Digital Evidence & Cyber Forensics

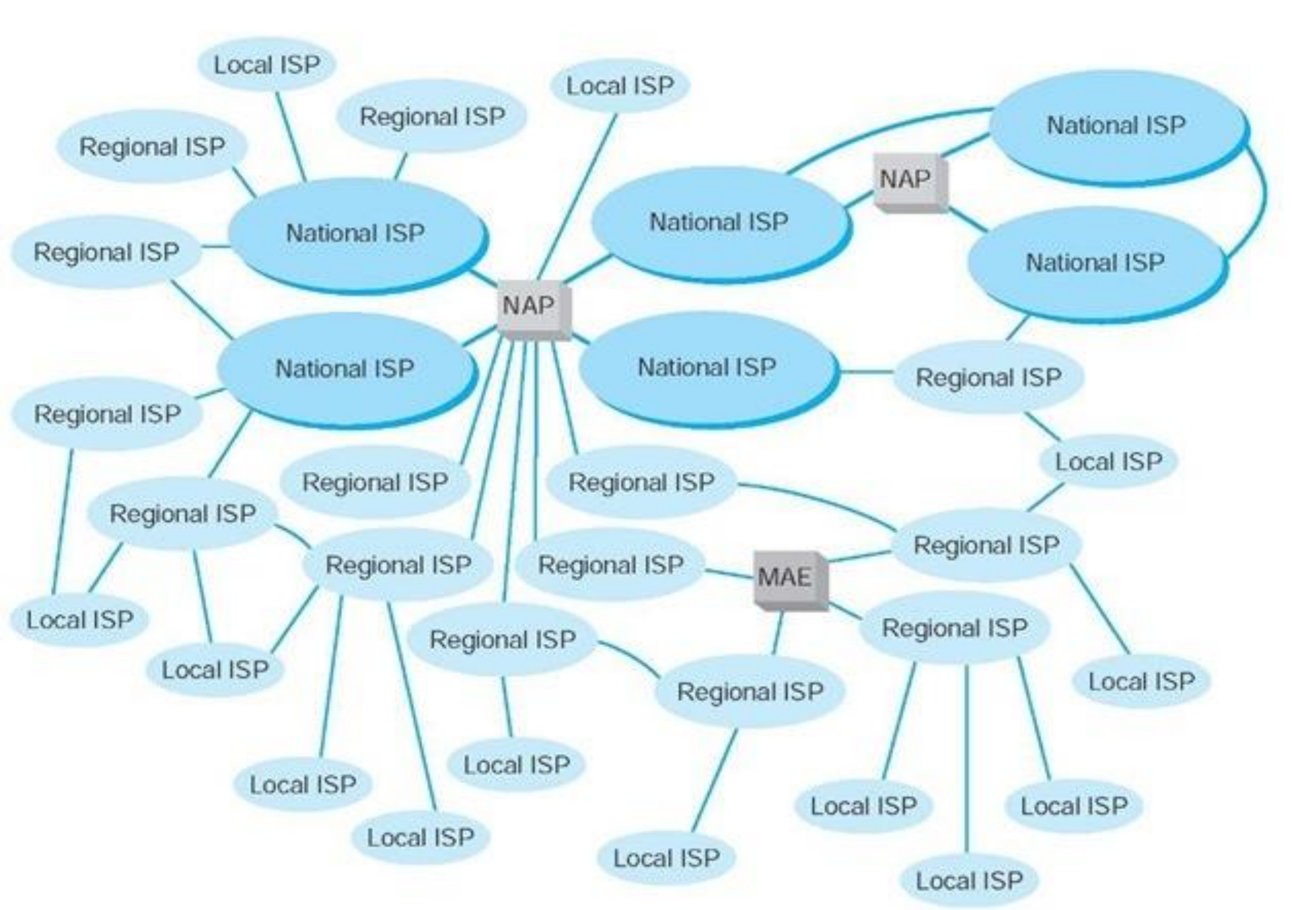
Dr. Harold D’costa
CEO – Intelligent Quotient Security System & President – Cyber Security Corporation
Advisor (Law Enforcement Agencies), Sr.Trainer (Judges and Public Prosecutors)
Mobile : +91-9637612097
Email : hld@rediffmail.com
Website: www.cybersolution.in

Cyber Security Corporation
Office Address: Office no 5, 3rd Floor, Anandi Gopal Bldg., Fergusson College Road, Pune 411005

Internet

- The internet is world wide, publicly accessible network of interconnected computer networks that transmit data by packet switching using the standard Internet Protocol (IP).
- The Internet's architecture is described in its name, a short from of the compound word "inter-networking". This architecture is based in the very specification of the standard TCP/IP protocol, designed to connect any two networks which may be very different in internal hardware, software, and technical design.

Internet MAP



WHO OWNS INTERNET ?

- No one actually owns the Internet, and no single person or organization or government controls the Internet in its entirely. Nobody can turn it off, its evolution depend on technical purpose and running court.

WHO IS RUNNING INTERNET ?

- According to an infographic from internet corporation for assigned name and number (ICANN) no one person,company,organisation or government runs internet.
- It is globally distributed computer network comprised of many voluntarily interconnected autonomous networks.

WHICH GOVERNING BODY CONTROLS INTERNET ?

- ICANN is not for profit organisation was established 1998. Its mission is to help and keep internet secure, stable & inter operable.
- ICANN has no control over contents and doesn't deal with access to internet.

CAN YOU SHUTDOWN INTERNET ?

