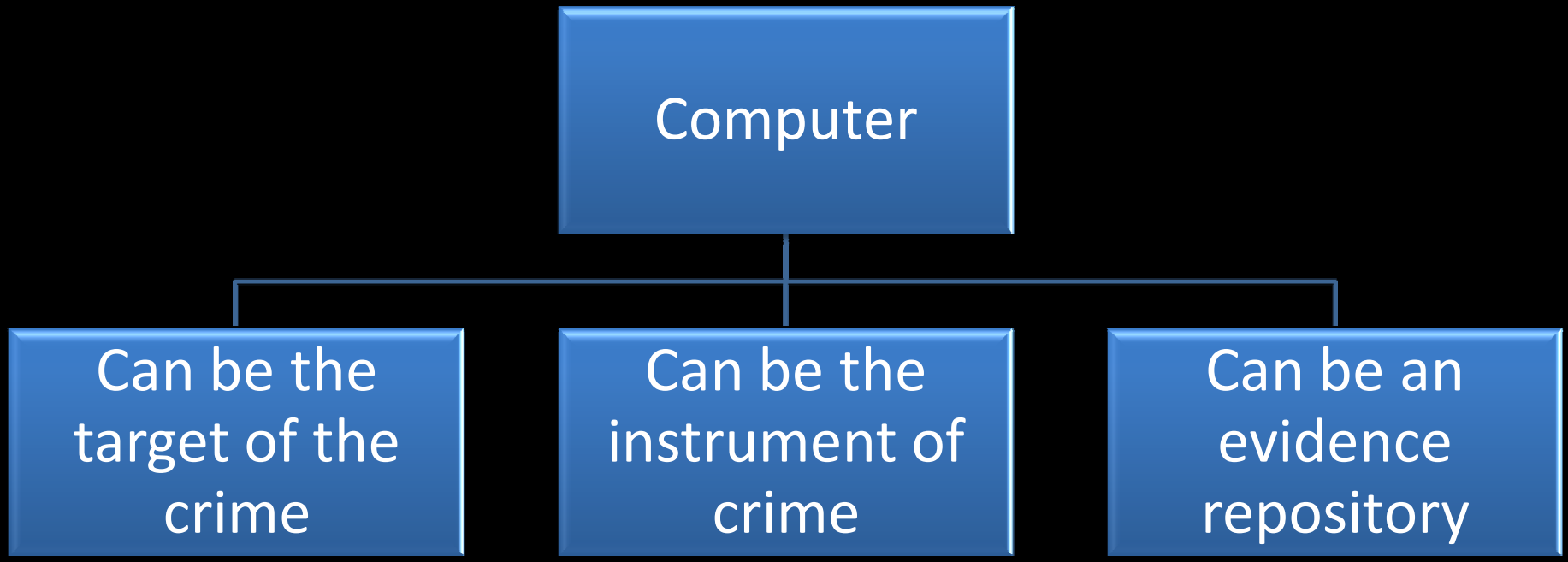

COMPUTER
FORENSICS

Computