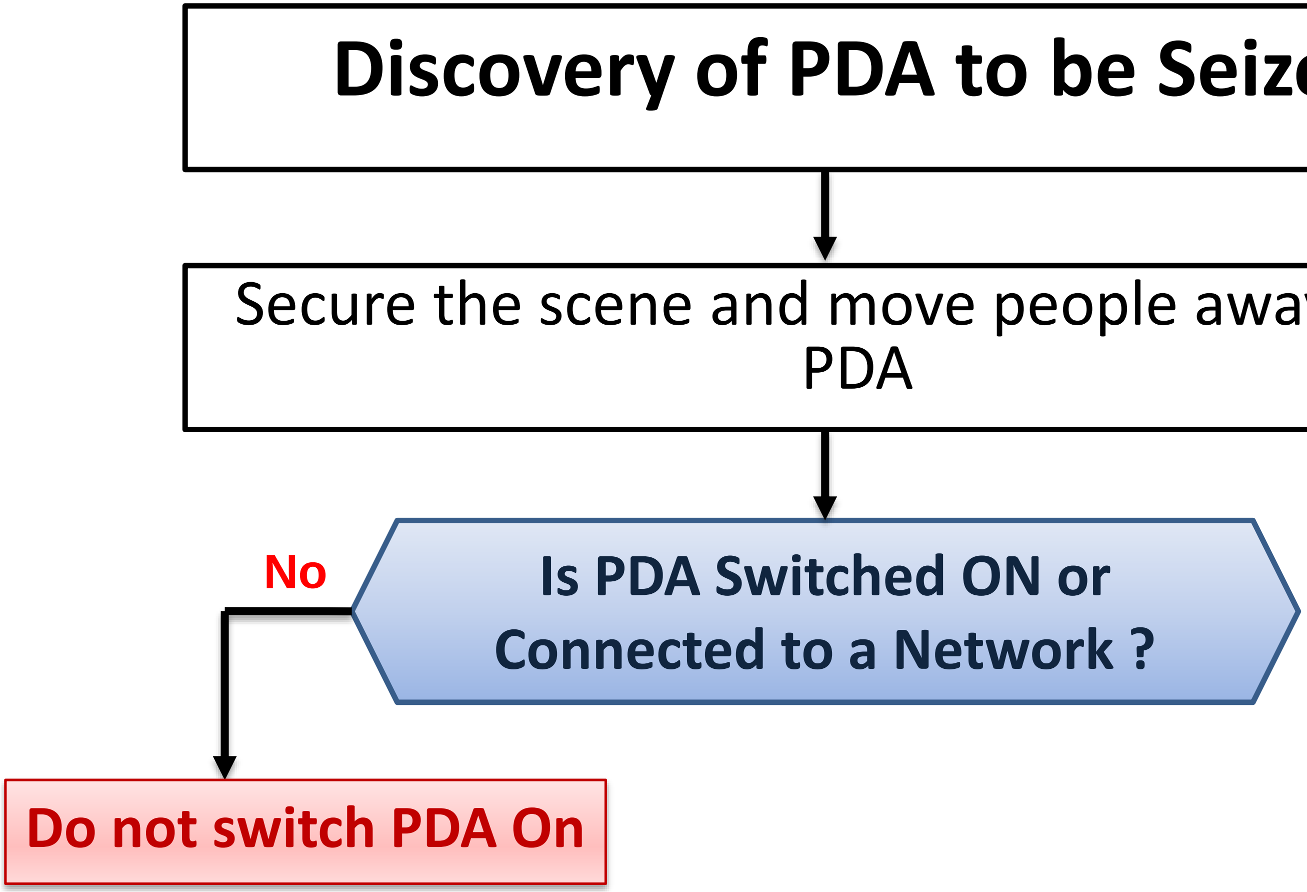


Discovery of PDA to be Seized

Secure the scene and move people away from PDA

Is PDA Switched ON or Connected to a Network ?

Flowchart/Pocket guide : Handheld devices (PDAs)



Discovery of PDA to be Seized

Secure the scene and move people away from PDA

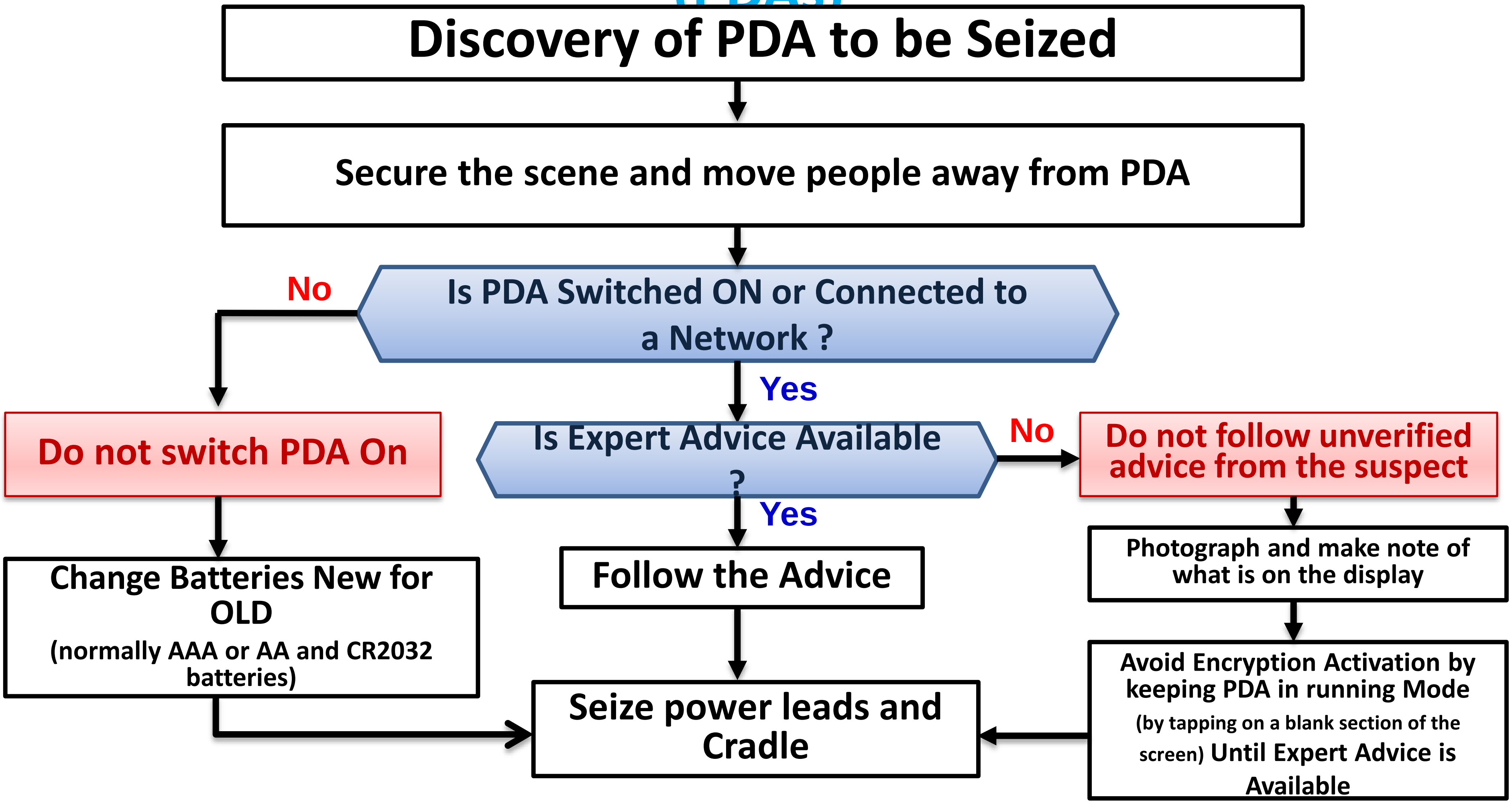
Is PDA Switched ON or Connected to a Network ?

No

Do not switch PDA On

CERTIFIED FORENSIC COMPUTER EXAMINER IACIS

Flowchart/Pocket guide : Handheld devices (PDAs)



Discovery of PDA to be Seized

Secure the scene and move people away from PDA

Is PDA Switched ON or Connected to a Network ?

No

Do not switch PDA On

Change Batteries New for OLD

(normally AAA or AA and CR2032 batteries)

Yes

Is Expert Advice Available ?

Yes

Follow the Advice

No

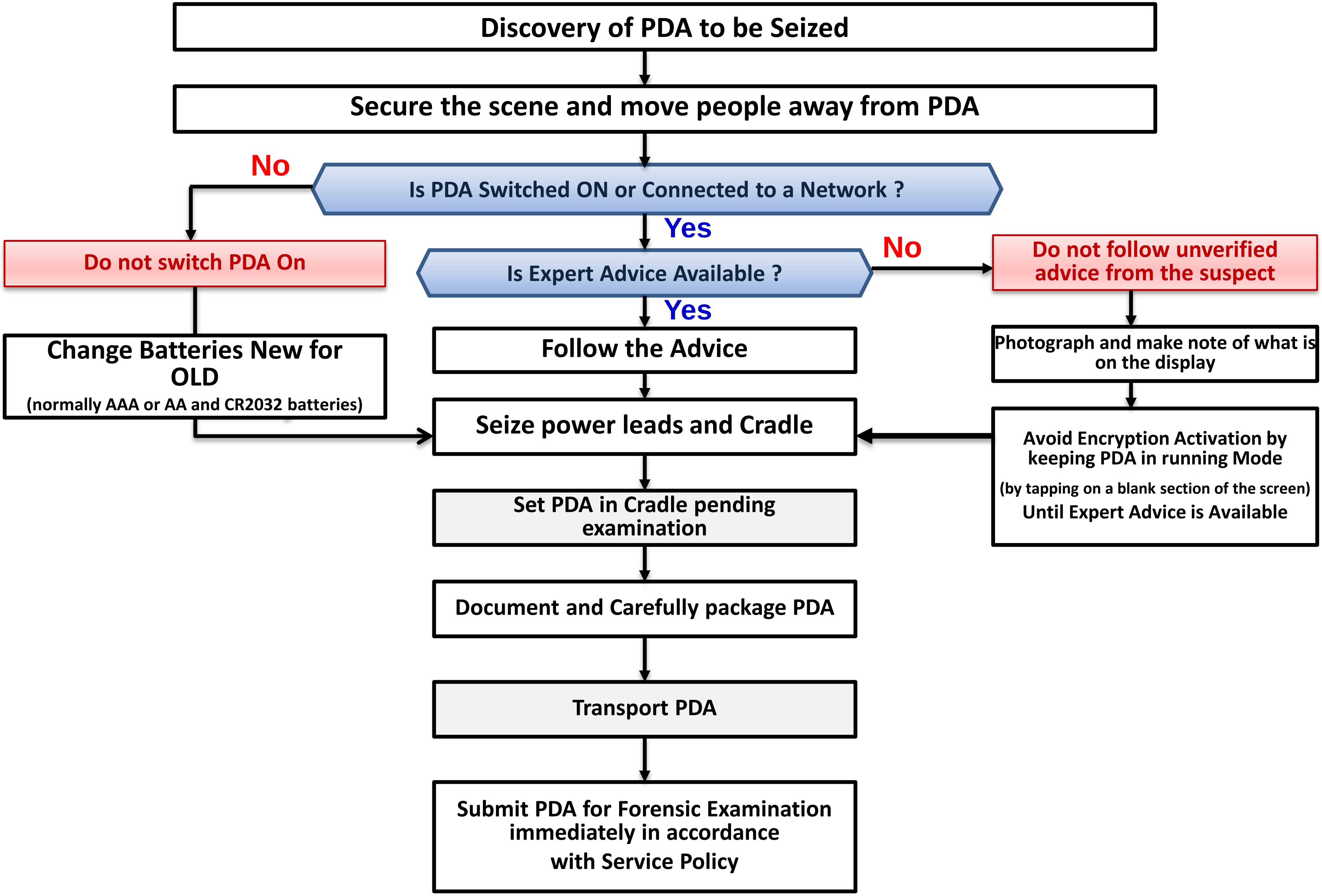
Do not follow unverified advice from the suspect

Photograph and make note of what is on the display

Avoid Encryption Activation by keeping PDA in running Mode (by tapping on a blank section of the screen) Until Expert Advice is Available

Seize power leads and Cradle

Flowchart/Pocket guide : Handheld devices (PDAs)



Discovery of PDA to be Seized

Secure the scene and move people away from PDA

Is PDA Switched ON or Connected to a Network ?

No

Do not switch PDA On

Change Batteries New for OLD

(normally AAA or AA and CR2032 batteries)

Yes

Is Expert Advice Available ?

No

Do not follow unverified advice from the suspect

Photograph and make note of what is on the display

Avoid Encryption Activation by keeping PDA in running Mode

(by tapping on a blank section of the screen)

Until Expert Advice is Available

Yes

Follow the Advice

Seize power leads and Cradle

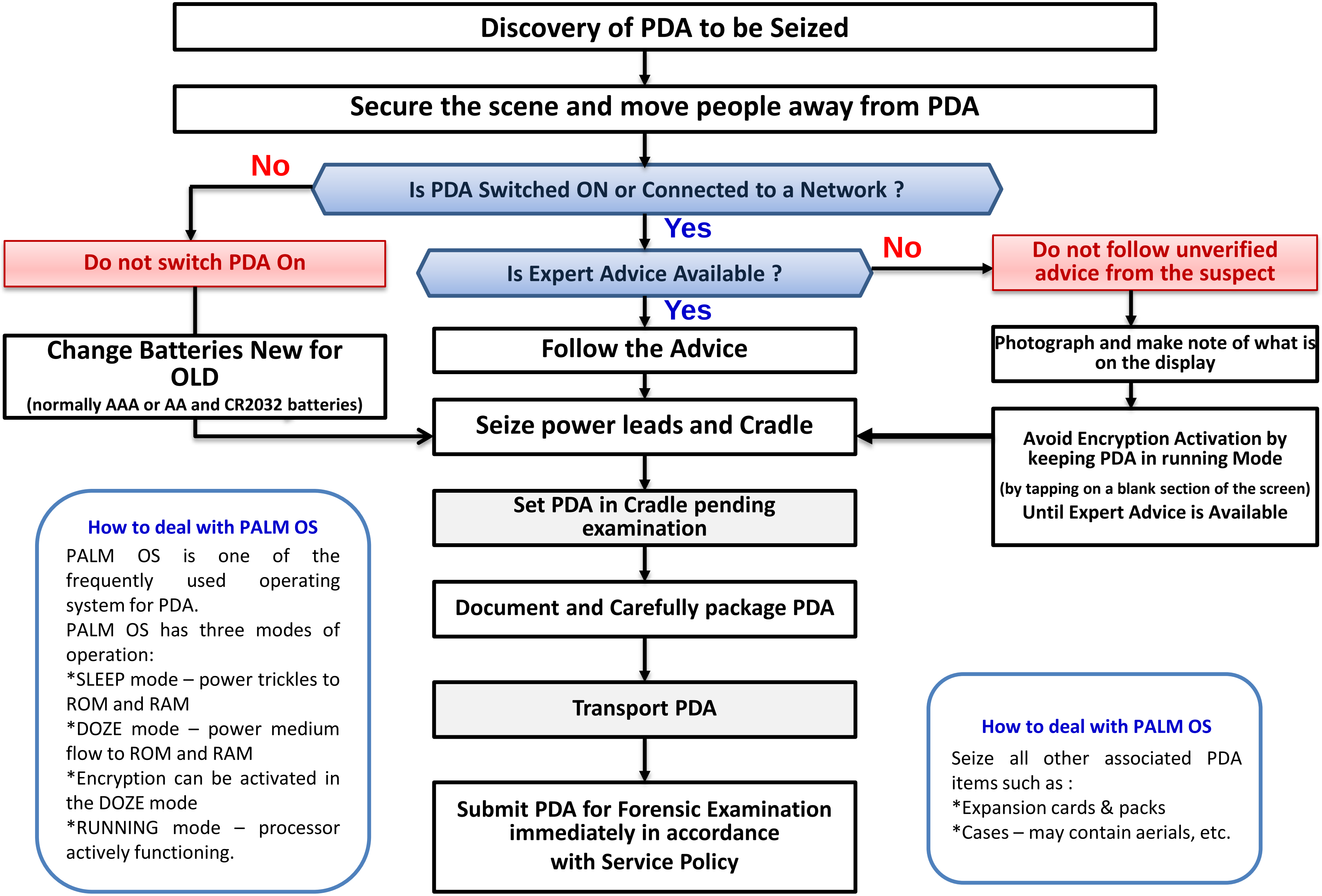
Set PDA in Cradle pending examination

Document and Carefully package PDA

Transport PDA

Submit PDA for Forensic Examination immediately in accordance with Service Policy

Flowchart/Pocket guide : Handheld devices (PDAs)



Discovery of PDA to be Seized

Secure the scene and move people away from PDA

Is PDA Switched ON or Connected to a Network ?