- If you really wanted to turn off the global internet you would have to seek out people on every continent and on every country. The internet is decentralised so there is no kill switch.

CAN YOU CRASH INTERNET ?

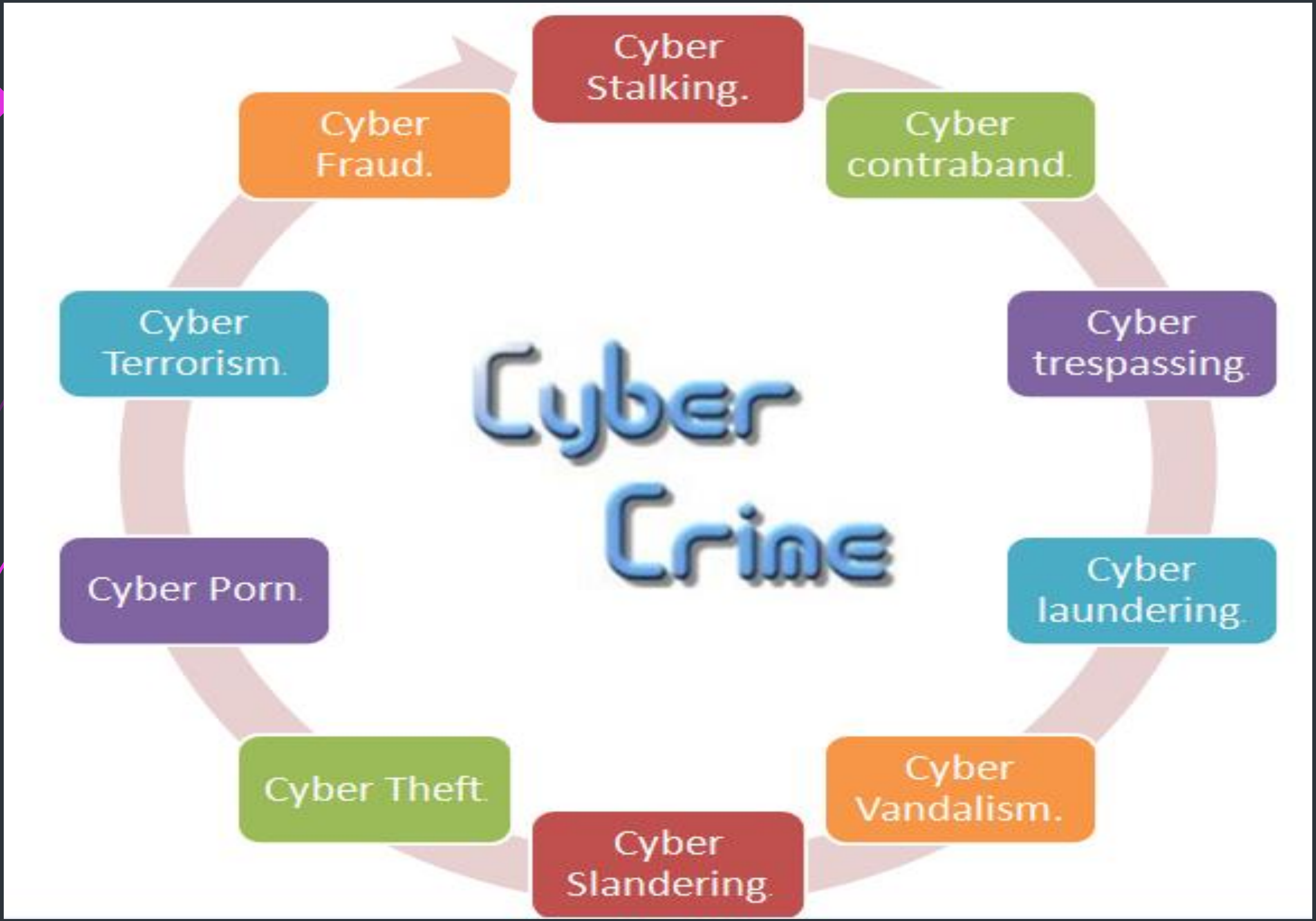
- When large outages occur, a sizeable portion of internet, or even entire country may affected. However, even this serious outages will not cause the internet to shutdown or crash.

CYBERSPACE

- The environment in which communication over computer networks occurs.
- Cyberspace's core feature is an interactive and virtual environment for a broad range of participants.

CYBER CRIME

Misuse of technology / communication device/ computing services.



Cyber Crime

Cyber Stalking.

Cyber contraband.

Cyber trespassing.

Cyber laundering.

Cyber Vandalism.

Cyber Slandering.

Cyber Theft.

Cyber Porn.

Cyber Terrorism.

Cyber Fraud.

ELECTRONIC EVIDENCE

Evidence means and includes all documents including electronic records produced for inspection of the court.

ELECTRONIC EVIDENCE IS FOUND IN:

1)E-mails

2)Photographs

3)ATM transaction Logs

4)Word Processing Documents

5)Instant Message History

6) Files Saved from Accounting Programs

7)Spreadsheets

8) Internet Browser History

9)Databases

Continued...