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

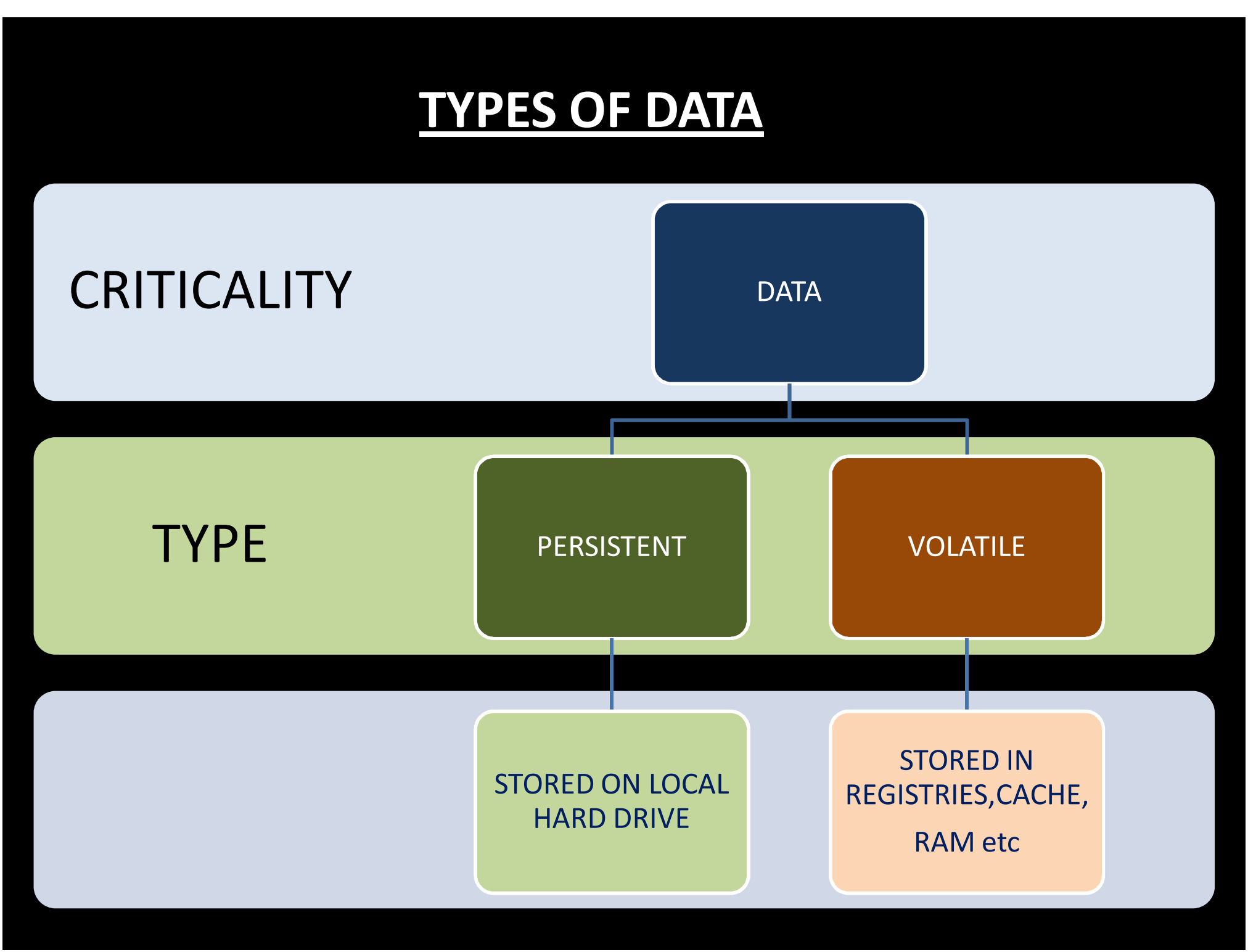
More simply….