No

Do not switch PDA On

Change Batteries New for OLD

(normally AAA or AA and CR2032 batteries)

Yes

Is Expert Advice Available ?

Yes

Follow the Advice

No

Do not follow unverified advice from the suspect

Photograph and make note of what is on the display

Avoid Encryption Activation by keeping PDA in running Mode

(by tapping on a blank section of the screen)

Until Expert Advice is Available

Seize power leads and Cradle

Set PDA in Cradle pending examination

Document and Carefully package PDA

Transport PDA

Submit PDA for Forensic Examination immediately in accordance with Service Policy

How to deal with PALM OS

PALM OS is one of the frequently used operating system for PDA.

PALM OS has three modes of operation:

*SLEEP mode – power trickles to ROM and RAM

*DOZE mode – power medium flow to ROM and RAM

*Encryption can be activated in the DOZE mode

*RUNNING mode – processor actively functioning.

How to deal with PALM OS

Seize all other associated PDA items such as :

*Expansion cards & packs

*Cases – may contain aerials, etc.

Chain of custody

- **Chain of Custody – A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for any transfers**

- **SOP**

Types of Digital Forensics

- 1.Computer Forensics.
- 2. Network Forensics.
- 3.Mobile device Forensics.
- 4. IoT Forensics.
- 5. Cloud Forensics
- 6. Voice Forensics
- 7.Photo Forensics

Forensic copy or image?

- Forensic image?

- Forensic copy?

Deleting a file

- when a file is simply deleted or erased pointers to the file are "zeroed” (i.e. alterations are made to the FAT or MFT) so that at the logical level the file does not appear to the user, but at the physical level the file data is still intact on the media and may be recovered.

Wiping a file

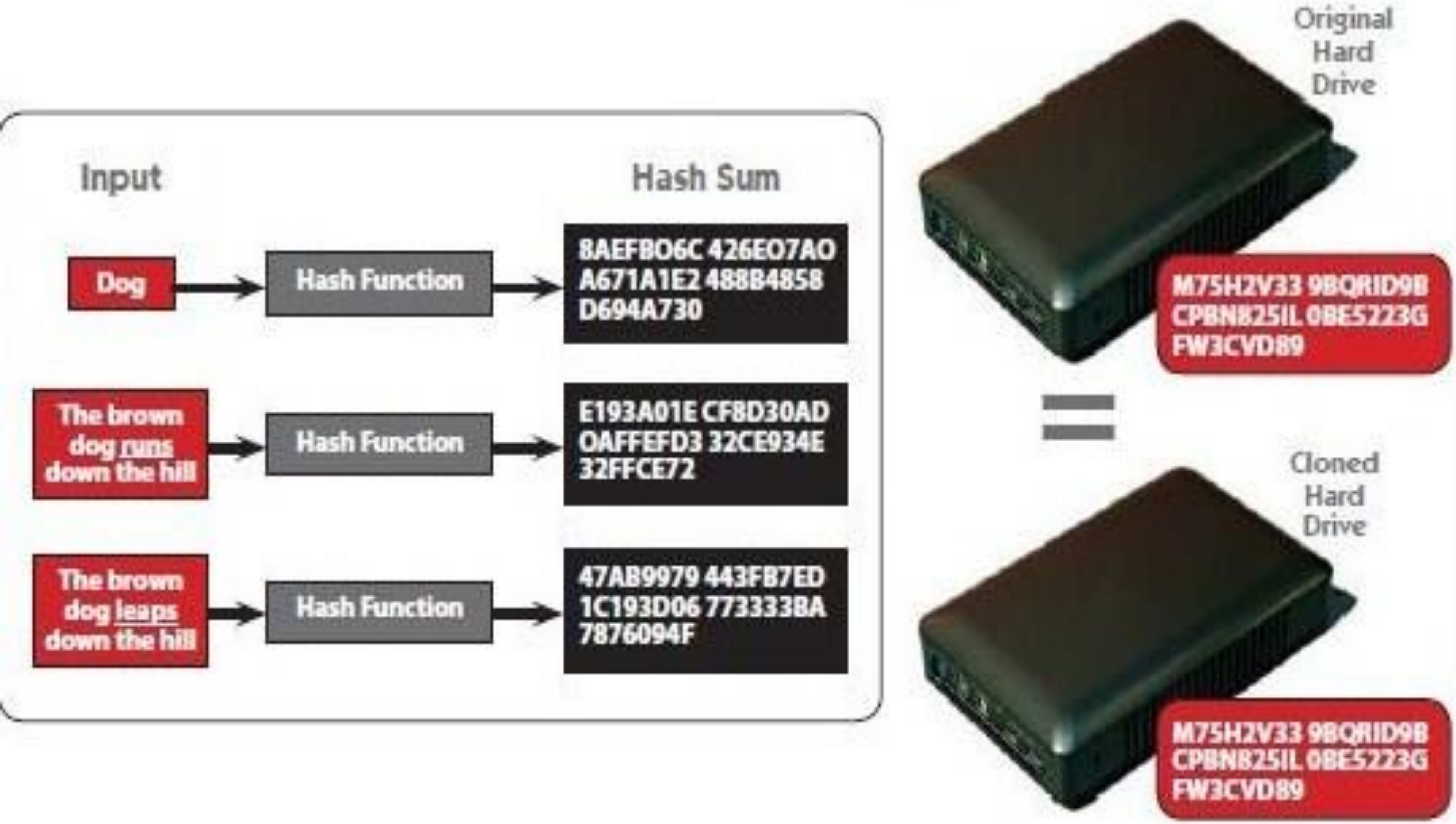
- when a file is wiped the entirety of the file is overwritten by a known or random hex character or pattern rendering it unrecoverable

Hash values

- Hash values can be thought of as fingerprints for files.
- ○ Way to represent a piece of Electronic data with a unique numerical value 'Hash Value' by applying a mathematical algorithm to the data
- ○ Two files with exactly the same bit patterns should hash to the same value using the same hashing algorithm
- Two algorithms are currently widely used to produce hash values: the MD5 and SHA1 algorithms.
  - MD5: 464668D58274A7840E264E8739884247
  - SHA-1: 4698215F643BECFF6C6F3D2BF447ACE0C067149F

How Are Evidence Copies Verified?

The Hash Value (Thumbprint) of the Source and Copied Data are Compared



Input

Hash Sum

Dog

Hash Function

8AEFBO6C 426EO7AO
A671A1E2 488B4858
D694A730

The brown dog runs down the hill

Hash Function

E193A01E CF8D30AD
OAFFEFD3 32CE934E
32FFCE72

The brown dog leaps down the hill

Hash Function

47AB9979 443FB7ED
1C193D06 773333BA
7876094F

Original Hard Drive

M75H2V33 9BQRID9B
CPBN825IL 0BE5223G
FW3CVD89

=

Cloned Hard Drive

M75H2V33 9BQRID9B
CPBN825IL 0BE5223G
FW3CVD89

Uses of Hashing

- Verification: (file, partition, disk drive, media device) has not changed.

- Hashing is a way to identify and eliminate from analysis all files that contain no potential evidence. E.g. Software files.

Programs that Utilize Hash Functions

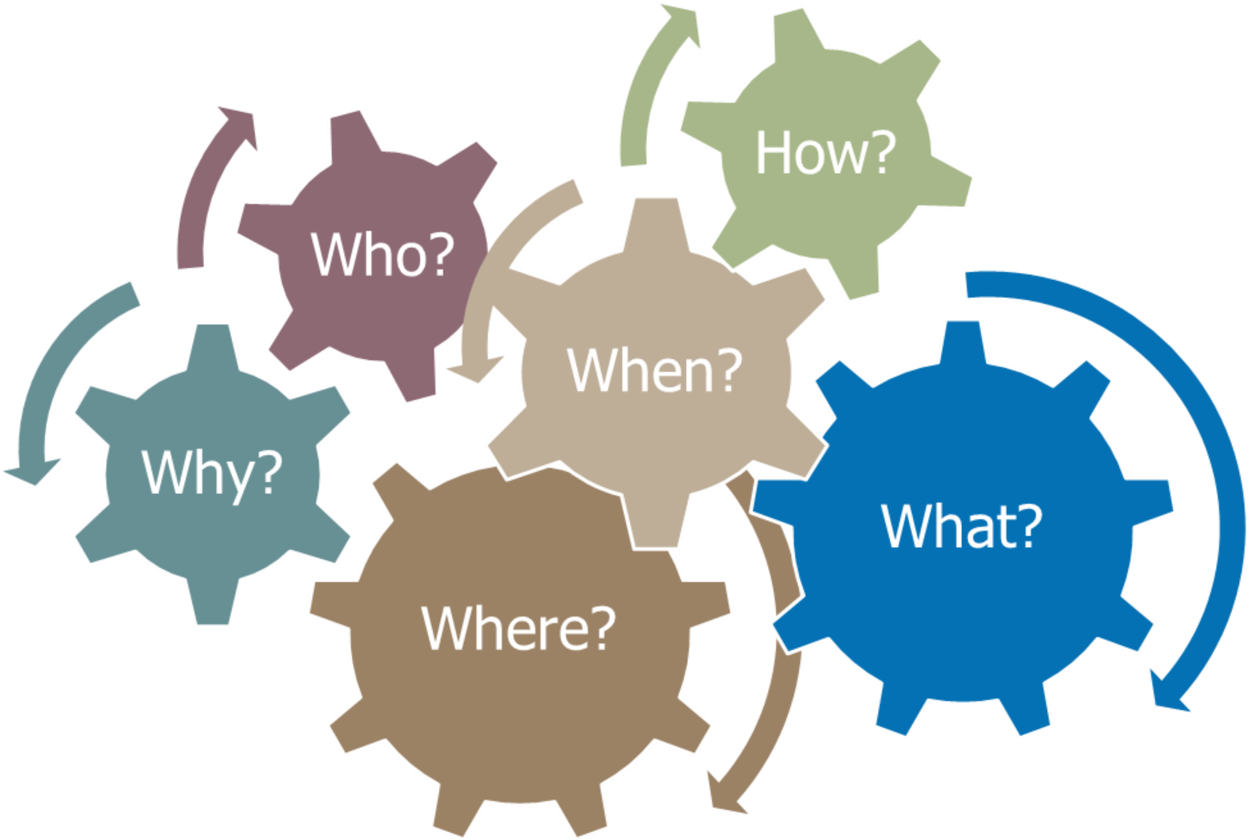
- HashCalc
- SPADA – provided to IACIS members
- FTK Imager: www.accessdata.com
- Encase, Cyber Check suite etc.
- Karen’s Power Tools
  - http://www.karenware.com/powertools/pthasher.asp
- Jacksum: http://sourceforge.net/projects/jacksum/
- CyoHash: http://cyohash.sourceforge.net/

No notifications for Cyber lab?

- In the absence of Notifications u/s79A of IT Act 2000

- Provisions under 293 Crpc is admissible

Meta data



Data Reporting

Who	• created the data? • manages the data?
Where	• is the study area? • can I access the data?
What	• is the data content? • source data was used?
How	• was the data created? • is the data distributed?
When	• is the time period of the content? • was the data created?
Why	• was the data created? • are there missing values?

Social Media

- Online Social Networking (OSN)
- More than 200 Social Network sites,
- only 15 are most popular Social networks based on number users Viz
- Face book, twitter whats app, YouTube etc.

Social Media Issues

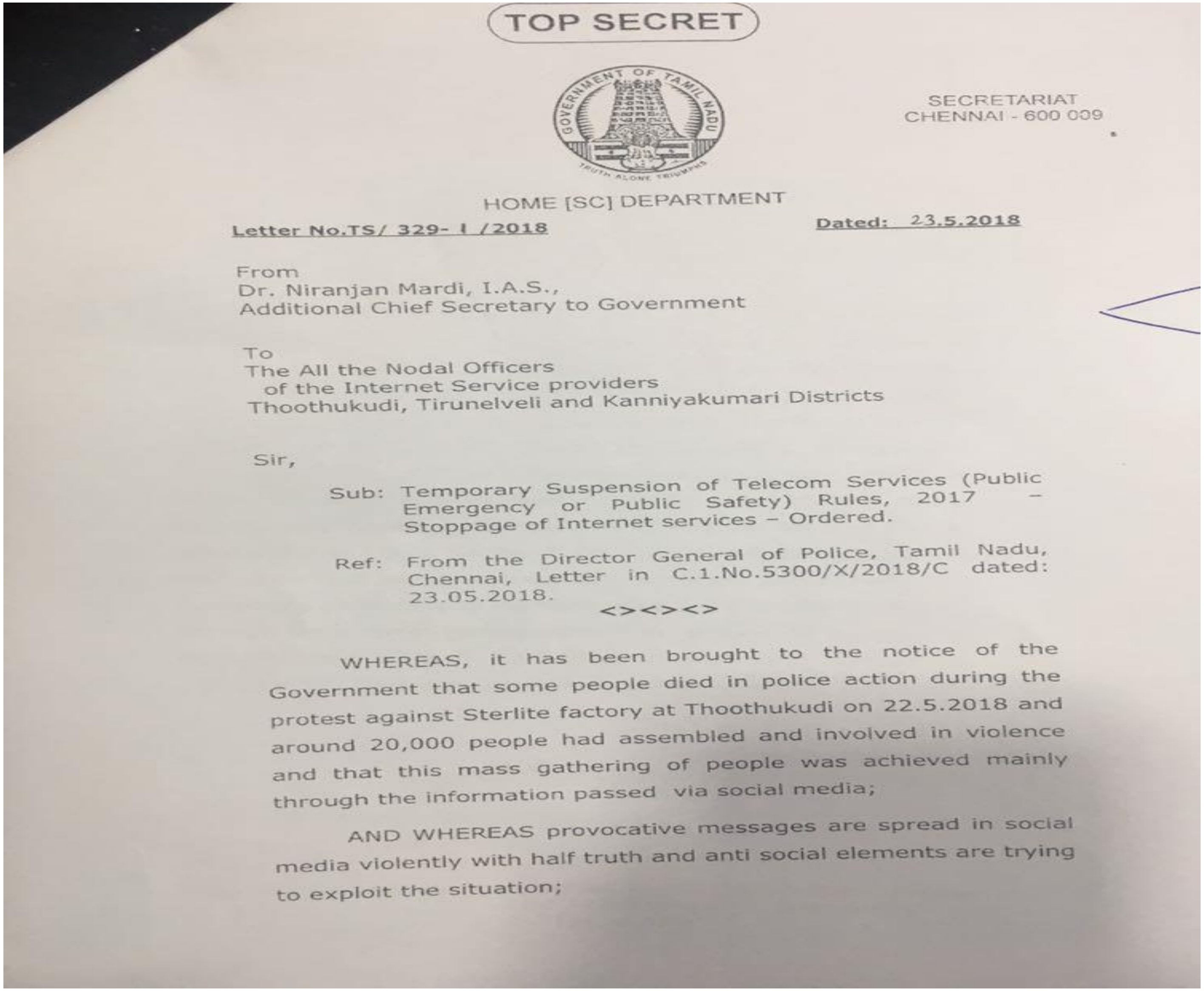
- 1.Harrasment,humilations,cyber bullying
- 2.Use,misuse and Abuse of Art .19 of Indian Constitution: Freedom of Speech
- 3.Sec 506, 153,A,B IPC , 354A, 354B, 354C and 354D IPC
- 4. Netizen Rights
- Ban on Social Media
- Sec 144 Crpc
- Sec 5 and 7 of ITA 1885

Internet ban by States

- **Section 144 of the CrPC.**
  Gaurav Sureshbhai Vas Vs State of Gujarat 2016

- **section 7 of the Indian Telegraph Act, 1885**

  Rule 2(1)Temporary Suspension of Telecom Services
  (Public Emergencies or Public Safety) Rules 2017.