10) Contents of Computer Memory

11) Computer Backup

12) Computer Printouts

13) Global Positioning System Tracks

14) Logs from a Electronic Door Locks

15) Digital Video or Audio Files

CHARACTERISTICS OF DIGITAL EVIDENCE

- E-Evidence tends to be more voluminous
- It is more difficult to destroy
- It can be easily modified
- It can be easily duplicated
- Potentially more expressive
- More readily available

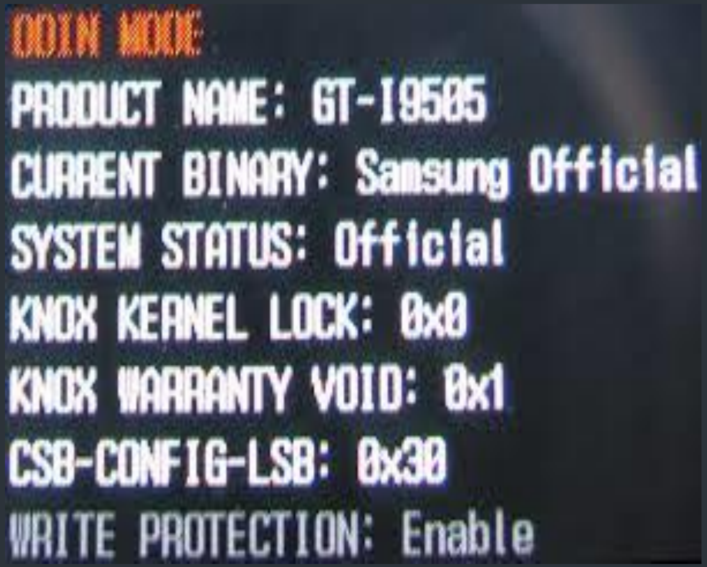
DIGITAL FORENSICS

- Computer Forensics is a branch of computer science pertaining to legal evidence found in computers and digital storage mediums.

- Computer Forensics is also known as digital forensics.

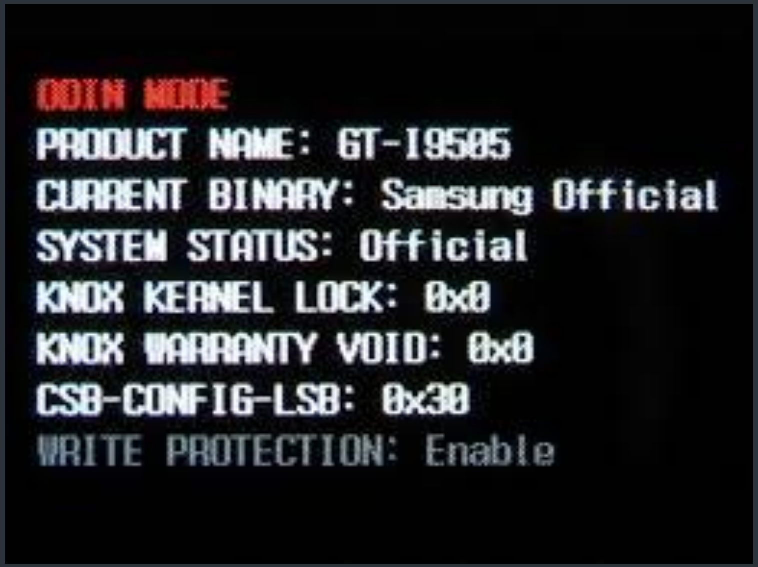
- The goal of computer forensics is to explain the current state of a digital artifact.

Root Status in Mobile Devices



```
ODIN MODE
PRODUCT NAME: GT-I9505
CURRENT BINARY: Samsung Official
SYSTEM STATUS: Official
KNOX KERNEL LOCK: 0x0
KNOX WARRANTY VOID: 0x1
CSB-CONFIG-LSB: 0x30
WRITE PROTECTION: Enable
```

Rooted

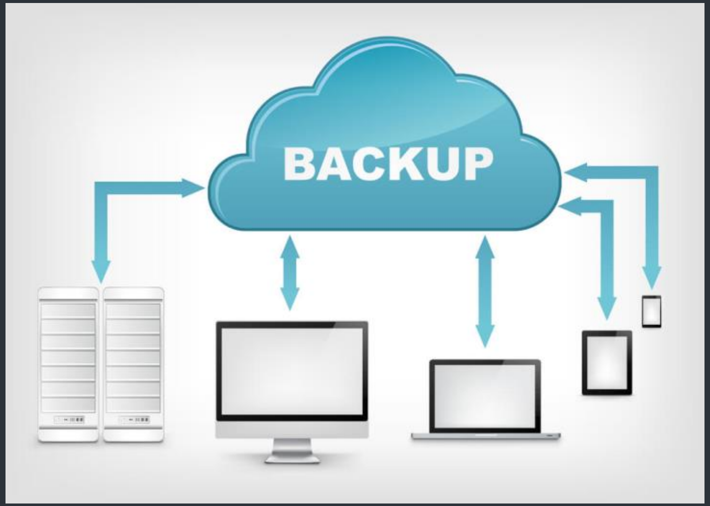


```
ODIN MODE
PRODUCT NAME: GT-I9505
CURRENT BINARY: Samsung Official
SYSTEM STATUS: Official
KNOX KERNEL LOCK: 0x0
KNOX WARRANTY VOID: 0x0
CSB-CONFIG-LSB: 0x30
WRITE PROTECTION: Enable
```

Unrooted

Evidence that can be Gathered Digitally

- Computer documents, emails, text and instant messages, transactions, images and Internet histories are examples of information that can be gathered from electronic devices and used very effectively as evidence.
- For extended example, mobile devices use online-based based backup systems, also known as the "cloud", that provide forensic investigators with access to text messages and pictures taken from a particular phone or different phones with same ID.
- In addition, many mobile devices store information about the locations where the device traveled and when it was there. To gain this knowledge, investigators can access an average of the last 200 cell locations accessed by a mobile device.