…….Process of Investigation

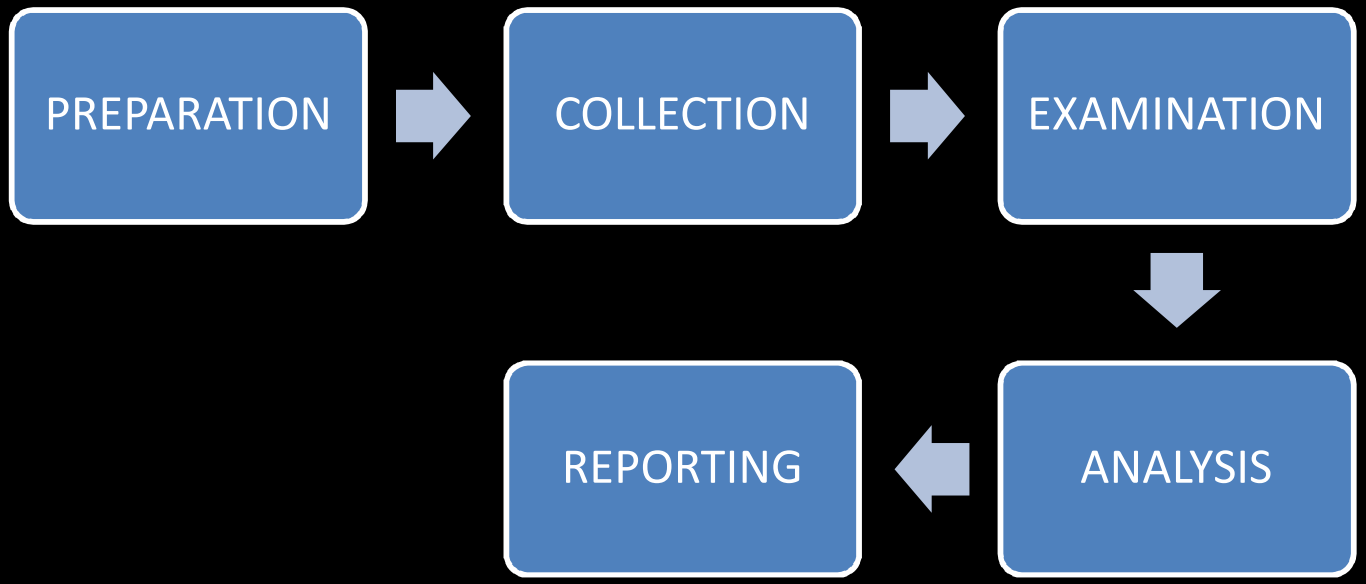
TYPE OF INCIDENT



TYPES OF DATA



STEPS TO FORENSICS



TYPES OF COMPUTER FORENSIC TOOLS

Hardware Forensic Tools

Software Forensic Tools

ACCREDITIONS BEFORE SETTING UP

- American Society of Crime Laboratory Directors (ASCLD)
- Encase Certification
- EMR
- Forensic Recovery of Evidence Device (F.R.E.D.)
- High-Tech Crime Network (HTCN)
- High Technology Crime Investigation Association (HTCIA)

EAVES DROP : EMR

Someone sitting in a van outside a person's house can read the EMR that is emanating from the user's laptop computer inside the house and reconstruct the information from the user's monitor on a different device.

Different devices have different levels of susceptibility .

A handheld calculator gives off a signal as much as a few feet away, and computer's electromagnetic field can give off emissions up to half a mile away. The distance at which emanations can be monitored depends on whether or not there are conductive media such as power lines, water pipes or even metal cabinets in the area that will carry the signals further away from the original source.

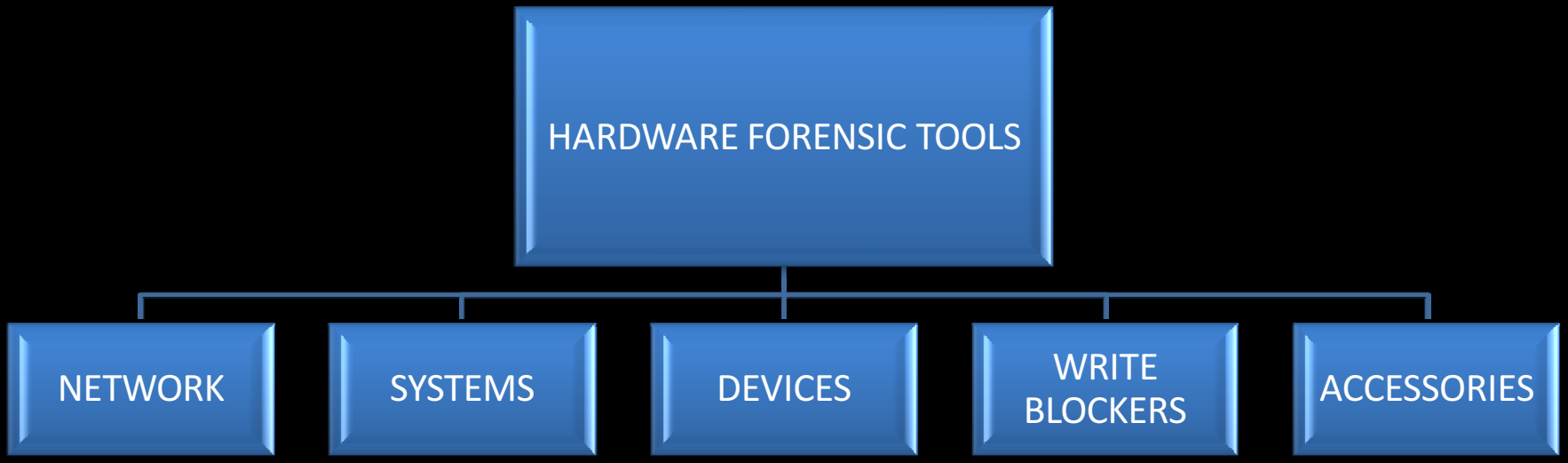
Phenomenon is more commonly referred to as van Eck phreaking, named after Wim van Eck, who has demonstrated that the screen content of a video display unit could be reconstructed at a distance using low-cost home-built equipment - a TV set with its sync pulse generators replaced with manually controlled oscillators.