TOP SECRET

SECRETARIAT
CHENNAI - 600 009

HOME [SC] DEPARTMENT

Letter No.TS/ 329- I /2018 **Dated: 23.5.2018**

From
Dr. Niranjan Mardi, I.A.S.,
Additional Chief Secretary to Government

To
The All the Nodal Officers
of the Internet Service providers
Thoothukudi, Tirunelveli and Kanniyakumari Districts

Sir,

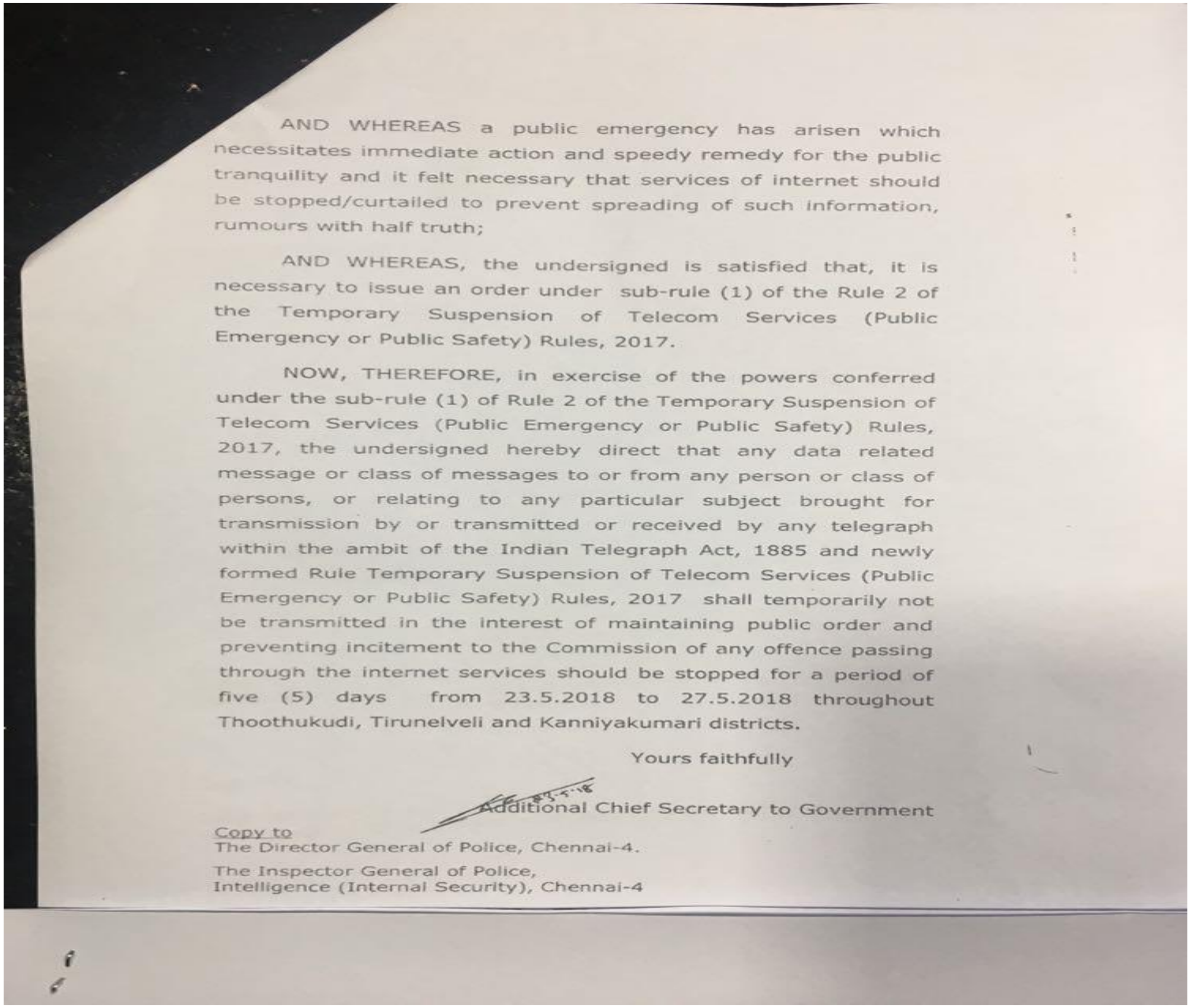
Sub: Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 – Stoppage of Internet services – Ordered.

Ref: From the Director General of Police, Tamil Nadu, Chennai, Letter in C.1.No.5300/X/2018/C dated: 23.05.2018.

<><><>

WHEREAS, it has been brought to the notice of the Government that some people died in police action during the protest against Sterlite factory at Thoothukudi on 22.5.2018 and around 20,000 people had assembled and involved in violence and that this mass gathering of people was achieved mainly through the information passed via social media;

AND WHEREAS provocative messages are spread in social media violently with half truth and anti social elements are trying to exploit the situation;



AND WHEREAS a public emergency has arisen which necessitates immediate action and speedy remedy for the public tranquility and it felt necessary that services of internet should be stopped/curtailed to prevent spreading of such information, rumours with half truth;

AND WHEREAS, the undersigned is satisfied that, it is necessary to issue an order under sub-rule (1) of the Rule 2 of the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017.

NOW, THEREFORE, in exercise of the powers conferred under the sub-rule (1) of Rule 2 of the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, the undersigned hereby direct that any data related message or class of messages to or from any person or class of persons, or relating to any particular subject brought for transmission by or transmitted or received by any telegraph within the ambit of the Indian Telegraph Act, 1885 and newly formed Rule Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 shall temporarily not be transmitted in the interest of maintaining public order and preventing incitement to the Commission of any offence passing through the internet services should be stopped for a period of five (5) days from 23.5.2018 to 27.5.2018 throughout Thoothukudi, Tirunelveli and Kanniyakumari districts.

Yours faithfully

23-5-18

Additional Chief Secretary to Government

Copy to
The Director General of Police, Chennai-4.

The Inspector General of Police,
Intelligence (Internal Security), Chennai-4

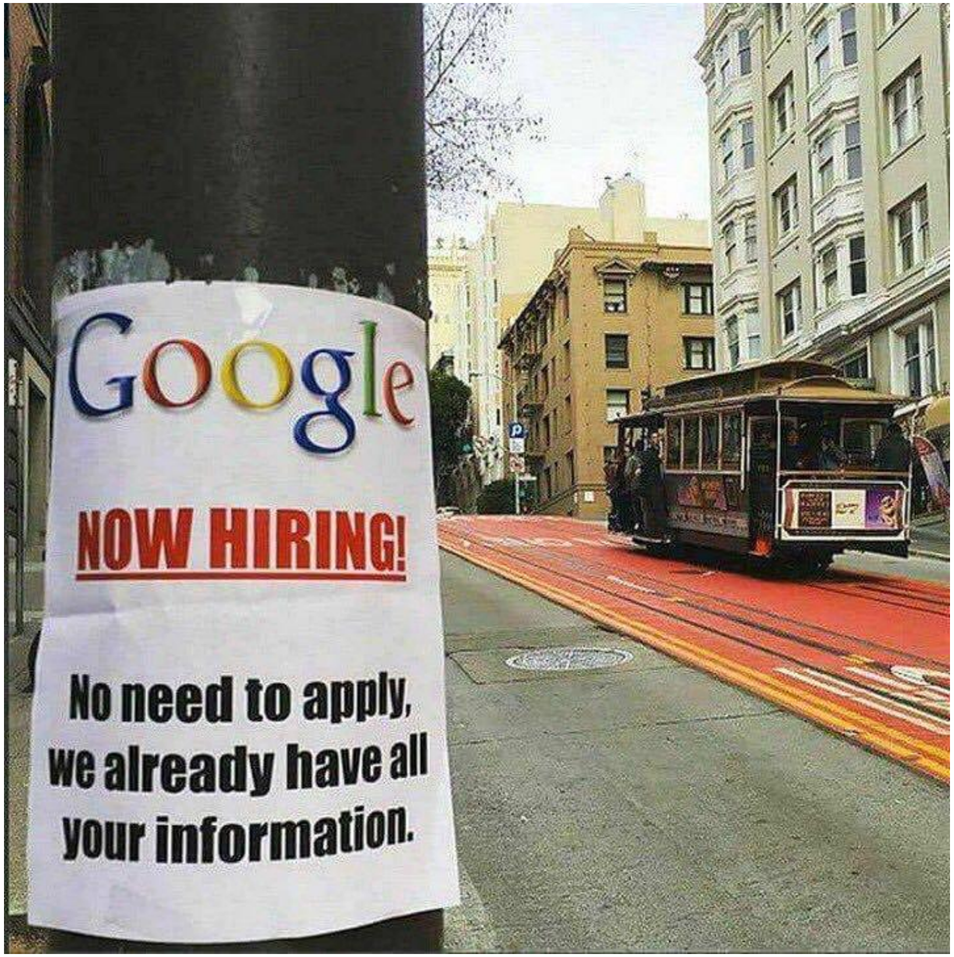
Room No 632

K.R.Ramamoorthi

26-11-2008

Google

- Google knows you better than you know yourself!
- Google does not forget
- Google does not delete
- Over 254 Google Products & Services You Probably Don’t Know


Google
NOW HIRING!
No need to apply,
we already have all
your information.

Rotten Apple

Android atrocities

- You are not the Customer

  You are the Product.
- Cookies
- Google maps
- Gmail issues

Anti virus

- 65 companies

- 100billion business

Google My Activity

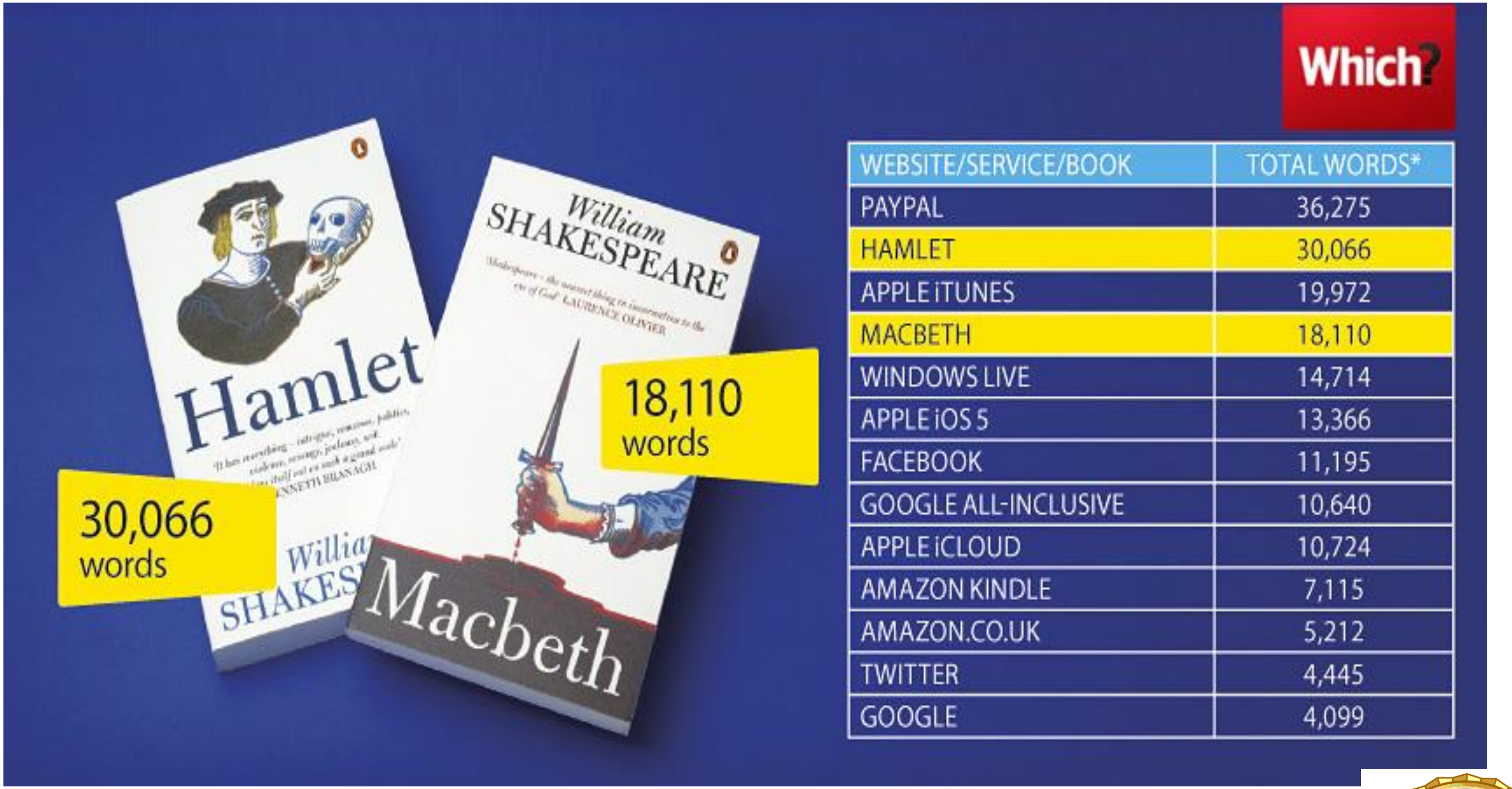
- https://myactivity.google.com/myactivity
- 1.Activity controls
- 2.Web & App Activity
- 3.Location History
- 4.Device Information
- 5.Voice & Audio Activity
- 6.YouTube Search History
- 7.YouTube Watch History

How many words in the English language?

- 171,476 words (approximately)

- The Second Edition of the 20-volume Oxford English Dictionary contains full entries for 171,476 words in current use,

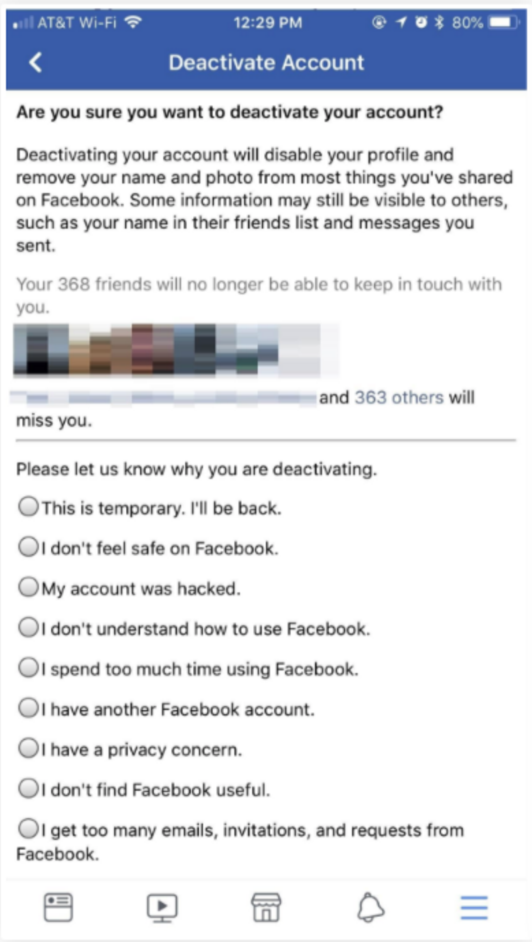
Terms and Conditions (against You)


Which?
Hamlet
William SHAKESPEARE
Macbeth
30,066 words
18,110 words

WEBSITE/SERVICE/BOOK	TOTAL WORDS*
PAYPAL	36,275
HAMLET	30,066
APPLE iTUNES	19,972
MACBETH	18,110
WINDOWS LIVE	14,714
APPLE iOS 5	13,366
FACEBOOK	11,195
GOOGLE ALL-INCLUSIVE	10,640
APPLE iCLOUD	10,724
AMAZON KINDLE	7,115
AMAZON.CO.UK	5,212
TWITTER	4,445
GOOGLE	4,099

MY DAD TOLD ME YOU'RE SPYING ON US
HE'S NOT YOUR DAD
imgflip.com

HOW TO DEACTIVATE



AT&T Wi-Fi 12:29 PM 80%

Deactivate Account

Are you sure you want to deactivate your account?