- Satellite navigation systems and satellite radios in cars can provide similar information. Even photos posted to social media such as Facebook may contain location information.
- Photos taken with a Global Positioning System (GPS)-enabled device contain file data that shows when and exactly where a photo was taken.
- By gaining a subpoena for a particular mobile device account, investigators can collect a great deal of history related to a device and the person using it.

FIVE HURDLES OF ADMISSIBILITY:

- **Relevance:**

  Is the evidence is related to the case?

- **Authenticity:**

  Is the submitted evidence authentic?

- **Hearsay:**

  Is the evidence strong enough or just a hearsay?

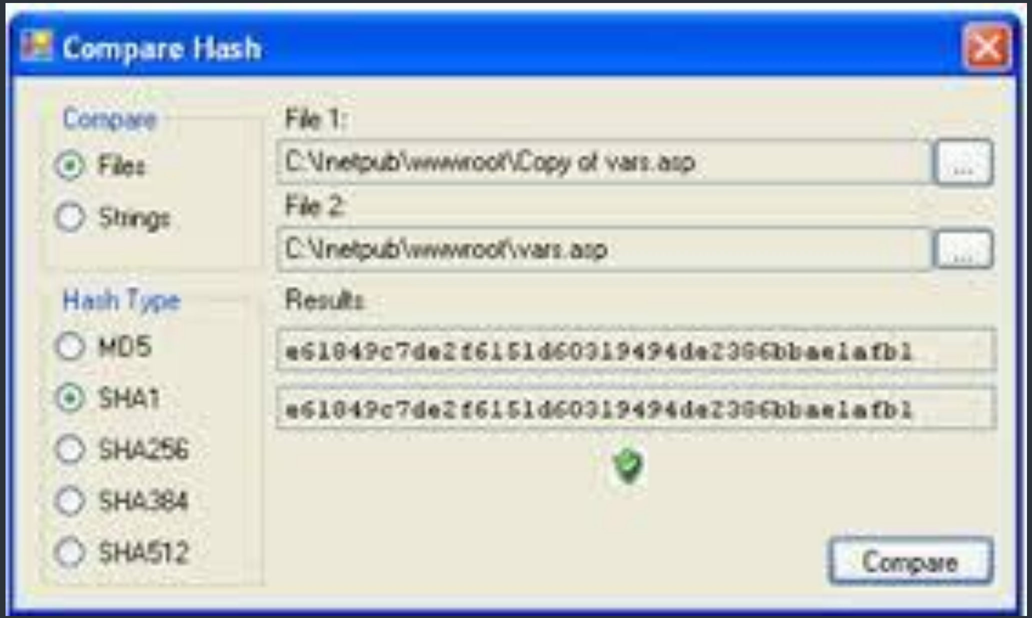
- ✓ **Unfair Prejudice**:
  Is the evidence presented under unfair prejudice?

Original Writing Rule:
Is the evidence presented first hand and not the copy?

HASH TECHNOLOGY

- The process of creating a specific alpha numeric identifier for each file is known as hashing and the value is known as hash value.

- Any change in the file will produce a dramatically different hash value.



Compare Hash

Compare: ● Files ○ Strings

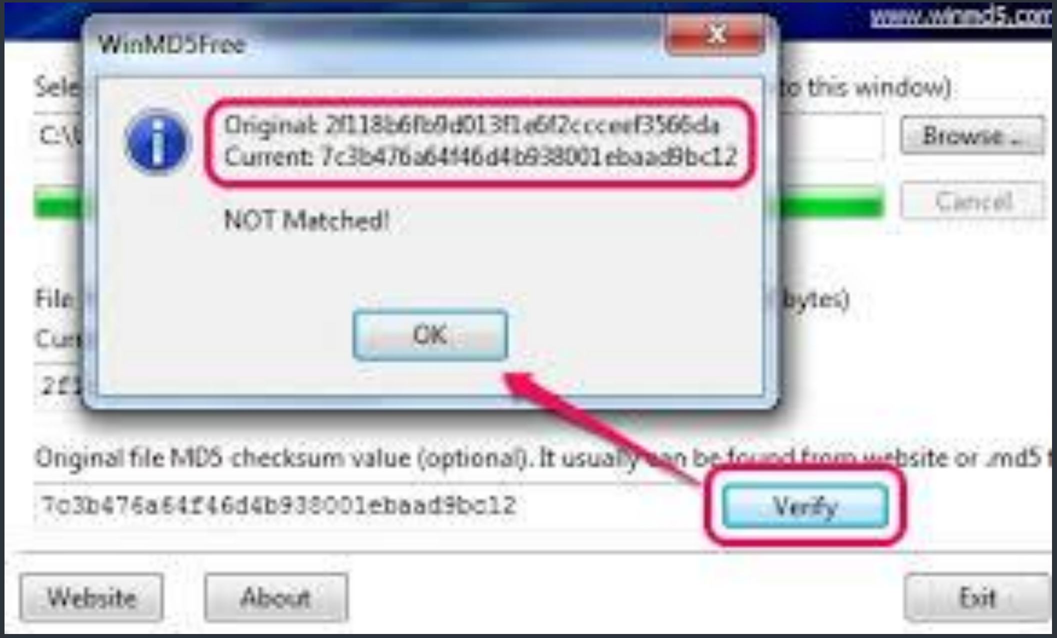
File 1: C:\Inetpub\wwwroot\Copy of vars.asp

File 2: C:\Inetpub\wwwroot\vars.asp

Hash Type: ○ MD5 ● SHA1 ○ SHA256 ○ SHA384 ○ SHA512

Results:

```
e61049c7de2f6151d60319494de2306bbae1afb1
e61049c7de2f6151d60319494de2306bbae1afb1
```



WinMD5Free

Original: 2f118b6fb9d013f1e6f2ccceef3566da
Current: 7c3b476a64f46d4b938001ebaad9bc12

NOT Matched!

