The Omega Case

- July 31, 1996
- The Servers of CNC department in Omega Corporation are booted
- Message flash saying file server is being fixed
- Subsequent system crash
- All programs deleted, manufacturing halts

The Omega Case

- No backup tapes found
- All programs and code generators destroyed
- 25, 000 products to customize 500, 000 designs affected
- 34 years of growth lost in 1 year
- Disgruntled network administrator
- Fired because of non – cooperation

The Omega Case

- Network Administrator's house searched
  - Computers, CDs, motherboards, 500 disks, 12 hard drives, 2 formatted backup tapes
  - Backup tapes were labeled 14/5/96 and 1/7/96
- The cause of deletion, a six line program

The Omega Case

- 30/7/96 (Trigger Date)
- F: (Accessing the server)
- F:\LOGIN\LOGIN 12345 (first user logs in with supervisory rights and no password)
- CD\PUBLIC (gives access to the PUBLIC directory, a file system area)
- FIX.EXE /Y F:*.* (Run code, A=Yes, All files)
- PURGE F:\ /ALL

Electronic Evidence

- All items seized from the suspect's house: CDs, HDD, formatted Back up tapes, etc.

- But what is needed to establish guilt beyond reasonable doubt?
  - Correct procedure having been followed by IO
  - The function of the 6 line program (Expert Opinion)
  - The fact that it could only have been installed by the suspect

Collection of digital evidence - Challenges

- Any action during investigation should not compromise evidence
- If accessing original media is necessary, the IO responsible must be competent to do so
- All procedures should be documented and preserved in a manner verifiable by an independent third party

Internet based crimes

- DNS spoofing
- Web defacement
- FTP attacks
- Bogus Websites
- Web spoofing
- Website based launch of malicious code, cheating and fraud

Fundamentals of investigation

- The KEY to almost all web based crimes
  - **IP Address**
    - Figures in server logs
    - Figures in email headers
- Identify the correct IP address
  - Time zones
  - Shivaji Maharaj (Airtel case)

Fundamentals of investigation

- Track physical location of the IP Address
- Identify the suspect computer to which the IP address was allotted
- Collect corroborative evidence from suspect computer

Whois Search

Whois search for 208.113.199.97 using www.whois.net

```
OrgName:      New Dream Network, LLC
OrgID:        NDN
Address:      417 Associated Rd
Address:      PMB #257
City:         Brea
StateProv:    CA
PostalCode:   92821
Country:      US

NetRange:     208.113.128.0 - 208.113.255.255
CIDR:         208.113.128.0/17
NetName:      DREAMHOST-BLK6
NetHandle:    NET-208-113-128-0-1
Parent:       NET-208-0-0-0-0
NetType:      Direct Allocation
NameServer:   NS1.DREAMHOST.COM
NameServer:   NS2.DREAMHOST.COM
NameServer:   NS3.DREAMHOST.COM
Comment:
RegDate:      2006-04-12
Updated:      2007-11-01
```

Extended Info

IP Address: 208.113.199.97

IP Location:  United States

Website Status: active

Server Type: Apache/2.0.61 (Unix) PHP/4.4.7 mod_ssl/2.0.61 OpenSSL/0.9.7e mod_fastcgi/2.4.2 DAV/2 SVN/1.4.2

Cache Date: 2008-04-29 03:21:29 MST

Server Logs

#Software: Microsoft Internet Information Services 6.0

#Version: 1.0

#Date: 2007-10-13 06:45:10

2007-10-13 00:45:26 *172.224.24.114* -67.19.217.53 80 GET /index.htm - 200 7930 248 31 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+2000+Server)

Section 65B(4)

- "In any proceedings where it is desired to give a statement in evidence by virtue of this section, a ***certificate***....."
  - identifying the electronic record.. and describing the manner in which it was produced;
  - giving such particulars of any device involved ..
  - dealing with any of the matters to which the conditions mentioned in subsection (2) relate,

Section 65B(4) Contd…….

and purporting to be ***signed by a person occupying responsible official position*** in relation to

– the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate

Who will give the Certificate under 65B(4)

- In criminal cases, where accused's computer is seized and his HDD is cloned
  - The cyber forensic analyst cloning the HDD and presenting evidence after analysis of the clone

- In civil cases
  - The Plaintiff or the Defendant who desires to furnish evidence from his computer

Nature of 65B(4) Certificate

- Not an expert opinion report
- Only makes evidence admissible
- After admissibility
  - Evidentiary value of evidence to be examined through expert opinion
  - E.g., deep fakes require opinion by person expert in State-of-the Art Advanced Morphing Detection

Amendment to Bankers' Books Evidence Act (Contd…)

- Printout/Copy of entry or the book shall be accompanied by
  - Cert. by Manager identifying the entry
  - Cert. by computer-in-charge giving details of data storage, safeguards and computer where such data is stored
  - Cert. by comp-in-charge (manner of affidavit) relating to integrity of printout and computer

State Vs. Navjot Sandhu

- Parliament attack case
- Laptop, storage devices recovered from a truck in Srinagar
- Laptop contained files relating to identity cards, stickers used by terrorists

State Vs. Navjot Sandhu

- Findings
  - If accuracy of computer evidence is to be challenged, burden lies on the side who makes such a challenge
  - User created files and system files, difference
  - Mere theoretical doubts cannot be cast on evidence