Deactivating your account will disable your profile and remove your name and photo from most things you've shared on Facebook. Some information may still be visible to others, such as your name in their friends list and messages you sent.

Your 368 friends will no longer be able to keep in touch with you.

[redacted] and 363 others will miss you.

Please let us know why you are deactivating.

○ This is temporary. I'll be back.

○ I don't feel safe on Facebook.

○ My account was hacked.

○ I don't understand how to use Facebook.

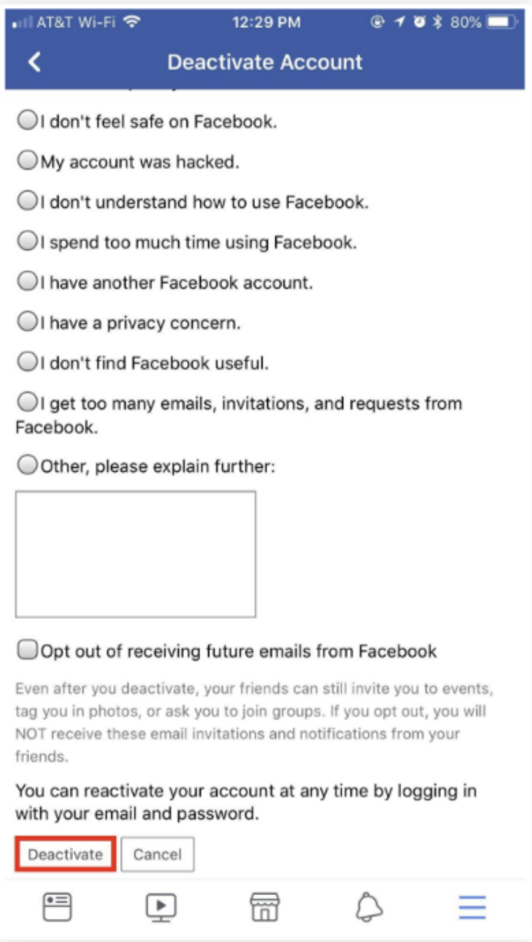
○ I spend too much time using Facebook.

○ I have another Facebook account.

○ I have a privacy concern.

○ I don't find Facebook useful.

○ I get too many emails, invitations, and requests from Facebook.



AT&T Wi-Fi 12:29 PM 80%

Deactivate Account

○ I don't feel safe on Facebook.

○ My account was hacked.

○ I don't understand how to use Facebook.

○ I spend too much time using Facebook.

○ I have another Facebook account.

○ I have a privacy concern.

○ I don't find Facebook useful.

○ I get too many emails, invitations, and requests from Facebook.

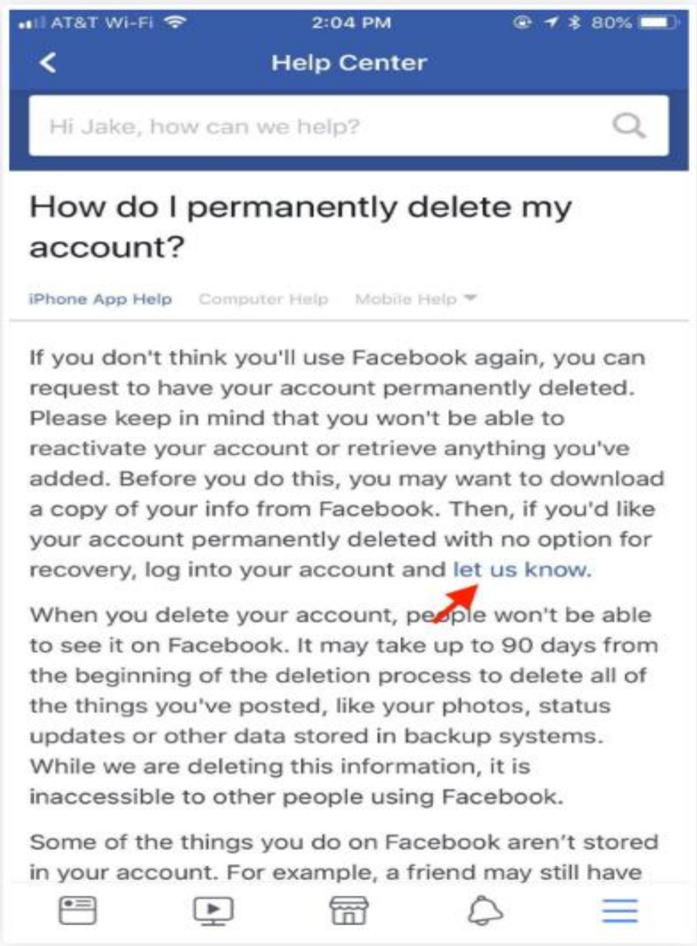
○ Other, please explain further:

□ Opt out of receiving future emails from Facebook

Even after you deactivate, your friends can still invite you to events, tag you in photos, or ask you to join groups. If you opt out, you will NOT receive these email invitations and notifications from your friends.

You can reactivate your account at any time by logging in with your email and password.

Method 2 — Deleting Your Account (Permanent)

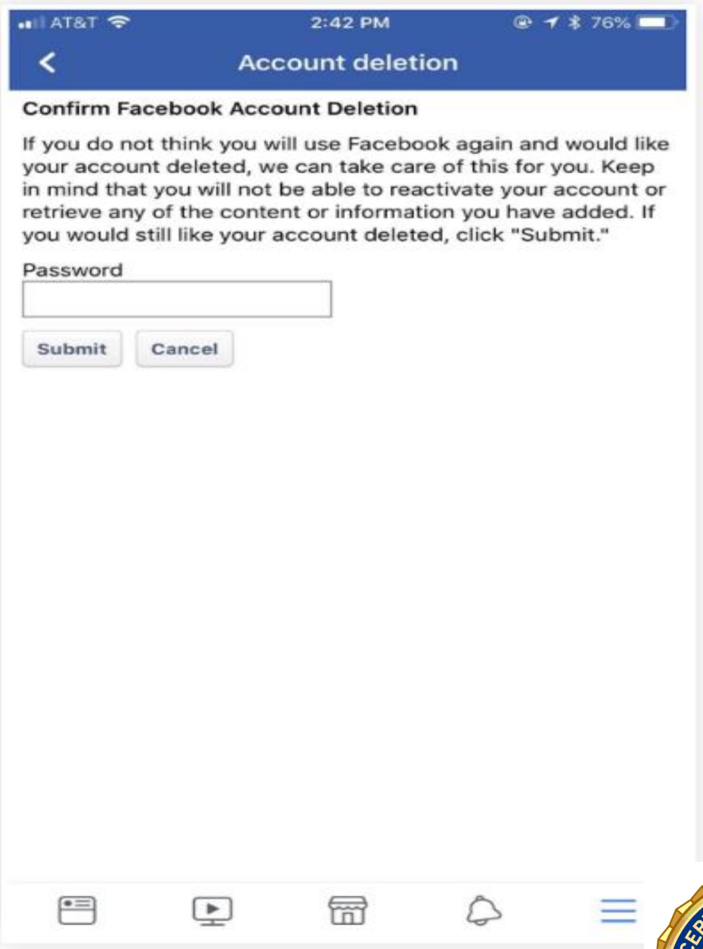


How do I permanently delete my account?

If you don't think you'll use Facebook again, you can request to have your account permanently deleted. Please keep in mind that you won't be able to reactivate your account or retrieve anything you've added. Before you do this, you may want to download a copy of your info from Facebook. Then, if you'd like your account permanently deleted with no option for recovery, log into your account and let us know.

When you delete your account, people won't be able to see it on Facebook. It may take up to 90 days from the beginning of the deletion process to delete all of the things you've posted, like your photos, status updates or other data stored in backup systems. While we are deleting this information, it is inaccessible to other people using Facebook.

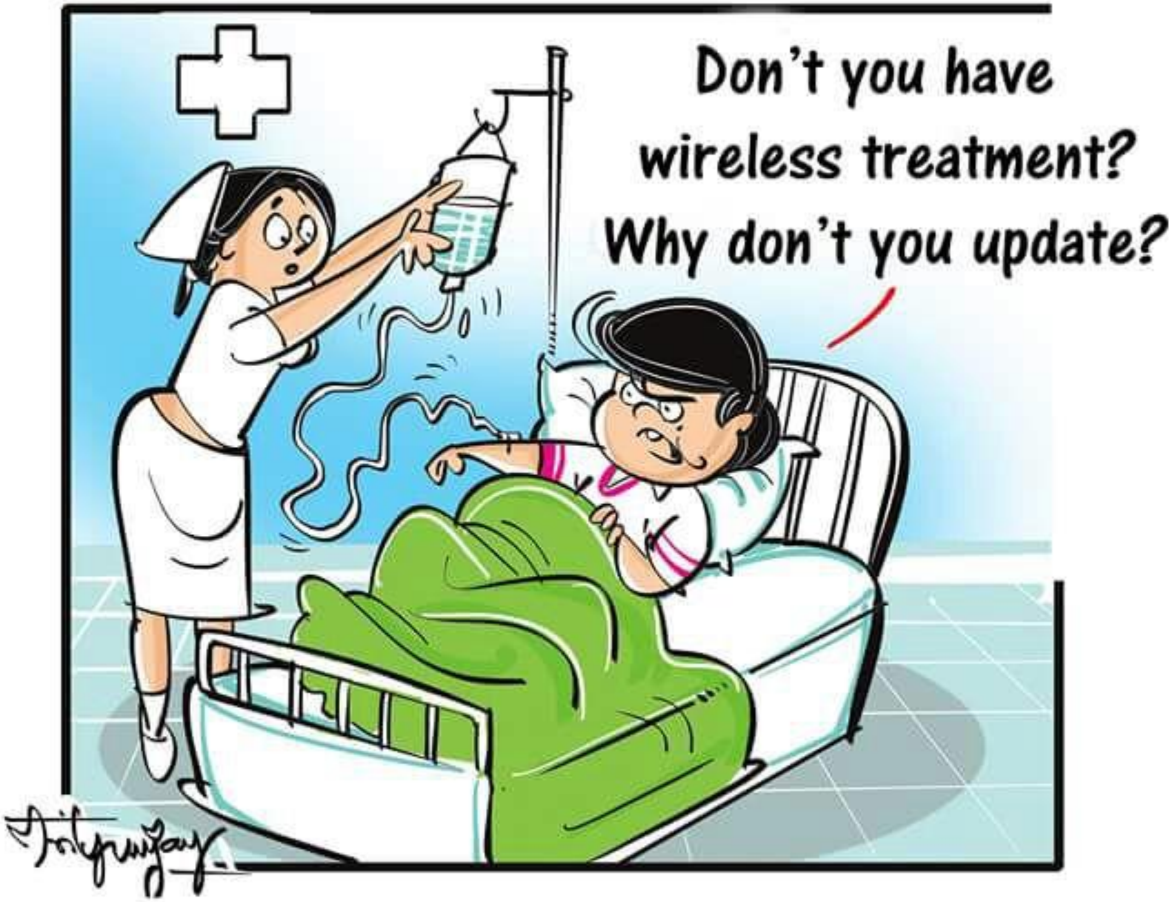
Some of the things you do on Facebook aren't stored in your account. For example, a friend may still have



Confirm Facebook Account Deletion

If you do not think you will use Facebook again and would like your account deleted, we can take care of this for you. Keep in mind that you will not be able to reactivate your account or retrieve any of the content or information you have added. If you would still like your account deleted, click "Submit."

Password


Don't you have wireless treatment? Why don't you update?

Free wifi

- All the Airports are connected with free wifi for an hour at lest to all by service providers

- Google has installed free wifis on 140 railway stations

- Google not only has access to all your search records but also to metadata/search analytics from all your connected devices now.

How to See Who's On Your Wi-Fi?

- Wireless Network Watcher
- Who Is On My WiFi from the Mac App Store.

- Both tools will provide a list of every device currently connected to your network, so you can identify the ones that belong to you.

Are you safe with your e mail Accounts?

Gmail,yahoo,etc not safe

No social media platform is safe

.ios/ icloud also not safe!

Use privacy settings pl

Use your own e mail accounts..

Which is the safe e mail?

1.CounterMail

2. Protonmail
3. Hushmail
4. Mailfence
5. Tutanota

Email encryption

Institutions e mails

Driver behaviour service

IBM Watson IoT Driver Behaviour Service lets you analyze drivers' behavior from vehicle probe data and contextual data

You can analyze driver behavior such as harsh acceleration and harsh braking, frequent braking, speeding, sharp turn, and so on.

Useful for Accident/ Insurance cases investigations!

EE: 2020 Vision…

- Software will disrupt most traditional industries in the next 5-10 years.
  - Uber
  - Airbnb
  - IBM Watson,
- Autonomous cars:
- In 2018 the first self driving cars
- Around 2020, the complete Automobile industry will start to be disrupted.
- You don't want to own a car anymore.
- Next generation will never get a driving license and will never own a car.

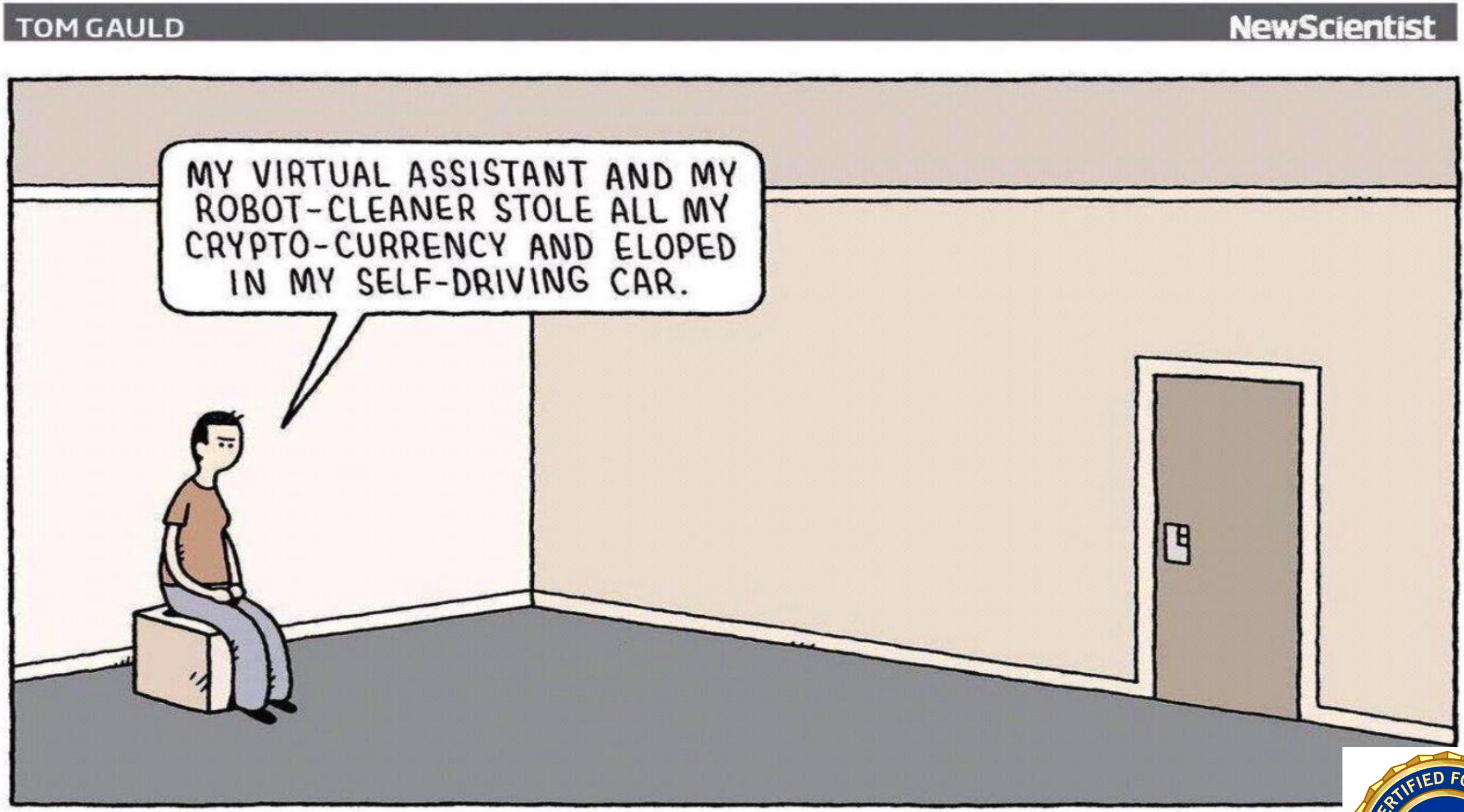
Autonomous cars:

- In 2018 the first self driving cars
- Around 2020, the complete Automobile industry will start to be disrupted.
- You don't want to own a car anymore.
- Just a phone call
- Next generation will never get a drivering license and will never own a car.