Sele
C:\
to this window)
File
Curr
2f1
bytes)

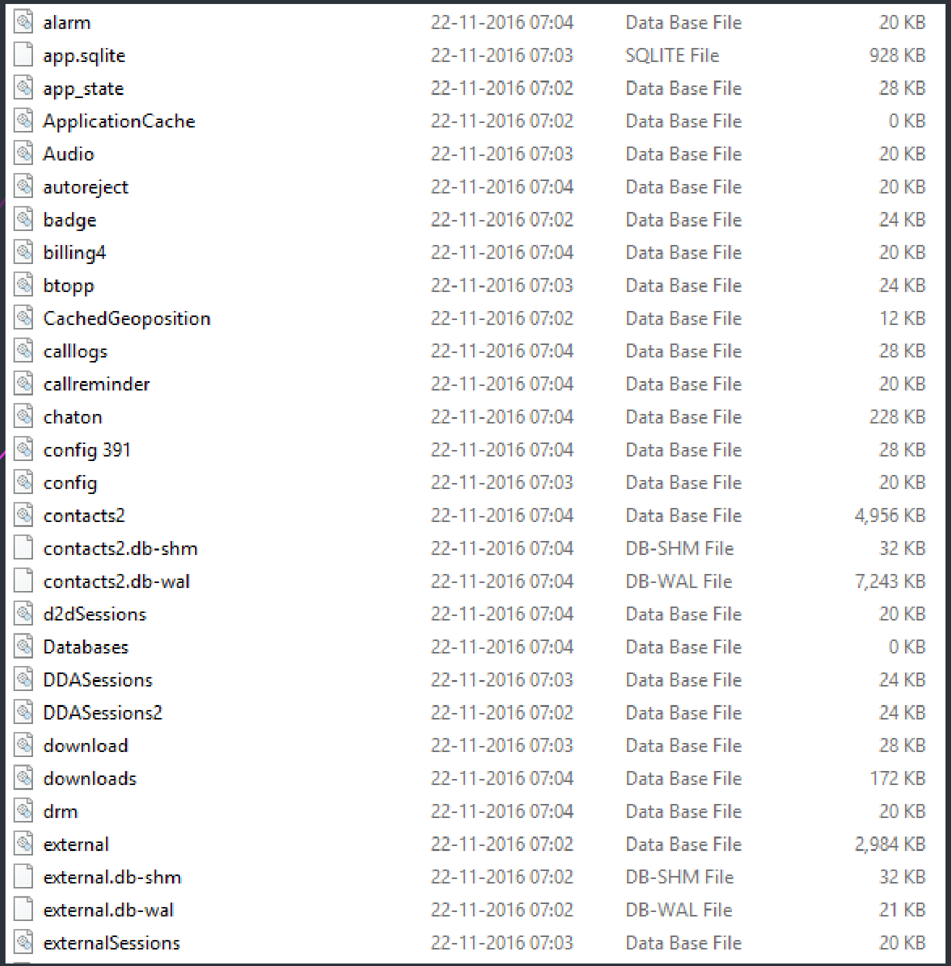
Original file MD5 checksum value (optional). It usually can be found from website or .md5

