Admissibility, Appreciation & Attribution of Digital Evidence

By

Antara Jha

What is Digital Evidence?

Any electronically stored or transmitted information that holds the potential to serve as proof in a legal proceeding.

Types of Digital Evidence

- Documents & Files
- Emails
- Messages & Chats
- Images & videos
- Data bases
- Social Media post
- Meta data
- Internet browsing history
- Geolocation data
- Call records
- Financial records
- System logs
- Computer memory
- Deleted or altered files

Factors on which Digital Evidence can be made admissible in the Court

- Relevance
- Authenticity
- Integrity
- Best Evidence Rule
- Expert testimony
- Chain of custody
- Legal requirements

- Expert testimony
- Chain of custody
- Legal requirements

- Technology reliability

Process of Appreciation for Digital Evidence

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Reporting

Legal recognition of electronic records:-

- Section 2 (BSA) says about document:

An electronic record on emails, server logs, documents on computers, laptop or smartphone, messages, websites, locational evidence and voice mail messages stored on digital devices are documents.

- Section 141 (BSA) says about the Judge to decide as to admissibility of evidence.
- Section 61 (BSA) says about electronic or digital record.
- Section 62 (BSA) says about Special provisions as to evidence relating to electronic record.

Cont.

- Section 63 (BSA) says about Admissibility of Electronic record.
- Section 2(t) (IT Act) says about electronic record:

“Data, record or data generated image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.”

- Section 81 (BSA) says about Presumption as to Gazettes in electronic or digital record.
- Section 85 (BSA) says about Presumption as to electronic agreements.

Cont.

- Section 86 (BSA) says about Presumption as to electronic records and electronic signatures.
- Section 87 (BSA) says about Presumption as to electronic signature certificates.
- Section 90 (BSA) says about Presumption as to electronic messages.
- Section 93 (BSA) says about Presumption as to electronic records five years old.

Case Laws

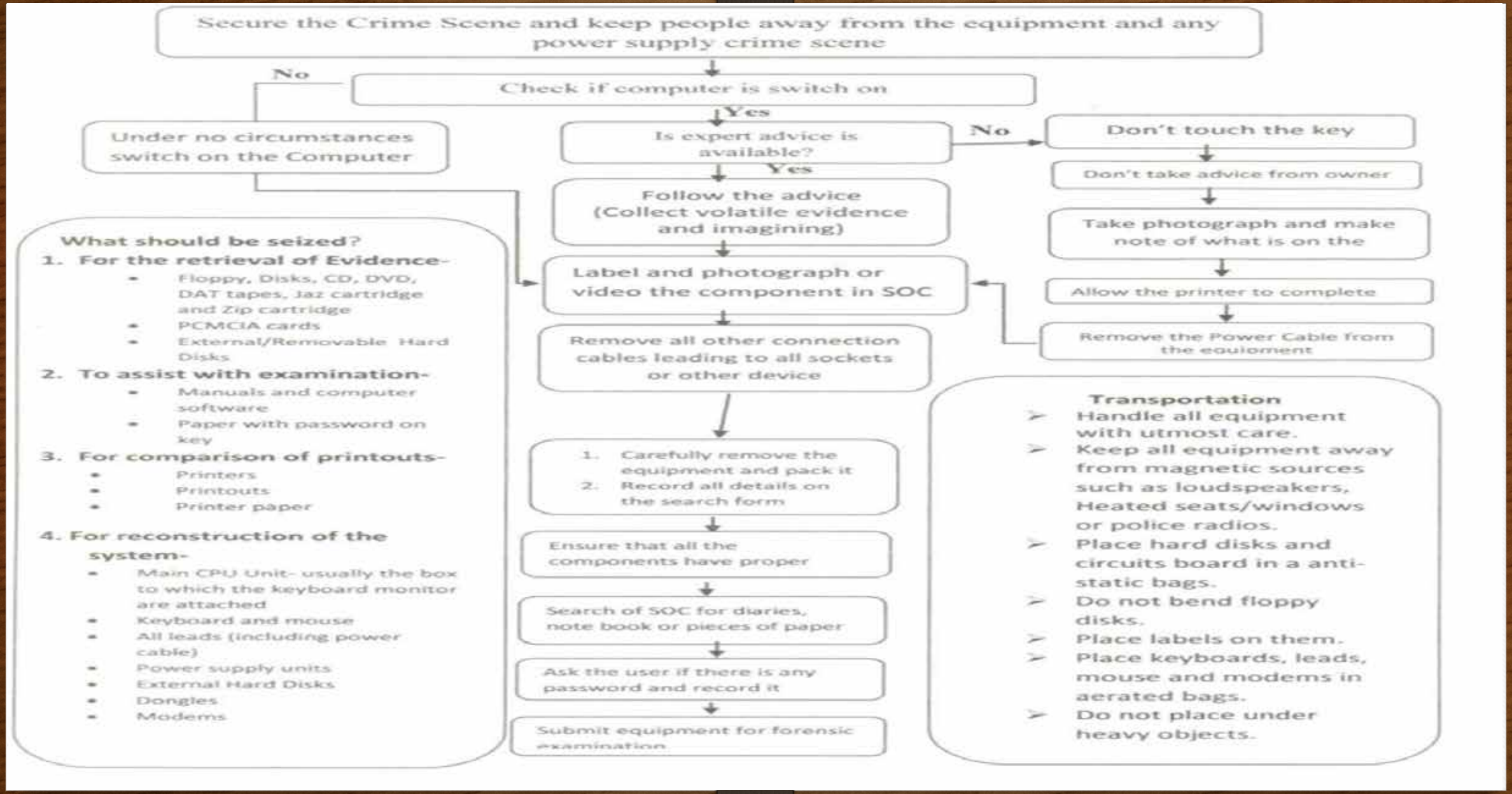
- State (NCT of Delhi) vs. Navjot Sandhu (2005)
- Anvar P.V. v. P.K. Basheer (2014)
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)