Zero Accident, no car parking…

- No need for huge Car Parking
- we can save a million lives each year.
- Insurance companies
- Real estate will change.
- Medical tourism

Recent cybercrime trends…


TOM GAULD
NewScientist
MY VIRTUAL ASSISTANT AND MY ROBOT-CLEANER STOLE ALL MY CRYPTO-CURRENCY AND ELOPED IN MY SELF-DRIVING CAR.

1: Crime-as-a-Service

The Electronic underground is underpinned by a growing Crime-as-a-Service model that interconnects specialist providers of cybercrime tools and services with an increasing number of organised crime groups. Terrorist actors clearly have the potential to access this sector in the future.

- Reset temperature settings on refrigerators storing blood & drugs and cause spoilage.
- Altering Electronic medical records.
- Restart / reboot critical equipment.
- Spoofed blood test reports.

CERTIFIED FORENSIC COMPUTER EXAMINER IACIS

2.Ransomware

Ransomware

- A type of malware which restricts access to the computer system, and demands a ransom paid to the creator(s) of the malware

- Some forms of ransomware encrypt files on the system's hard drive (cryptoviral extortion), while some may simply lock the system and display messages

Wannacry author

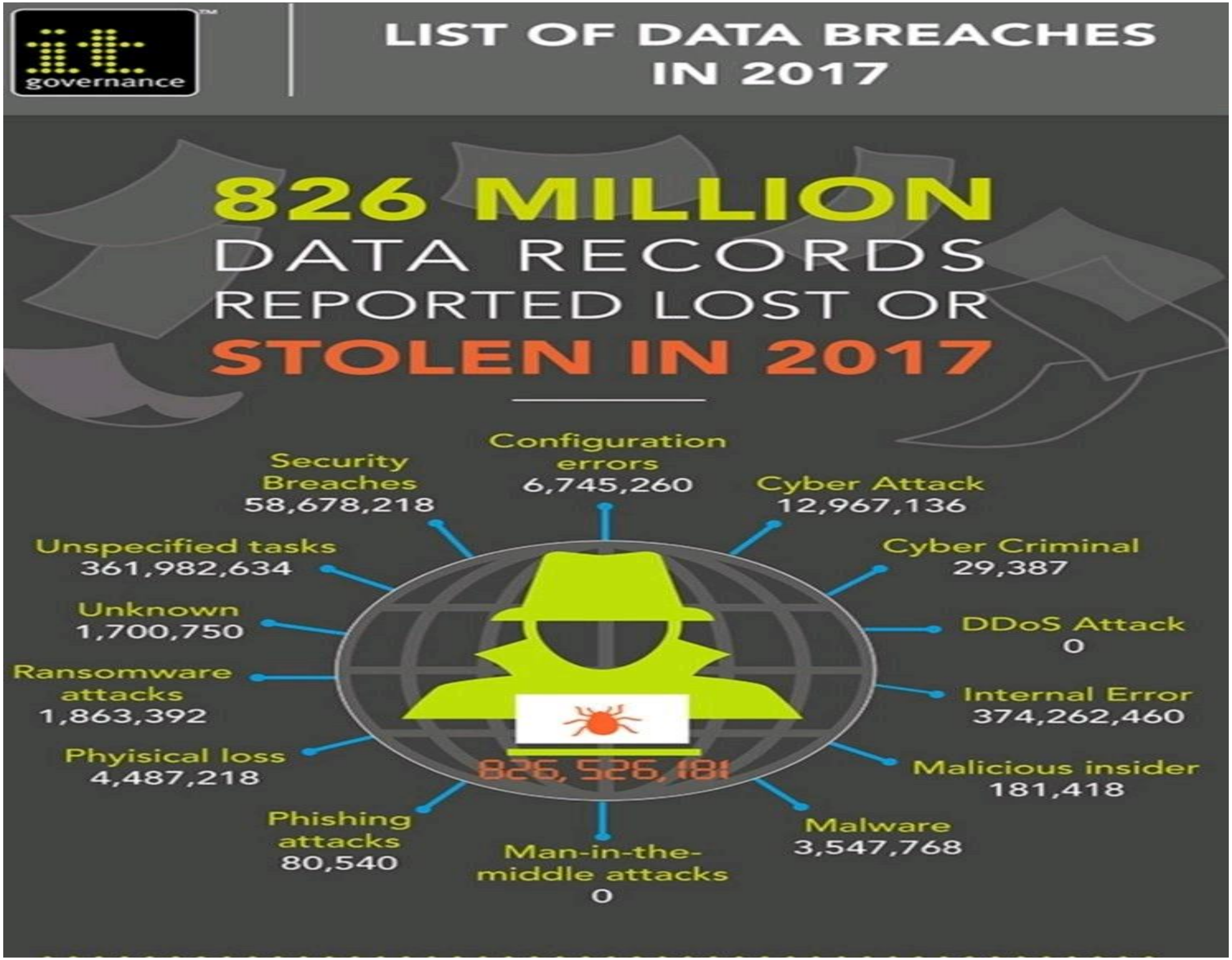
- Hacker Konstantin Kozlovsky from Lurk Hacker group admits that he is one of the Author of WannaCry ransomware and the work was commissioned by intelligence agencies
- WannaCry (WannaCrypt, WanaCrypt0r 2.0, Wanna Decryptor) Attack Started on 12 May 2017 and Infected more than 3,00,000 computers in over 150 countries which consider as one of the Biggest Ransomware cyber Attack which world Never Faced
- .He was arrested in Yekaterinburg a city in Russia, in charge of a scam in part of Lurk Hacker group.
- According to Kozlovsky, the ransomware was created by Lurk Hacker group.

3.The criminal use of data

Aadhar Data leaking

Apple , Facebook, Samsung

Biometric   data   Finger print eye scan



LIST OF DATA BREACHES IN 2017

826 MILLION DATA RECORDS REPORTED LOST OR **STOLEN IN 2017**

Configuration errors	6,745,260
Cyber Attack	12,967,136
Cyber Criminal	29,387
DDoS Attack	0
Internal Error	374,262,460
Malicious insider	181,418
Malware	3,547,768
Man-in-the-middle attacks	0
Phishing attacks	80,540
Phyisical loss	4,487,218
Ransomware attacks	1,863,392
Unknown	1,700,750
Unspecified tasks	361,982,634
Security Breaches	58,678,218

826, 526,181

4: Online Payment Frauds

All type of on line /off line frauds

ATM frauds

Plastic card frauds

Over 25,800 fraud cases involving about ₹ 179 crore related to credit/debit cards and Internet Banking were reported in 2017

CYBER ATTACK ON CBS

- 1.Bangaladesh Central Bank 2016
- $ 81 Million
- 2.PNB Feb 2018
- Rs 280.7 crores
- 3. CUB TAMILNADU Feb 2018

CERTIFIED FORENSIC COMPUTER EXAMINER IACIS

COSMOS BANK ATTACK

- 1. Rs 94 cr on August 11th 2018.
- 2. malware attack on server by Canadian hacker
- Malicious SW will be sent through a link to the target with executable code
- ATM – CBS- VISA- Issue Bank- return
- 14,800 transactions, from 28 countries
- Violations of RBI instructions.

CERTIFIED FORENSIC COMPUTER EXAMINER IACIS

STATE BANK OF MAURITIUS

- Attack on 2-10-2018
- Rs. 143 crore
- Malware issue
- This case will likely to be transferred BF&SC branch of CBI Mumbai.

CROSS BORDER MOVEMENTS OF FUNDS

SWIFT

- SOCIETY FOR WORLDWIDE INTER BANK FINACIAL TELE COMMUNICATIONS.(SWIFT)
- 10,000 FIs
- 212 Different countries
- To send and receive information about financial transactions to each other
- TELEX was used earlier.
- IBAN Inter Bank Ac number
- BIC Bank Identifier Code
- GPI Global Payment Innovations
- RBI Instructions connect CBS with SWIFT

5: Online child sexual abuse

P**ornography**

Child pornography

Surface Web - ClearNet

Bing
Facebook
Yahoo
Wikipedia
Google
YouTube

Deep Web

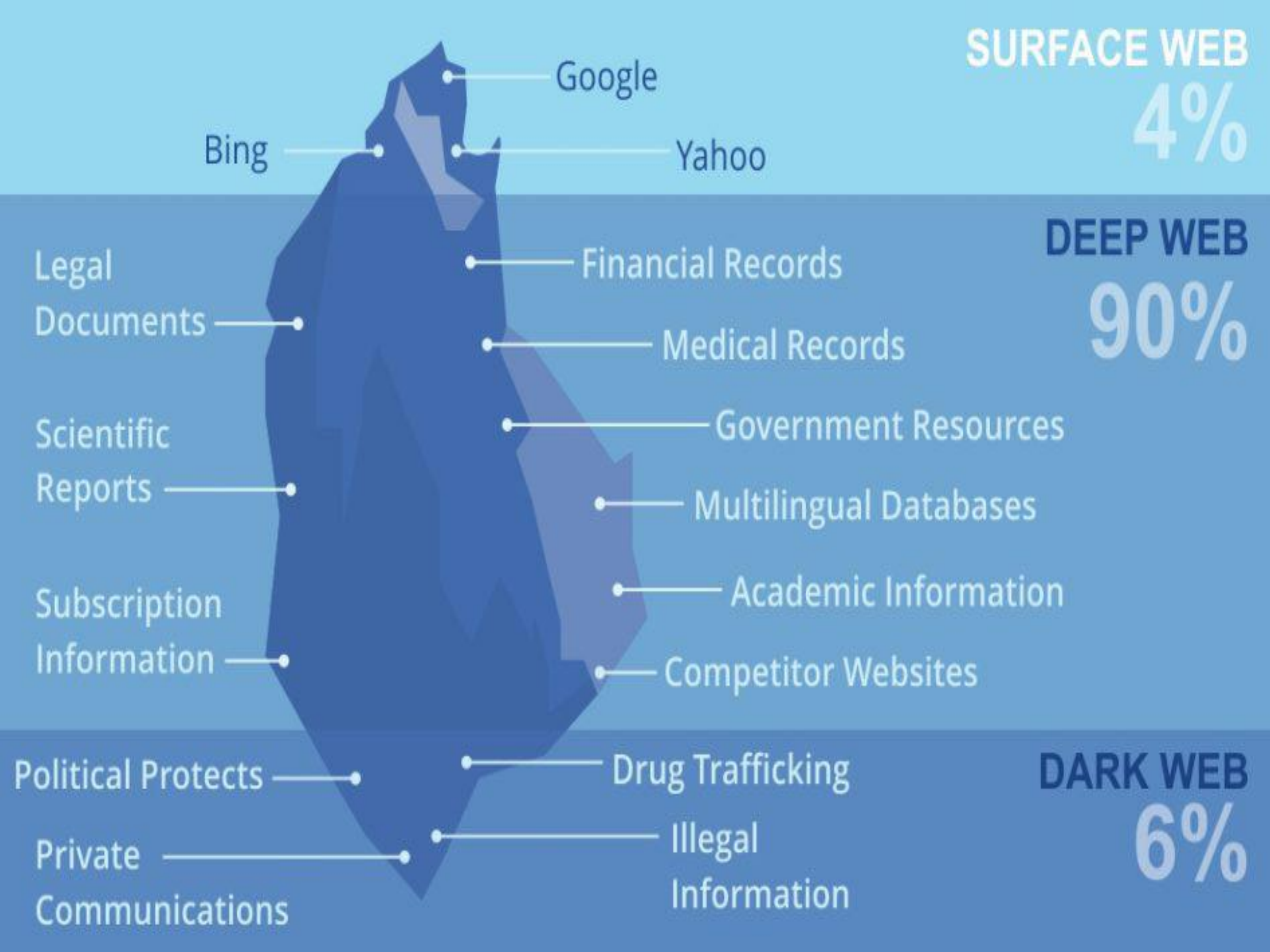
Represents anywhere from 90-96% of all content available on the internet

- Legal Documents
- Medical Records
- Science Journals
- Academic Information
- Subscriptions
- Government Resources
- Financial Records
- Organizational Repositories

DarkNet

Only 30,000 to 50,000 websites thought to exist

- Hitmen
- Classified Communication
- Leaked Material
- Drug Sales
- Passport Forging
- Encrypted.onion sites



SURFACE WEB
4%

Google

Bing

Yahoo

DEEP WEB
90%

Legal Documents

Financial Records

Medical Records

Scientific Reports

Government Resources

Multilingual Databases

Subscription Information

Academic Information

Competitor Websites

DARK WEB
6%

Political Protects

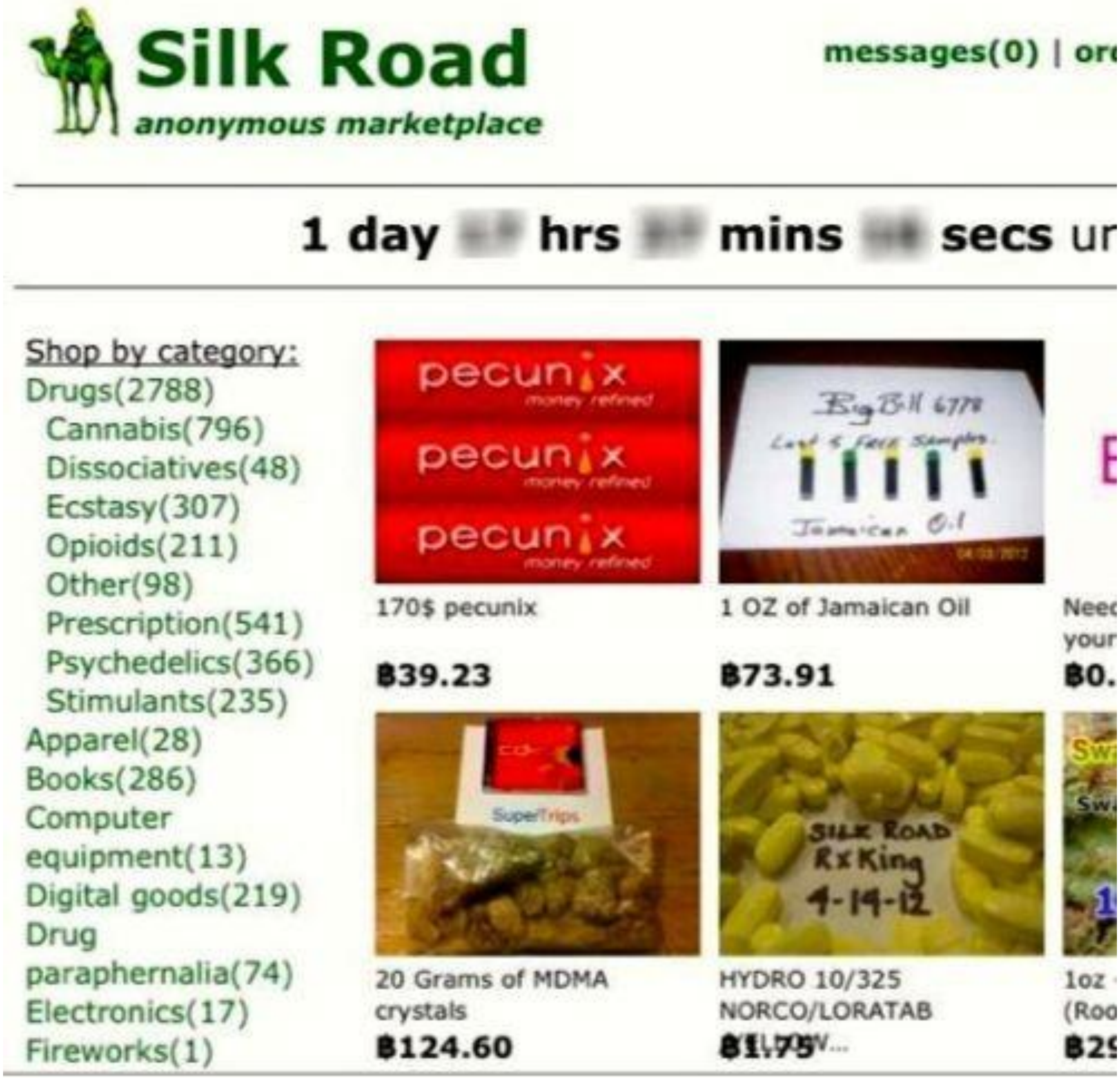
Drug Trafficking

Private Communications

Illegal Information

6.Deep web challenges

- 1.Accessing the Dark Web
- Accessing the dark web is to download "TOR" The Onion Router Browser Bundle" from TorProject.org.
- 2.Anonymously and illegal
- 3.invisible web
- 4.Silk Road1.0 (Oct 2013)
- Silk Road2.0 (Nov 2014)
- Silk Road3.0 (May 2017)
- 5. Untraceable crypto currencies