7c3b476a64f46d4b938001ebaad9bc12

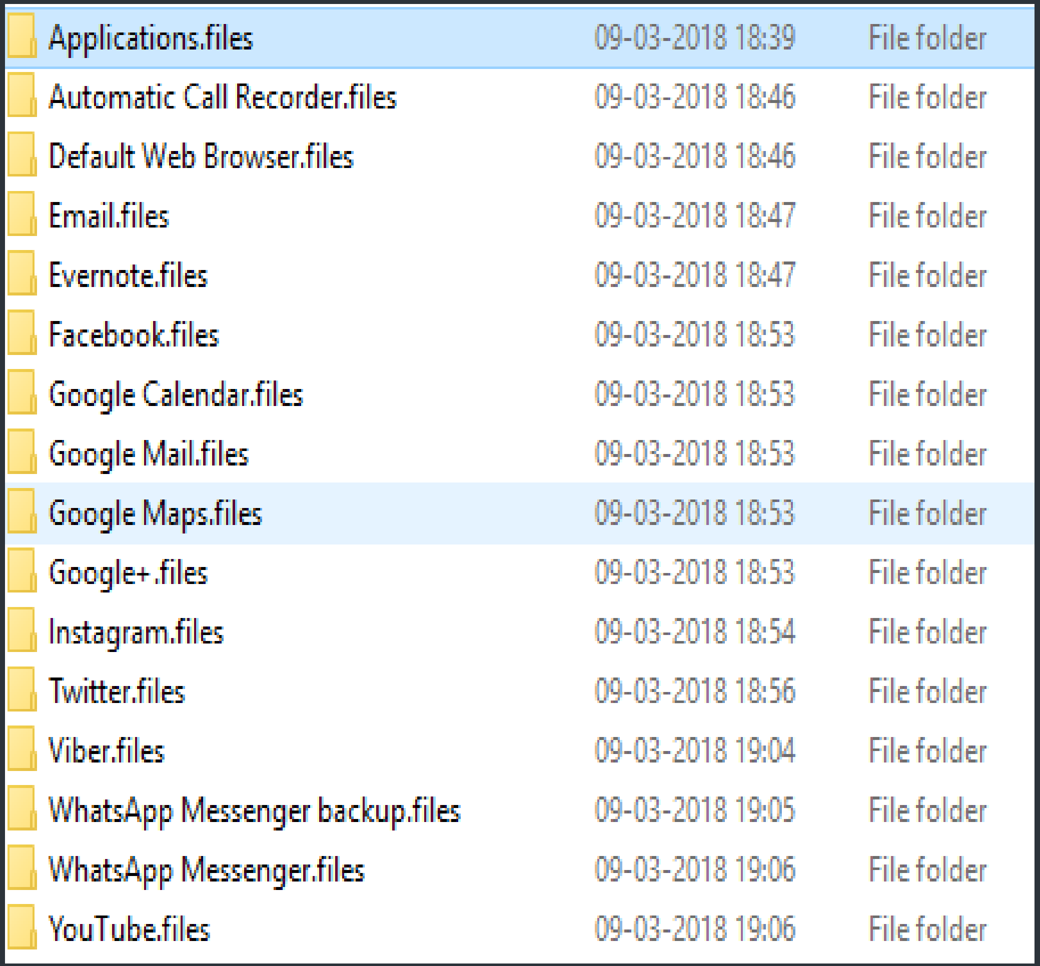
Raw Data to Organized Data

- The raw data collected is often contains too much data to analyze it sensibly. This is especially so for labs using computers as this may produce large amounts of data.
- The data needs to be organized or manipulated using deconstruction analysis techniques.
- Large amounts of data may contain voluminous data comprising of various evidences. Hence convergence of raw data to organized or sorted data is equally important than just producing it in the form of evidence.
- Partial collection of data i.e. existing evidence may lead an innocent to conviction.

TRANSITION OF RAW DATA TO ORGANIZED DATA



alarm	22-11-2016 07:04	Data Base File	20 KB
app.sqlite	22-11-2016 07:03	SQLITE File	928 KB
app_state	22-11-2016 07:02	Data Base File	28 KB
ApplicationCache	22-11-2016 07:02	Data Base File	0 KB
Audio	22-11-2016 07:03	Data Base File	20 KB
autoreject	22-11-2016 07:04	Data Base File	20 KB
badge	22-11-2016 07:02	Data Base File	24 KB
billing4	22-11-2016 07:04	Data Base File	20 KB
btopp	22-11-2016 07:03	Data Base File	24 KB
CachedGeoposition	22-11-2016 07:02	Data Base File	12 KB
calllogs	22-11-2016 07:04	Data Base File	28 KB
callreminder	22-11-2016 07:04	Data Base File	20 KB
chaton	22-11-2016 07:04	Data Base File	228 KB
config 391	22-11-2016 07:04	Data Base File	28 KB
config	22-11-2016 07:03	Data Base File	20 KB
contacts2	22-11-2016 07:04	Data Base File	4,956 KB
contacts2.db-shm	22-11-2016 07:04	DB-SHM File	32 KB
contacts2.db-wal	22-11-2016 07:04	DB-WAL File	7,243 KB
d2dSessions	22-11-2016 07:04	Data Base File	20 KB
Databases	22-11-2016 07:04	Data Base File	0 KB
DDASessions	22-11-2016 07:03	Data Base File	24 KB
DDASessions2	22-11-2016 07:02	Data Base File	24 KB
download	22-11-2016 07:03	Data Base File	28 KB
downloads	22-11-2016 07:04	Data Base File	172 KB
drm	22-11-2016 07:04	Data Base File	20 KB
external	22-11-2016 07:02	Data Base File	2,984 KB
external.db-shm	22-11-2016 07:02	DB-SHM File	32 KB
external.db-wal	22-11-2016 07:02	DB-WAL File	21 KB
externalSessions	22-11-2016 07:03	Data Base File	20 KB



Applications.files	09-03-2018 18:39	File folder
Automatic Call Recorder.files	09-03-2018 18:46	File folder
Default Web Browser.files	09-03-2018 18:46	File folder
Email.files	09-03-2018 18:47	File folder
Evernote.files	09-03-2018 18:47	File folder
Facebook.files	09-03-2018 18:53	File folder
Google Calendar.files	09-03-2018 18:53	File folder
Google Mail.files	09-03-2018 18:53	File folder
Google Maps.files	09-03-2018 18:53	File folder
Google+.files	09-03-2018 18:53	File folder
Instagram.files	09-03-2018 18:54	File folder
Twitter.files	09-03-2018 18:56	File folder
Viber.files	09-03-2018 19:04	File folder
WhatsApp Messenger backup.files	09-03-2018 19:05	File folder
WhatsApp Messenger.files	09-03-2018 19:06	File folder
YouTube.files	09-03-2018 19:06	File folder

ADMISSIBILITY OF ELECTRONIC EVIDENCE

- **Conditions of Admissibility:**

✓ The computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process the information for the purpose of any activities regularly carried on over that period by the person having lawful control over use of computer.

✓ During the said period information contained in the electronic recorder of the kind from which the information so contained is derived was regularly fed into computer in the ordinary course of said activities.

Continued...