State Vs. Navjot Sindhu

- Gist of findings
  - Accessing a suspect computer after date of seizure *ipso facto* does not render evidence inadmissible;
  - If accuracy of computer evidence is challenged, burden is on party making such challenge;
  - Certificate under 65(B)(4) is not mandatory for making electronic evidence admissible

Anwar Vs. PK Basheer, SC Sep ’14

- Electronic record by way of secondary evidence is inadmissible unless accompanied by cert. under 65B(4)

- Earlier proposition laid down in *Navjot Sindhu* regarding no mandatory requirement of Cert. in 65B is bad in law and is overruled

Shafi Mohammed Vs. State of Rajasthan, 2017, SC

- Ss. 65A and 65B cannot be held to be a complete code on the subject
- Requirement of certificate under Section 65B(4) is not always mandatory
- Party not in possession of device from which document is produced
  - cannot be required to produce certificate under Section 65B(4) of the Evidence Act

Arjun Panditrao Khotkar Vs. Kailash Kushanroa Gorantyal & Ors.,SC, July 2019

- In view of Anvar P.V., the pronouncement of this Court in Shafi Mohammad needs reconsideration.
- With the passage of time, reliance on electronic records during investigation is bound to increase.
- The law therefore needs to be laid down in this regard with certainty.
- It was then considered appropriate to refer the matter to a larger Bench.

Arjun Panditrao Khotkar Vs. Kailash Kushanrao Gorantyal & Ors., SC, July 2020

- Reference considered by a larger Bench
  - Shafi Mohammed Overruled
    - *An application can always be made to a Judge for production of such a certificate from the requisite person under Section 65B(4) in cases in which such person refuses to give it.*
  - But where all possible steps for obtaining the certificate have failed, obligation for production is to be relieved
    - *Has to be decided on a case-to-case basis*
    - *Person required to produce must first initiate own efforts*
    - *If that fails, will apply to the Court for a direction to produce*

Arjun Panditrao Khotkar Vs. Kailash Kushanrao Gorantyal & Ors., SC, July 2020

- *Anvar P.V.,* is correct law
- *Tomaso Bruno* is *per incurium*
- *Shafi Mohammed* overruled
- ISPs and TSPs to maintain CDRs and other records for the concerned period
  - in tune with Section 39 of the Evidence Act (only relevant part of a longer record to be maintained)
  - in a segregated and secure manner if a particular CDR or other record is seized during investigation in the said period

Arjun Panditrao Khotkar Vs. Kailash Kushanrao Gorantyal & Ors., SC, July 2020

- Cert. can be produced at any stage during trial with copy to the other party
- Directions to ISPs and TSPs shall be applied in criminal trials till
  - appropriate directions are issued under relevant terms of the applicable licenses, or
  - under Section 67C of the IT Act
    - *Intermediaries to retain information in manner and format and for the duration prescribed by the C.G.*

Examiner of Electronic Evidence

- Examiner of elec. Evidence (S/79A, IT Act)
  - Central Govt. may notify in O.G.
  - Any agency/dept/body of C.G. or S.G.
  - For expert opinion on electronic evidence
- Opinion becomes relevant fact u/s 45A (new) of the Evidence Act
- Bottleneck
  - Why only C.G. or S.G. Agency?
  - Why not private agencies of proven competency?
  - Contributing to pendency of cases?

Admissibility of Text Messages

- Printouts of text message may be admitted following the usual method under Section 65B
- Court may summon the service provider to give details of text messages from a particular number
- Printouts must contain date, time, telephone number of each text message for verification

Admissibility of Whatsapp Messages

- The same procedure to be followed like in case of text messages
- However, Whatsapp messages are not stored on Whatsapp servers unlike TSPs in text messages
- Reliability must be established, if questioned

Admissibility of Evidence from Instagram, Facebook

- Pages may be saved
- Screenshots may be taken
- If above are produced in Court, 65B Cert. must be produced
- Where contents are questioned, it may be necessary to establish truthfulness by exhibiting original *(Recollect Arjun P. Khotkar Case)*

CCTV footage

- Admissible
- Procedure under Section 65B to be followed
- If 65B cert. exists, oral evidence necessary only when authenticity is questioned
- If 65B conditions are met, original medial is not necessary as an exhibit
- Only when court is not satisfied with evidence led, it may require original media

Website

- Entire website may be downloaded
- Screenshots may be taken
- Original website may also be exhibited directly on a computer/phone in which case no need for 65B Cert.
- However, better to have 65B Cert. in case original website has been removed

Emails

- Procedure under Section 65B
- Contents of e-mails as evidence
  - If parties admit the contents
  - If email is digitally signed
  - By subsequent conduct of parties
- In the alternative, by an IP address trace
- Finally, by examination of witnesses

Emails

- If emails have been produced after
  - Following procedure in 65B
  - Genuineness has been proved by witnesses

  Subsequent deletion is inconsequential
- 65B(1) – Email admitted as direct evidence
- 65(c) – When the original has been lost or destroyed

IT Act 2000

- No Procedure for search and seizure specifically described
- 65B, Evidence Act talks only about admissibility on basis of Cert. under 65B(4)
- Conclusion?

Questions?