Silk Road

anonymous marketplace

messages(0) | or

1 day [redacted] hrs [redacted] mins [redacted] secs ur

Shop by category:

Drugs(2788)
- Cannabis(796)
- Dissociatives(48)
- Ecstasy(307)
- Opioids(211)
- Other(98)
- Prescription(541)
- Psychedelics(366)
- Stimulants(235)

Apparel(28)
Books(286)
Computer equipment(13)
Digital goods(219)
Drug paraphernalia(74)
Electronics(17)
Fireworks(1)

170$ pecunix
฿39.23

1 OZ of Jamaican Oil
฿73.91

Need your
฿0.

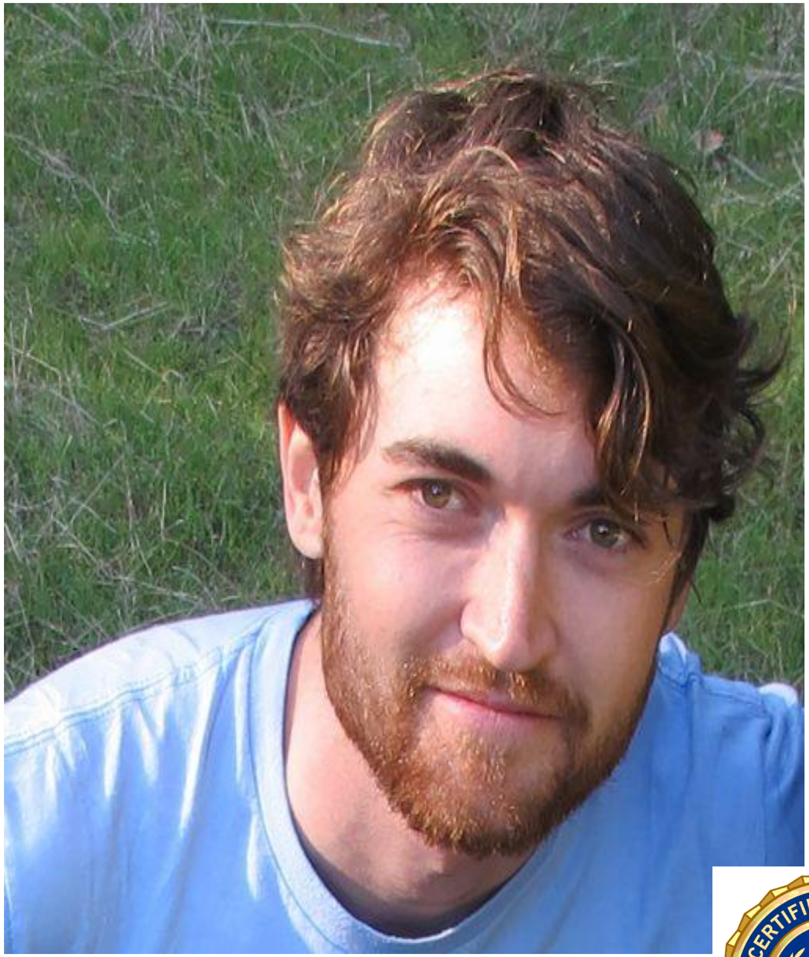
20 Grams of MDMA crystals
฿124.60

HYDRO 10/325 NORCO/LORATAB YELLOW...
฿1.75

1oz (Roo
฿29

DPR

Ross William Ulbricht is a convicted American drug trafficker and darknet market operator, best known for creating and running the Silk Road website from 2011 until his arrest in 2013. He was known under the pseudonym "Dread Pirate Roberts



Fentanyl

- Fentanyl is an opioid used as a pain medication and together with other medications for anesthesia. Fentanyl is also made illegally and used as a recreational drug, often mixed with heroin or cocaine
- 351 people overdosed fatally on opiates last year in New Hampshire

Darkmarket

Online Carding Forum

Darkmarket facilitated the buying and selling of stolen financial information

Set up in 2008 by Renukanth Subramaniam in London in 2008

Had 2500 members

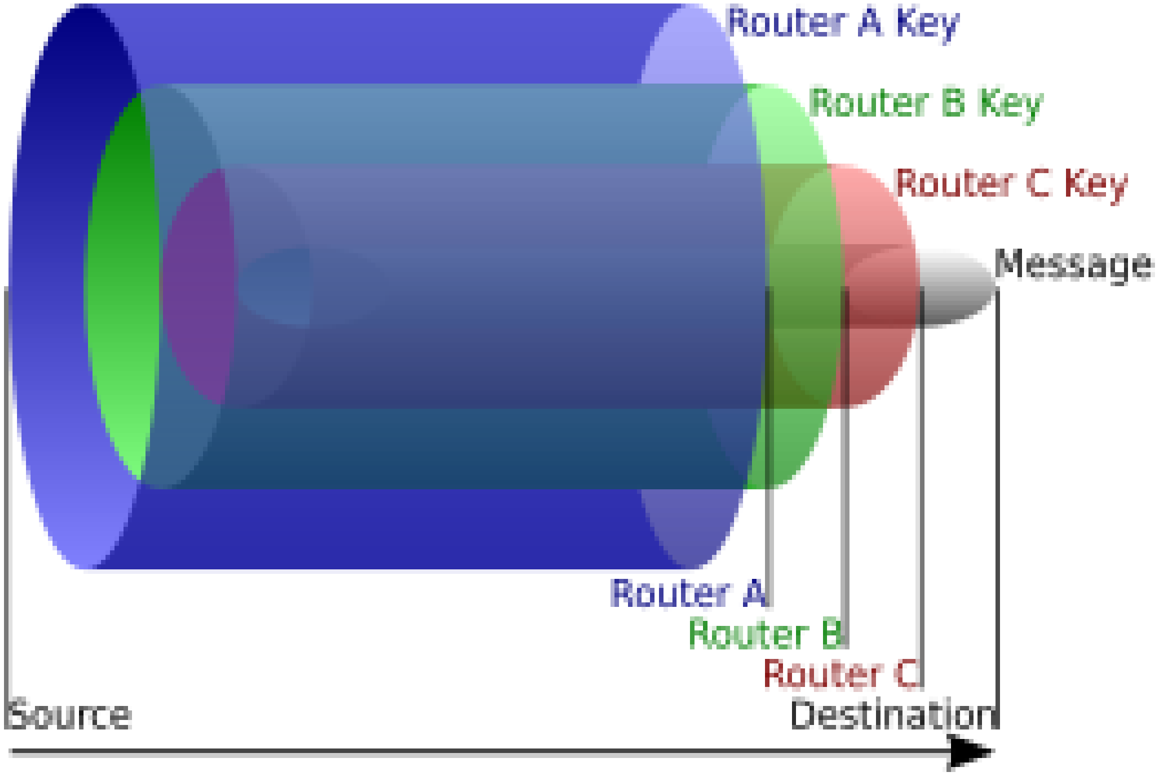
- stolen credit card data,
- login credentials, and
- equipment for carrying out financial crimes.

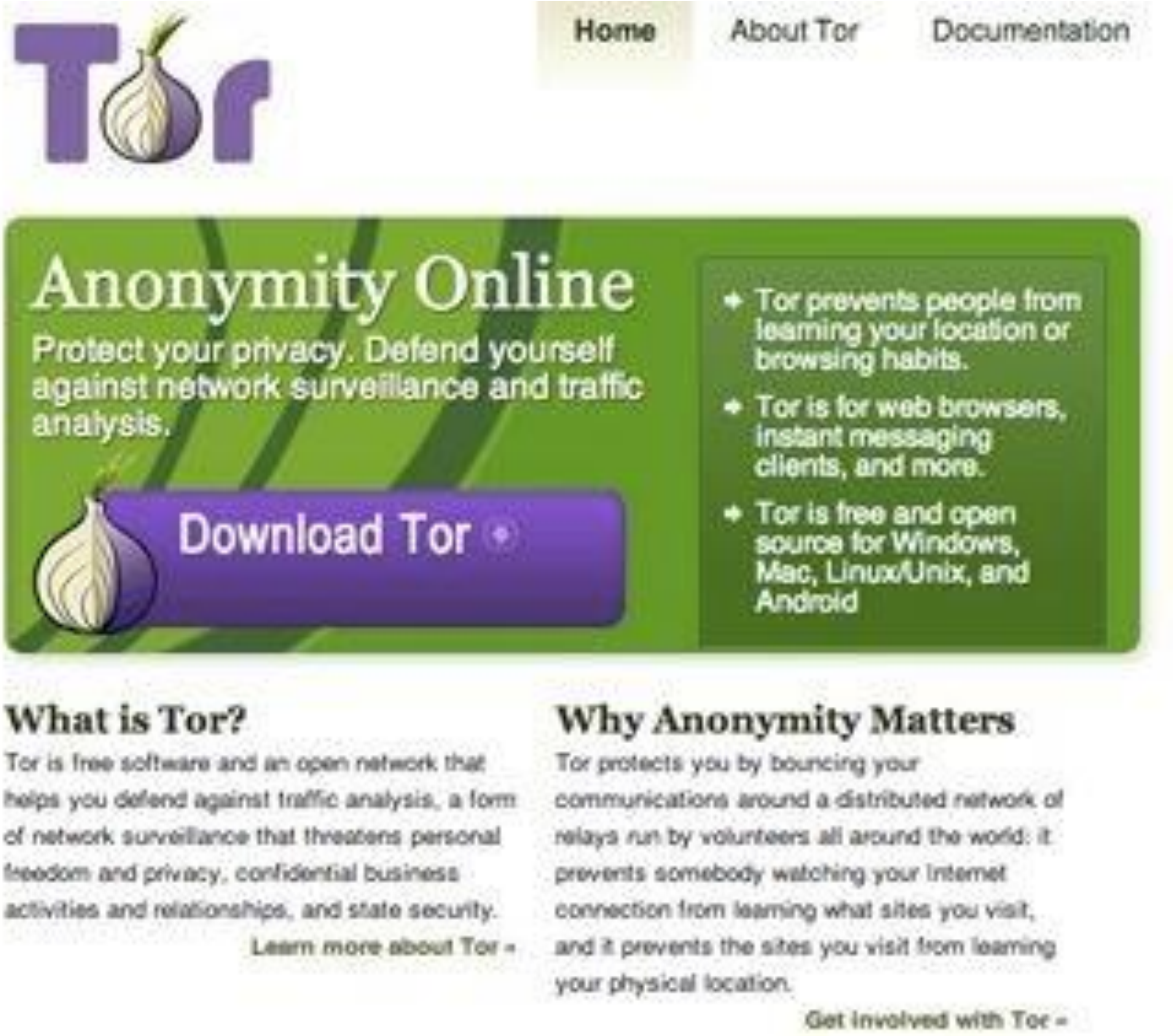
Taken down in 2010

El Chapo

Joaquín Archivaldo Guzmán Mexican Drug Lord who headed the SINALOA Cartel a criminal organization He is also Known as **"El Chapo“** considered the "most powerful drug trafficker in the world”

TOR


Router A Key
Router B Key
Router C Key
Message
Router A
Router B
Router C
Source
Destination



Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

What is Tor?

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Learn more about Tor »

Why Anonymity Matters

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Get involved with Tor »

Block chain

- **The blockchain is an undeniably ingenious invention – the brainchild of a person or group of people known by the [Satoshi Nakamoto]().**
- **The blockchain is an incorruptible Electronic ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value**

Blockchain Application

- Electronic Identities
- Health
- Distributed cloud Storage
- Electronic Voting

  Passports
- E-Residency
- Birth /death Certificates
- Wedding Certificates
- Land Records
- Online Account Login

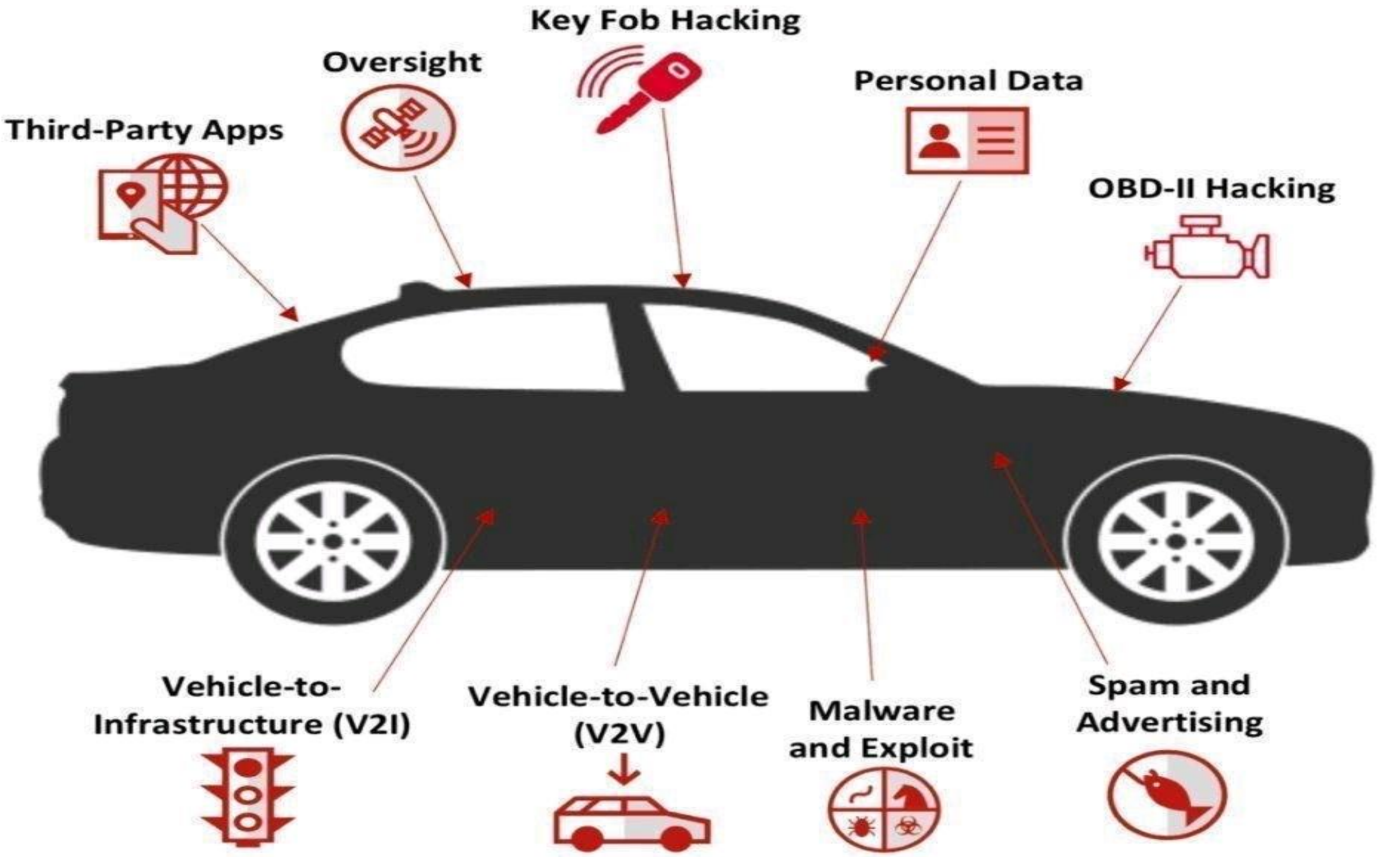
7: Social engineering

An increase of phishing aimed at high value targets has been registered by enforcement private sector authorities.