- ✓ Throughout the material part of the said period the computer was operating properly or if not then in respect of any period in which it was out of operation during that part of the period was not such as to affect the electronic record or accuracy of the content.

- ✓ The information contained in the electronic record produces or is derived from such information fed into the computer in ordinary course of said activity.

CALL DATA RECORDS AS EVIDENCE

- Call Data Records do aid in preliminary investigation but cannot be taken as conclusive evidence because of following problems

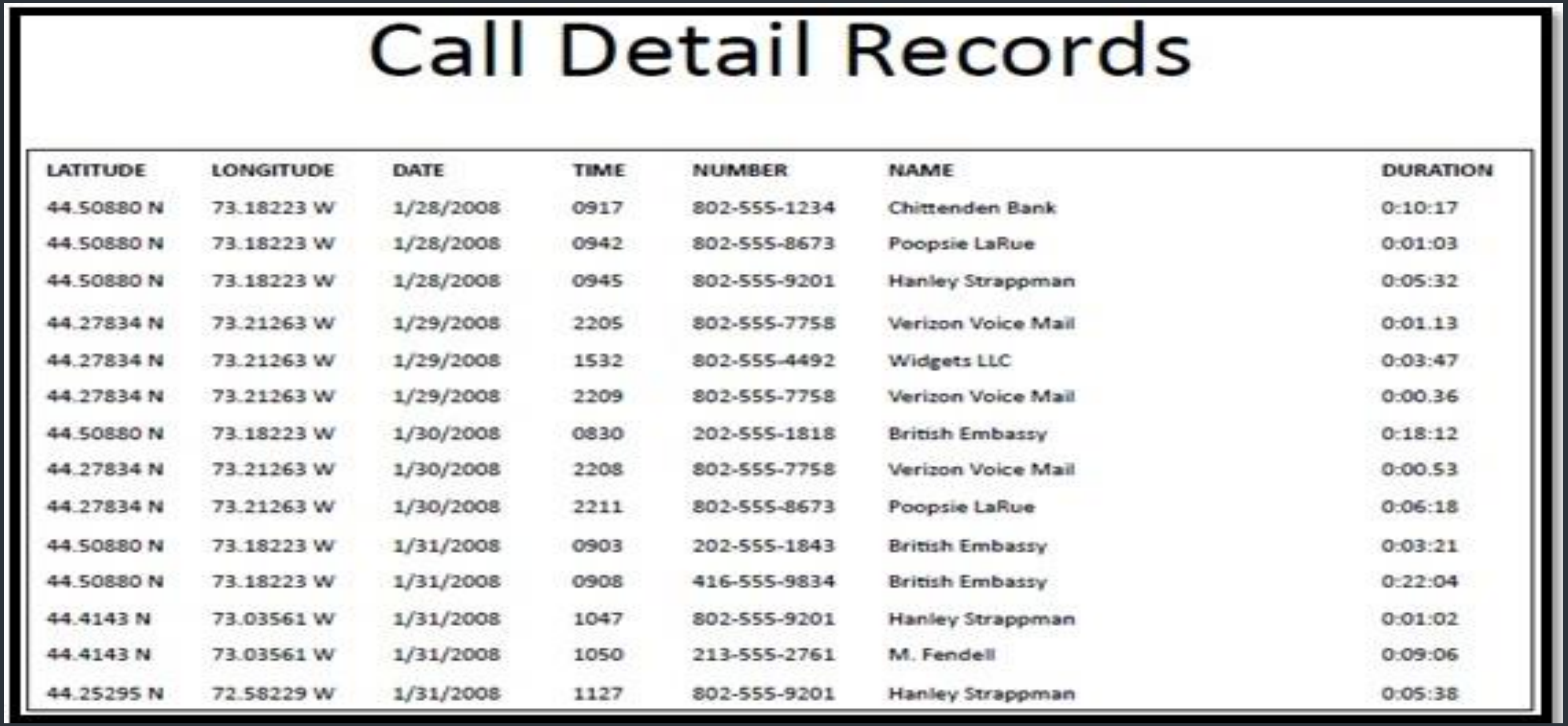
✓ The mobile handset or SIM could be in someone else's name as written in receipt/invoice.

✓ Call Data records are not certified.

✓ SIM Card was cloned or IMEI number was spoofed.

✓ Mobile number snooping has taken place using soft wares.