Van Eck phreaking is a major security concern in an age of increasing pervasive computing. High-security government agencies are protecting themselves by constructing safe rooms that through the use of metallic shielding block the EMR from emanating out of the room or by grounding the signals so that they cannot be intercepted. It is possible, though costly, for individual users to shield their home computer systems from EMR leakage.

HARDWARE FORENSIC TOOLS

Hardware forensic tool varies and may range from simple, single purpose components to complete systems and servers. An example of the single-purpose component is the ACARD AEC-7720WP Ultra Wide SCSI-to-IDE Bridge. This device helps to write-block an IDE drive connected to a SCSI cable.

HARDWARE FORENSIC TOOLS



HARDWARE FORENSIC TOOLS

DIGITAL INTELLIGENCE F.R.E.D. SYSTEMS

FRED is our **F**orensic **R**ecovery of **E**vidence **D**evice. The FRED family of forensic workstations are highly integrated, flexible and modular forensic platforms

Designed for stationary laboratory

Approx Cost : 8000 $

Write blockers *are devices that allow acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents. They do this by allowing read commands to pass but by blocking write commands, hence their name.*

WRITE BLOCKERS

First FireWire Write-Blocker.

Completely integrated / internal system solution.

Integrated Write Blocked (Read-Only) Ports:

- SATA
- IDE
- SCSI
- USB
- FireWire 1394b/800 (1394a/400 backward compatible).

Integral LCD/keypad for viewing device and bridge status/info and configuration.

HARDWARE FORENSIC TOOLS

DIBS ADVANCED FORENSIC WORKSTATION

Highly developed and versatile item of forensic equipment .

Provides copying and analysis of drives using Windows XP operating system.

Designed for use in the laboratory. It can be used to both copy and analyze suspect hard drives.

HARDWARE FORENSIC TOOLS

PORTABLE UNITS (E.G TALON)

Powerful forensic data capture system specifically designed for the requirements of law enforcement, military, corporate security, investigators, and auditors.

Verifies data at up to 4 GB/min.

SOFTWARE FORENSIC TOOLS

-used to create mirror-image (bit-stream) backup files of hard disks

-to make a mirror-image copy of an entire hard disk drive or partition.

USES:

- Used to create evidence grade backups of hard disk drives on Intel based computer systems.

- Used to exactly restore archived SafeBack images to another computer hard disk drive of
equal or larger storage capacity.

- Used as an evidence preservation tool in law enforcement and civil litigation matters.

- Used as an intelligence gathering tool by military agencies.

SOFTWARE FORENSIC TOOLS

-Enables systems administrators, consultants, and investigators find the data they need on a computer disc.

-Designed to the National Institute of Standards Disk Imaging Tool Specification 3.1.6 the **ProDiscover®** Family provides affordable solutions for:

- **Incident Response**
- **Corporate Policy Compliance Investigation**
- **E-discovery**
- **Computer Forensics**

SOFTWARE FORENSIC TOOLS

- Offers eDiscovery, data discovery, and computer forensics solutions for corporations and government agencies.

- Validated by numerous courts, corporate legal departments, and government agencies.

In computing, ***MaruTukku*** *is a deniable encryption archive containing multiple file systems whose existence can only be verified using the appropriate cryptographic key.*

Steganography *is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.*

THE INDIAN SCENE

-**RESOURCE CENTRE FOR CYBER FORENSICS (RCCF)** is a pioneering institute, pursuing research activities in the area of Cyber Forensics. The centre was dedicated to the nation by the Honorable union minister Thiru A Raja, MCIT in August 2008.

-- ASIAN SCHOOL OF CYBER LAWS

-GUJARAT FORENSIC SCIENCES UNIVERSITY is a unique super specialized University and first of its kind in the world for conducting Degree/Diploma/Certificate courses in the field of Forensic Science, Behavioral Science, Criminology and other allied areas.

-**PERRY4LAW, FIRST AND EXCLUSIVE TECHNO-LEGAL FIRM IN INDIA** is dealing with the legal issues associated with the use of ICT worldwide and is actively engaged in advocating and using ICT for legal purposes including ODR and establishment of E-courts in India.

IN CASE YOU LIKED THIS PPT…PLS LEAVE A MESSAGE AT

anupam_tiwari@yahoo.com