8: Virtual currencies

Bitcoin remains the currency of choice for the payment for criminal products and services in the Electronic underground economy and the Darknet. Bitcoin has also become the standard payment solution for extortion payments

Major Modern Cars Security Risk



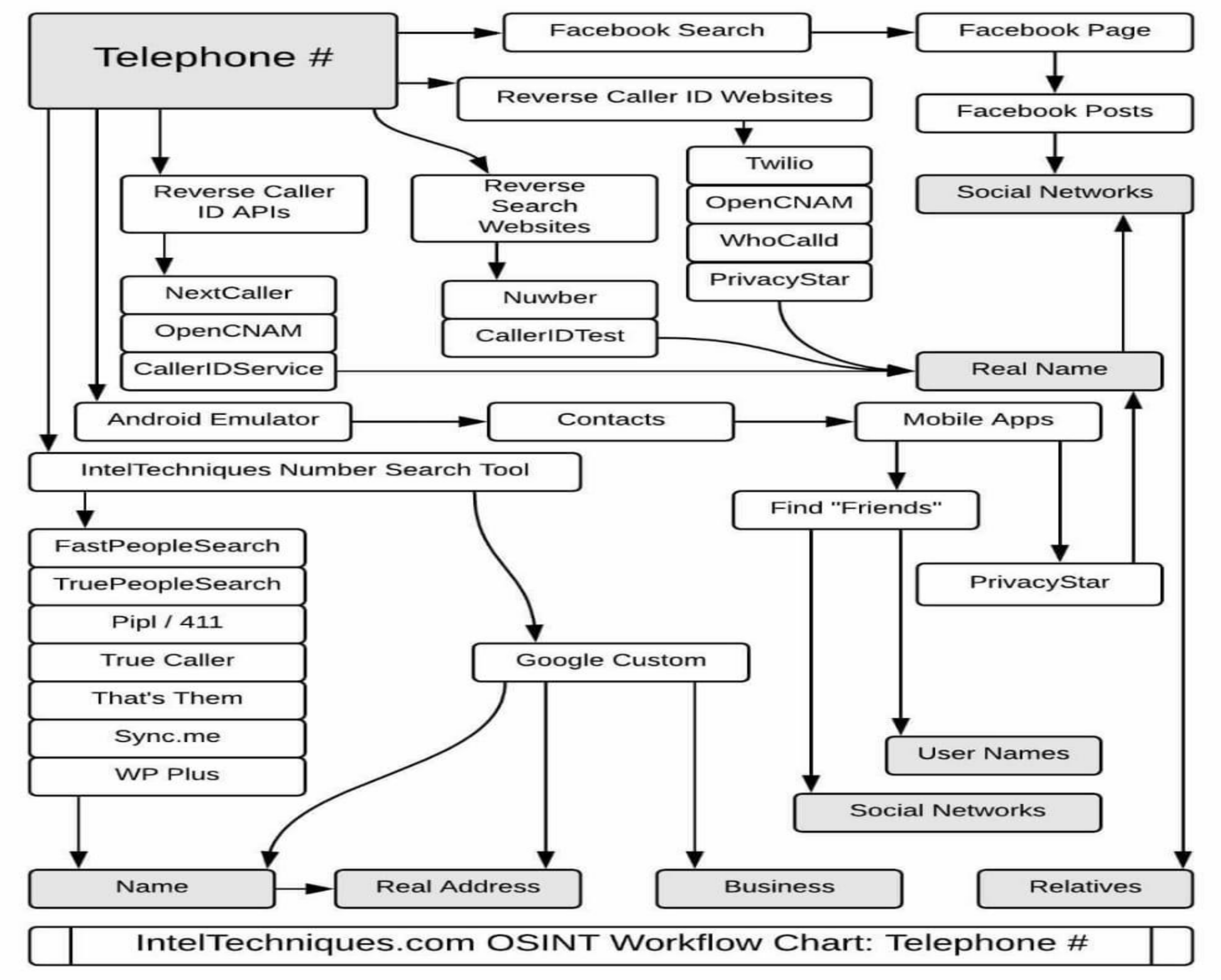
Major modern cars Security Risk…

- Stealing personally identifiable information(PII):
- Connection security: .
- Manipulating a vehicle’s operation:
- Unauthorized vehicle entry: .
- Mobile application security:

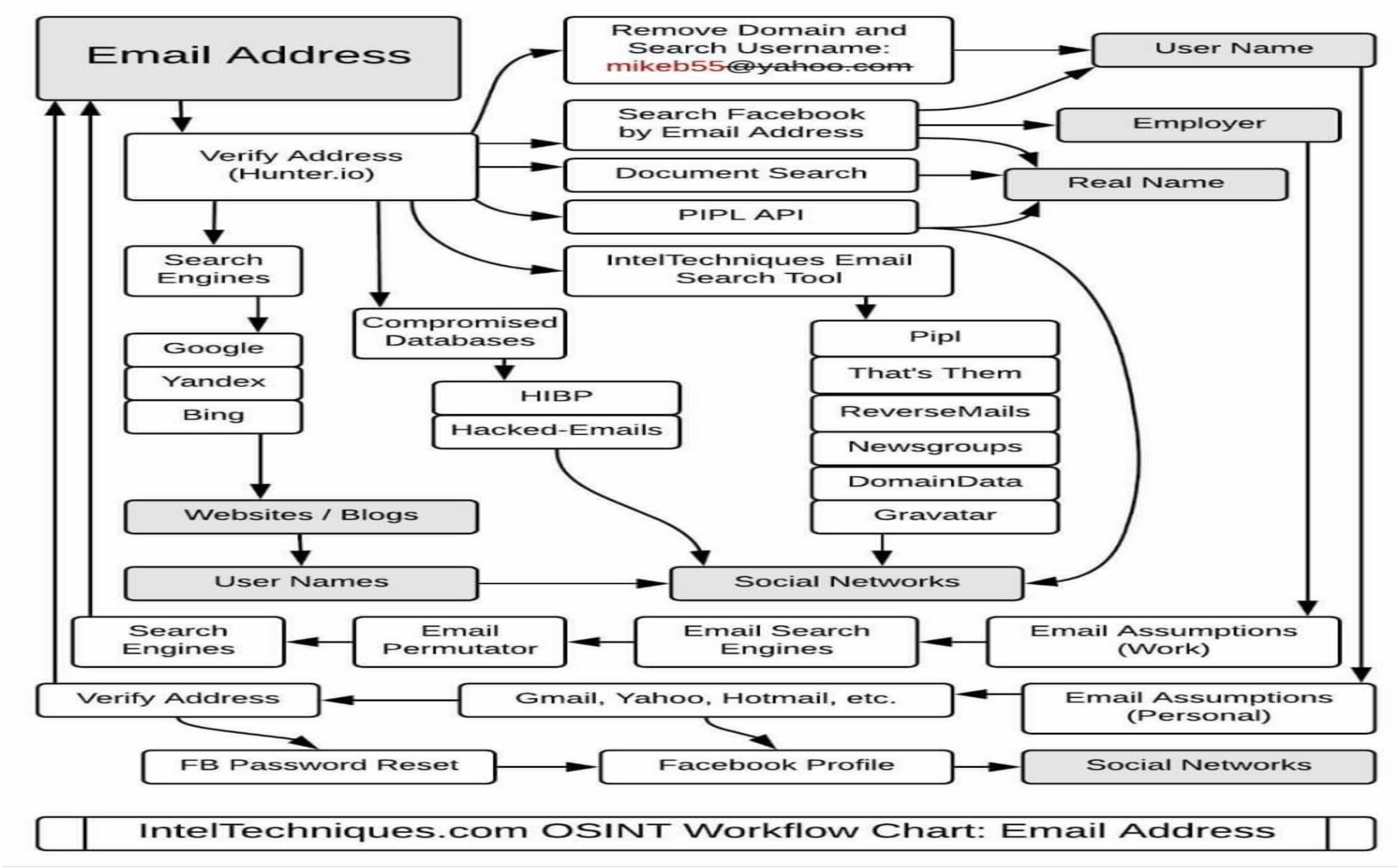
OSINT

- Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources).

From your Telephone



From your e mail id…



Email Address

Verify Address (Hunter.io)

Remove Domain and Search Username: mikeb55~~@yahoo.com~~

Search Facebook by Email Address

Document Search

PIPL API

IntelTechniques Email Search Tool

User Name

Employer

Real Name

Search Engines

Google

Yandex

Bing

Compromised Databases

HIBP

Hacked-Emails

Pipl

That's Them

ReverseMails

Newsgroups

DomainData

Gravatar

Websites / Blogs

User Names

Social Networks

Search Engines

Email Permutator

Email Search Engines

Email Assumptions (Work)

Verify Address

Gmail, Yahoo, Hotmail, etc.

Email Assumptions (Personal)

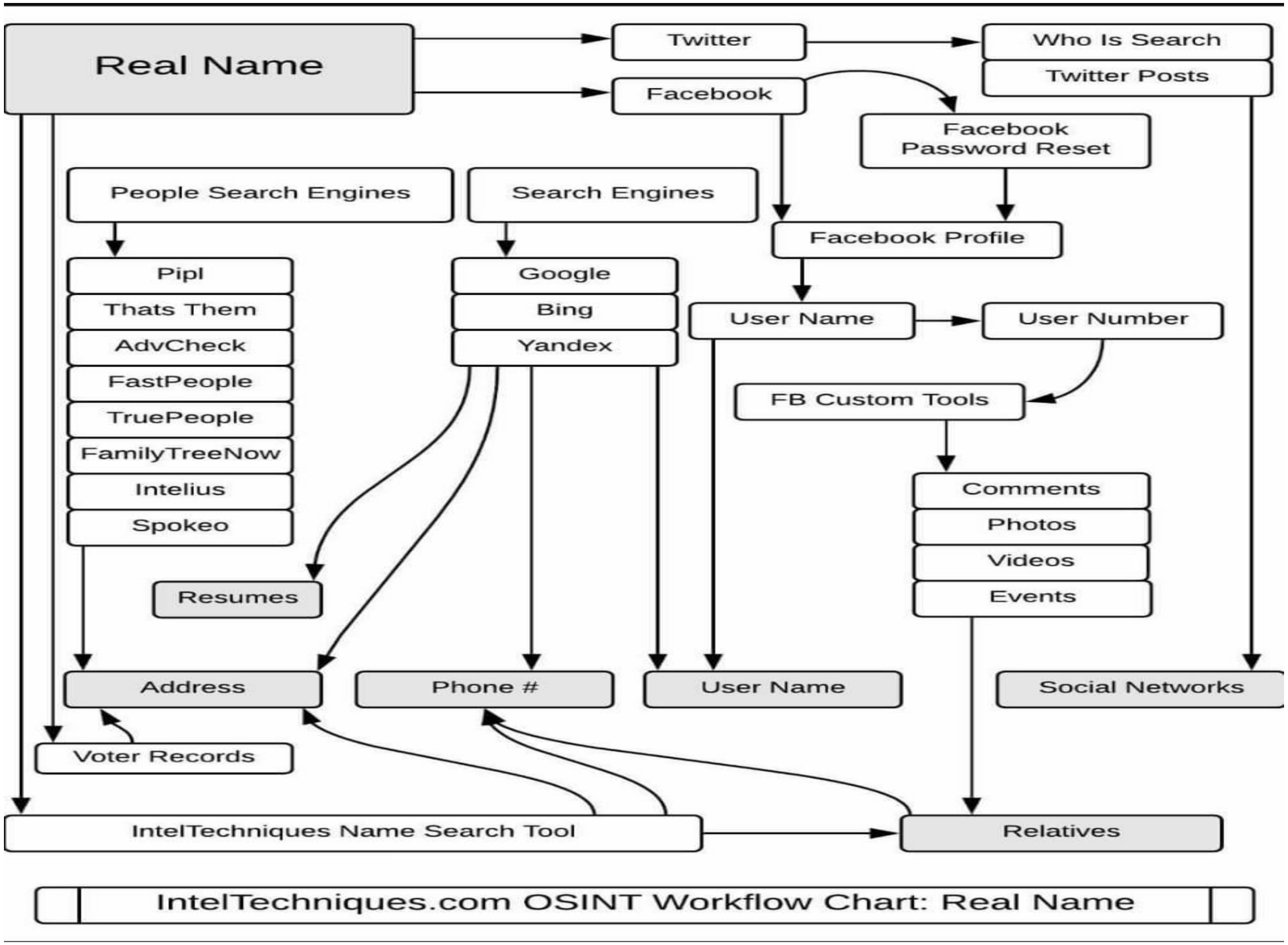
FB Password Reset

Facebook Profile

Social Networks

IntelTechniques.com OSINT Workflow Chart: Email Address

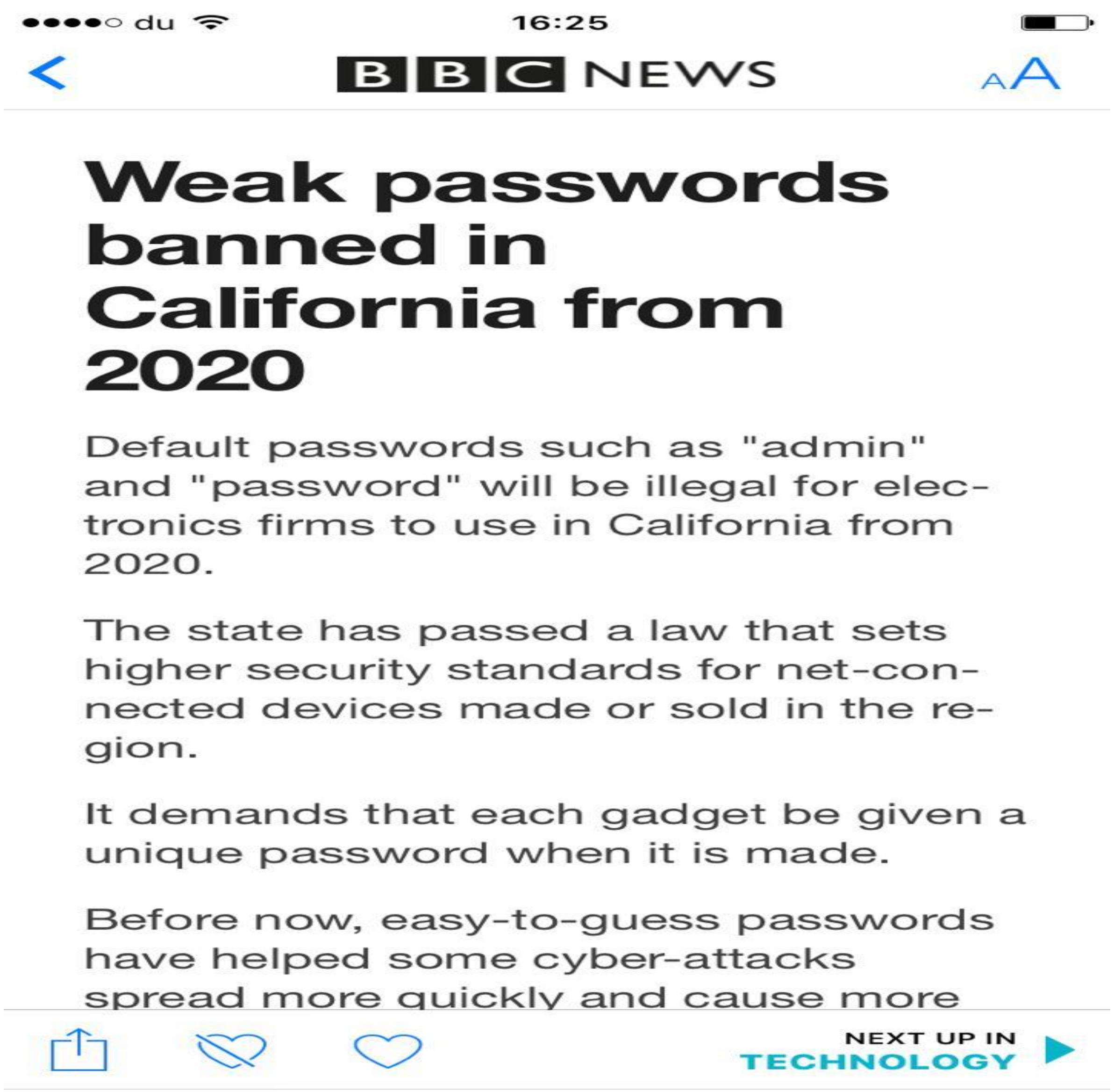
From your real Name



eSim

Simpler device setup without the need to insert or replace a SIM card;

- devices that can operate independently of a smart phone, with their own subscriptions;
- a range of new, enhanced mobile-connected devices.