Example



Call Detail Records

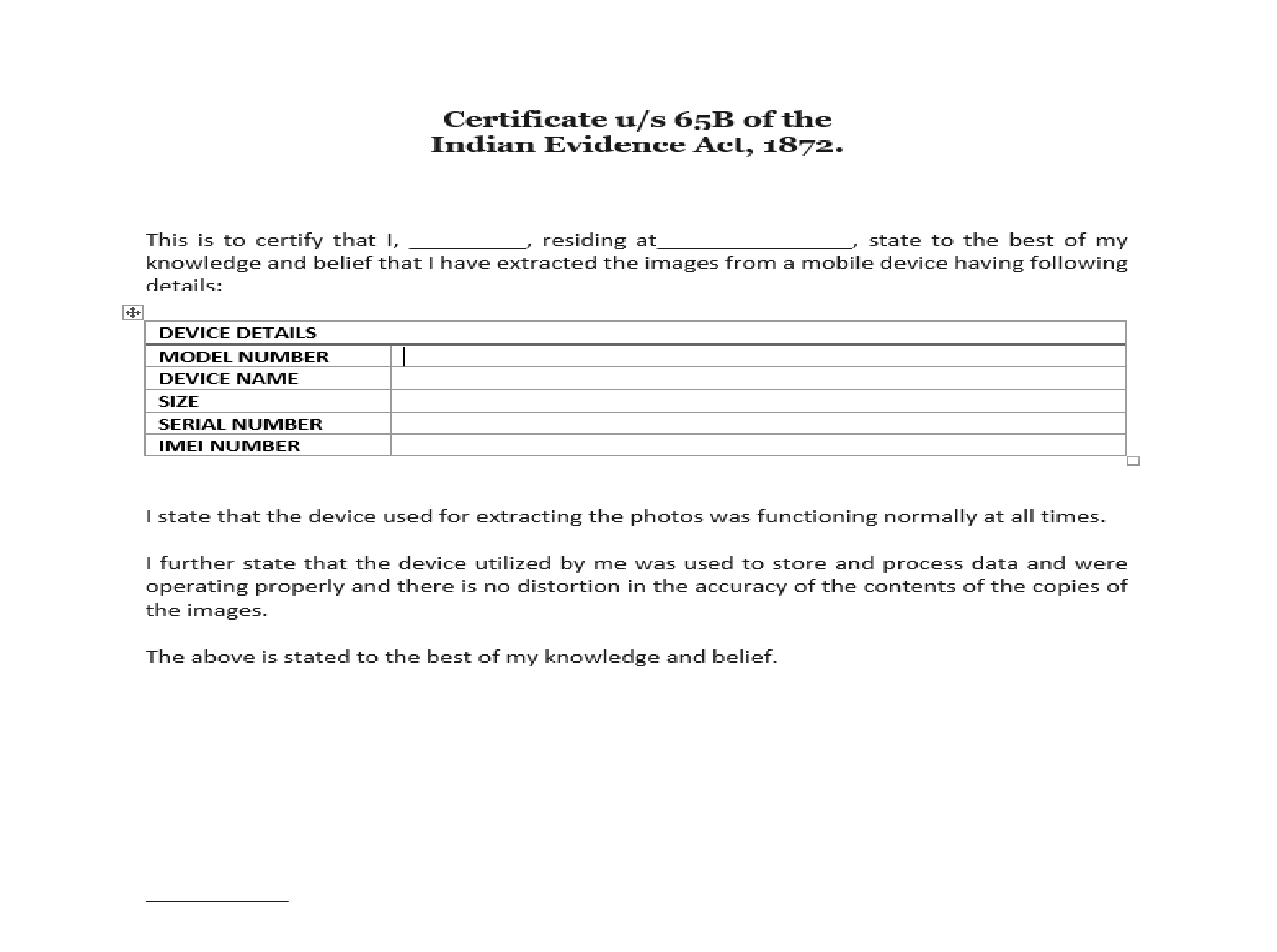
LATITUDE	LONGITUDE	DATE	TIME	NUMBER	NAME	DURATION
44.50880 N	73.18223 W	1/28/2008	0917	802-555-1234	Chittenden Bank	0:10:17
44.50880 N	73.18223 W	1/28/2008	0942	802-555-8673	Poopsie LaRue	0:01:03
44.50880 N	73.18223 W	1/28/2008	0945	802-555-9201	Hanley Strappman	0:05:32
44.27834 N	73.21263 W	1/29/2008	2205	802-555-7758	Verizon Voice Mail	0:01.13
44.27834 N	73.21263 W	1/29/2008	1532	802-555-4492	Widgets LLC	0:03:47
44.27834 N	73.21263 W	1/29/2008	2209	802-555-7758	Verizon Voice Mail	0:00.36
44.50880 N	73.18223 W	1/30/2008	0830	202-555-1818	British Embassy	0:18:12
44.27834 N	73.21263 W	1/30/2008	2208	802-555-7758	Verizon Voice Mail	0:00.53
44.27834 N	73.21263 W	1/30/2008	2211	802-555-8673	Poopsie LaRue	0:06:18
44.50880 N	73.18223 W	1/31/2008	0903	202-555-1843	British Embassy	0:03:21
44.50880 N	73.18223 W	1/31/2008	0908	416-555-9834	British Embassy	0:22:04
44.4143 N	73.03561 W	1/31/2008	1047	802-555-9201	Hanley Strappman	0:01:02
44.4143 N	73.03561 W	1/31/2008	1050	213-555-2761	M. Fendell	0:09:06
44.25295 N	72.58229 W	1/31/2008	1127	802-555-9201	Hanley Strappman	0:05:38

IP ADDRESS AS EVIDENCE

- IP Address provides only the location at which one of any number of computer devices ,much like a telephone number can be used for any number of telephones.

- Thus it is no more likely that the subscriber to an IP address carried out a particular computer function.

65(B) CERTIFICATE



Certificate u/s 65B of the
Indian Evidence Act, 1872.

This is to certify that I, ___________, residing at__________________, state to the best of my knowledge and belief that I have extracted the images from a mobile device having following details:

DEVICE DETAILS	
MODEL NUMBER	
DEVICE NAME	
SIZE	
SERIAL NUMBER	
IMEI NUMBER	

I state that the device used for extracting the photos was functioning normally at all times.

I further state that the device utilized by me was used to store and process data and were operating properly and there is no distortion in the accuracy of the contents of the copies of the images.

The above is stated to the best of my knowledge and belief.

____

Thank you

Dr. Harold D’costa - +91-9637612097
Email   : hld@rediffmail.com
Website: www.cybersolution.in