Weak passwords banned in California from 2020

Default passwords such as "admin" and "password" will be illegal for electronics firms to use in California from 2020.

The state has passed a law that sets higher security standards for net-connected devices made or sold in the region.

It demands that each gadget be given a unique password when it is made.

Before now, easy-to-guess passwords have helped some cyber-attacks spread more quickly and cause more

All your peripheral Devices

- Check all your peripheral Electronic Devices to be updated
- Copier
- Scanner
- Printers etc!
- Pen drive and other storage devices

Juice Jacking

Do you often charge your mobile device from public ports while travelling? Did you know this can lead to "**Juice Jacking**" ?

Beware of Juice Jacking

Attackers use USB charging ports available at public places to install malware, steal data or even take complete control of your device.

Tips to stay safe

- Disable data transfer feature on your mobile phone while charging
- Get a charge only cable instead of cable supporting charging and data transfer capabilities
- Try to carry a power bank
- If possible, switch off the device while charging from public ports

CERTIFIED FORENSIC COMPUTER EXAMINER IACIS

Indian Cyber Laws

Indian Cyber Laws were official born on 17th October 2000 with the Information Technology Act, 2000 coming into force.

- The Indian Penal Code (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.
- Electronic Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT Act).
- In case of bank records, the provisions of the Bankers' Book Evidence Act (as amended by the IT Act) are relevant.
- Investigation and adjudication of cyber crimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act.

Search and seizure

- Crpc Provisions
- Sec 93
- Sec 165
- IT Act 2000: sec .80
- Independent witnesses, video, photo

IT ACT 2000

- **Sec.80. Power of police officer and other officers to enter, search, etc.-(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Inspector of Police, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act.**

Provisions for the Proof of Electronic Evidence

- 65A. Special provisions as to evidence relating to electronic record
- 65B. Admissibility of electronic records
- 67A. Proof as to Electronic signature
- 73A. Proof as to verification of Electronic signature
- 81A. Presumption as to Gazettes in electronic forms
- 85A. Presumption as to electronic agreements
- 85B. Presumption as to electronic records and Electronic signatures 85C. Presumption as to Electronic Signature Certificates
- 85C. Presumption as to Electronic Signature Certificates
- 88A. Presumption as to electronic messages
- 90A. Presumption as to electronic records five years old
- 131. Production of documents or electronic records which another person, having possession, could refuse to produce

Admissibility: Before Court

- **Evidence collection**
  - **Correct legal processes**
  - **Accepted techniques and tools**
  - **Properly trained personnel**
- Chain of custody
- Testimony of Experts
- Corroboration

Admissibility of Electronic Evidence

- 65A and 65B are introduced to the Evidence Act under the Second Schedule to the IT Act.
- Section 5 of the Evidence Act provides that evidence can be given regarding only facts that are at issue or of relevance.
- Section 136 empowers a judge to decide on the admissibility of the evidence. Section 65A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B.
- Section 65B provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic record (ie, the contents of a document or communication printed on paper that has been stored, recorded and copied in optical or magnetic media produced by a computer ('computer output')), is deemed to be a document and is admissible in evidence without further proof of the original's production, provided that the conditions set out in Section 65B(2) to (5) are satisfied.

Electronic Evidence : Admissibility in court of law

- Section 65A and Section 65B of the Indian Evidence Act, 1872
- Introduced in the year 2000
- Aim was to lay down admissibility standard for electronic evidence in court of law.
- Fragile nature of electronic records leads to conflict between relevancy and admissibility of electronic evidence.
- Due to inconsistent and arbitrary pronouncements led to lack of uniformity w.r.t. methods for fulfilment of the conditions laid down in Sec 65A and Sec 65B.
- Supreme Court in Anvar P V Vs P K Basheer (2014) 10 SCC 473 put to rest all these controversies.

IEA 1872 : Section 65A , 65 B(1)

- Sec 65A states content of electronic record may be proved with due provisions of Sec 65B.
- Sec 65B complies with the Admissibility of Electronic Records.
- Sub Section (1) provides
  - any information contained in electronic records that is transferred on to any media admissible in court as evidence of electronic record.
  - Means parties are not obligated to produce primary evidence.
  - Sec 65B(1) is subject to condition under Sec 65B(2).

IEA 1872 : Section 65B (2)

- **Conditions U/s 65B(2) seeks to ensure that output was generated and the computer was used lawfully in the ordinary course of business. Specifically –**
  - **a) output from computer must be in period when it is being regularly used to store / process information.**
  - **b) by a person having lawful control over it.**
  - **c) information must be regularly fed into system in ordinary course of activities.**
  - **d) computer should haven been operating properly, if not then accuracy of information should have not been affected.**
  - **e) Information in electronic record must be copy of information fed in computer in ordinary course.**
- **The above five conditions are to be mandatorily compliec with**

IEA 1872 : Section 65B (3) (4) &(5)

- Section 65B (3) & (5) are related to nature of the computer and methods of supplying /producing information.
- Section 65B (4)
- Section 65B(4) gives Certificate in relation to electronic record. It provides
  - Who can issue
  - What will be the contents of certificate
  - The certificate must
    - Identify the electronic record containing the statement and describing the manner in which it was produced.
    - Giving the particulars of device
    - Dealing with any of the matters to which the conditions in sub section (2) relate
  - Must be signed by a person occupying a responsible official position in relation to operation of relevant devices or management of the relevant activities.
  - Must be to the best of the knowledge and belief of the signatory

IEA 1872 : Section 65B (4)

- Section 65B(4) gives Certificate in relation to electronic record. It provides
  - Who can issue
  - What will be the contents of certificate
  - The certificate must
    - Identify the electronic record containing the statement and describing the manner in which it was produced.
    - Giving the particulars of device
    - Dealing with any of the matters to which the conditions in sub section (2) relate
  - Must be signed by a person occupying a responsible official position in relation to operation of relevant devices or management of the relevant activities.
  - Must be to the best of the knowledge and belief of the signatory

CASE LAWS

1. In Amitabh Bagchi vs. Ena Bagchi
   (AIR 2005 Cal 11)
2. State of Maharashtra vs. Dr. Praful B Desai
   (AIR 2003 SC 2053)
3. Bodala Murali Krishna vs. Smt.Bodala Prathima
   (2007 (2) ALD 72)
4. Dharambir vs. Central Bureau of Investigation
   (148 (2008) DLT 289)
5. In Jagjit Singh vs. State of Haryana
   ((2006) 11 SCC 1)

Case Laws…

6. Twentieth Century Fox Film Corporation **vs.** NRI Film Production Associates (P) Ltd. (AIR 2003 KANT 148)
7. Anvar P.V. **vs** P.K. Basheer and others …
8. Sonu@Anvar Case **vs.** State of Haryana
9. Shreya Singhal **vs.** Union of India
10. CALL RECORDS : Rakesh Kumar and Ors. **Vs.** State, the High Court of Delhi
11. ELECTRONIC RECORDS : K.K. Velusamy **vs.** N. Palanisamy, 2011 EQ–SC–0–158 SCI

Judicial Judgments

2003	2005	2014
State Vs Mohd. Afzal	**State Vs Navjot Sandhu**	**Anvar P K Vs P V Basheer**
▪ First time test for admissibility under Sec 65B was considered. ▪ Defense's plea that call records were inadmissible as precondition of sec 65B(4) not satisfied. ▪ Prosecution's submission was conditions of Sec 65B(2) were met by oral testimony. ▪ High Court upheld prosecution's case	▪ SC affirmed Delhi HC decision. ▪ Held sufficient oral testimony of PWs. ▪ Also held even if requirement of sec 65B(4) not satisfied, evidence could be produced under sec 63 & sec 65 of Indian Evidence Act,1872. ▪ Decision relaxed standards for electronic evidence	▪ Basheer (Respondent) an elected legislator challenged the admissibility of CDs containing election propaganda. ▪ Certificate of sec 65B(4) not there. ▪ Kerala HC concurred with the respondent's argument. **SC in appeal by petitioner :-** – Excluded the applicability of all provisions of IEA except sec 65B. – Disagreed / overruled the SC's decision in **Afzal Guru** case. – Sec 61 to Sec 65 deals with general documentary evidence . Sec 65B refers only to electronic records. – Electronic records can solely be adduced under sec 65B. **Conclusion in case** a) conditions under sec 65B(2) are mandatory. b) certificate under sec 65B(4)

Judicial Judgments

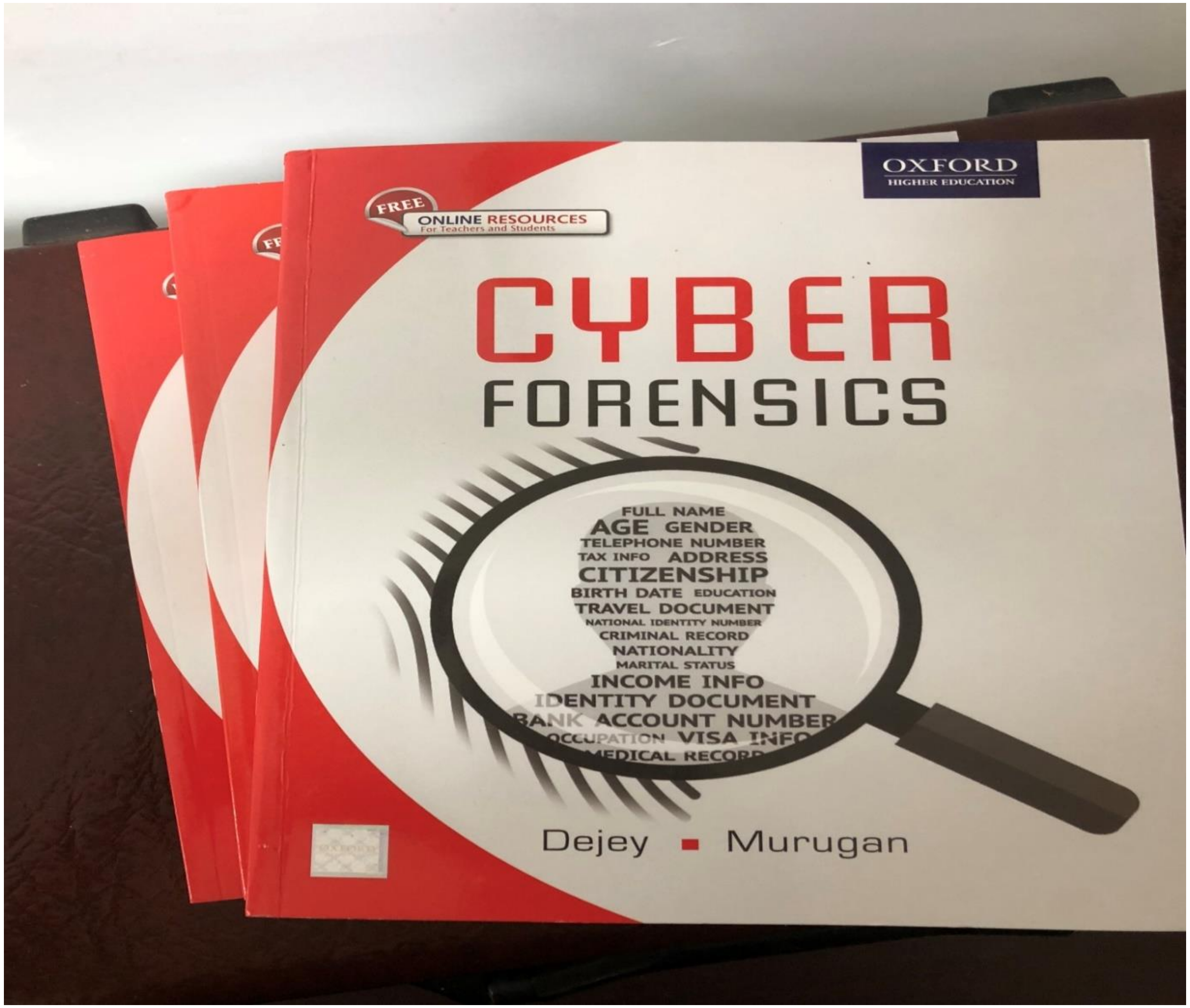
2017	2018, Hon’ble Supreme Court
Sonu Vs State of Haryana	**Mohd. Shafii**
▪ Followed Basheer judgement. ▪ Subsequent to Afzal Guru case till Basheer case many cases decided based on the ratio of the previous case. ▪ Held giving retrospective effect to Basheer judgement would be impracticable and create chaos and affects the administration of justice. ▪ It is a curable defect ▪ Objection by defense must be at the stage of admission of evidence. ▪ Challenge on ground that certificate under section 65B(4) not adduced is not at appeal stage maintainable.	▪ Deliberated upon significance of video-graphy as crucial means of evidence in connection with the requirements under sec 65B(4) of IEA. ▪ An exception to sec 65B(4) has been carved by SC. It held a) Electronic evidence produced by a party who is not in possession of a device applicability sec 63 and sec 65 of IEA can not be excluded. b) A party not in possession of a device from which the document is produced can not be required to be produced in certificate. ▪ It will lead to denial of justice.

12
Question
Time

About me…

- Dr. S. Murugan, IPS, a senior police officer, presently working as Inspector General of Police in Tamil Nadu police
- Rich experience in handling Cybercrime investigations and supervised high profile sensational cybercrime cases for the last 18 years.
- Worked in CBI for 5 years! Visited abroad for trg &investigations.
- My academic qualifications ranges from Masters in Economics, Management and Computer Applications to a doctorate in Cybercrime which focused on Frauds in Plastic Money from the University of Madras
- CFCE (Certified Forensics Computer Examiner) from IACIS (International Association of Computer Investigative Specialist), USA.
- A member of IACIS.
- Regular Guest faculty for Tamil Nadu Police Academy, Tamil Nadu Judicial Academy, CBI Academy New Delhi National Judicial Academy Bhopal and Gujarat forensics Sciences University Gandhi nagar etc

My book published by OXFORD



Contact me @….

- 919444049224

murugans@protonmail.com

CERTIFIED FORENSIC COMPUTER EXAMINER

IACIS

Thank you