Arjun Panditrao Khotkar Case:

- Certification requirement
- Original Document Production
- Application for Certificate
- Stage for filing Certificate
- Directions to Service Providers
- Framing of Rules

Classification of Digital Evidence

- Primary Evidence
- Secondary Evidence


Secure the Crime Scene and keep people away from the equipment and any power supply crime scene
Check if computer is switch on
No
Yes
Under no circumstances switch on the Computer
Is expert advice is available?
No
Yes
Don't touch the key
Don't take advice from owner
Take photograph and make note of what is on the
Allow the printer to complete
Remove the Power Cable from the equipment
Follow the advice (Collect volatile evidence and imagining)
Label and photograph or video the component in SOC
Remove all other connection cables leading to all sockets or other device
1. Carefully remove the equipment and pack it
2. Record all details on the search form
Ensure that all the components have proper
Search of SOC for diaries, note book or pieces of paper
Ask the user if there is any password and record it
Submit equipment for forensic examination
What should be seized?
1. For the retrieval of Evidence-
- Floppy, Disks, CD, DVD, DAT tapes, Jaz cartridge and Zip cartridge
- PCMCIA cards
- External/Removable Hard Disks
2. To assist with examination-
- Manuals and computer software
- Paper with password on key
3. For comparison of printouts-
- Printers
- Printouts
- Printer paper
4. For reconstruction of the system-
- Main CPU Unit- usually the box to which the keyboard monitor are attached
- Keyboard and mouse
- All leads (including power cable)
- Power supply units
- External Hard Disks
- Dongles
- Modems
Transportation
- Handle all equipment with utmost care.
- Keep all equipment away from magnetic sources such as loudspeakers, Heated seats/windows or police radios.
- Place hard disks and circuits board in a anti-static bags.
- Do not bend floppy disks.
- Place labels on them.
- Place keyboards, leads, mouse and modems in aerated bags.
- Do not place under heavy objects.

The Bharatiya Sakshya Adhiniyam, 2023

The Schedule

Certificate

Part A

(To be filled by the Party)

I, _____ (Name), Son/daughter/spouse of _____ residing/employed at _____ do hereby solemnly affirm and sincerely state and submit as follows:-

I have produced electronic record/output of the digital record taken from the following device/digital record source (tick mark):-

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____
Serial Number: _____
IMEI/UIN/UID/MAC/Cloud ID_____ (as applicable) and any other relevant information, if any, about the device/digital record____(specify). The digital device or the digital record source was under the lawful control for regularly creating, storing or processing information for the purposes of carrying out regular activities and during this period, the computer or the communication device was working properly and the relevant information was regularly fed into the computer during the ordinary course of business.

If the computer/digital device at any point of time was not working properly or out of operation, then it has not affected the electronic/digital record or its accuracy. The digital device or the source of the digital record is:-

Owned ☐ Maintained ☐ Managed ☐ Operated ☐
by me (select as applicable).

I state that the HASH value/s of the electronic/digital record/s is _____, obtained through the following algorithm:-

☐ SHA1:
☐ SHA256:
☐ MD5:
☐ Other_____ (Legally acceptable standard)
(Hash report to be enclosed with the certificate)

(Name and signature)

Date (DD/MM/YYYY): _____
Time (IST): _____hours (In 24 hours format)
Place: _____

Part B

(To be filled by the Expert)

I, _____ (Name), Son/daughter/spouse of _____ residing/employed at _____ do hereby solemnly affirm and sincerely state and submit as follows:-

The produced electronic record/output of the digital record are obtained from the following device/digital record source (tick mark):-

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____
Serial Number: _____
IMEI/UIN/UID/MAC/Cloud ID_____ (as applicable) and any other relevant information, if any, about the device/digital record_____(specify).

I state that the HASH value/s of the electronic/digital record/s is _____, obtained through the following algorithm:-

☐ SHA1:
☐ SHA256:
☐ MD5:
☐ Other_____ (Legally acceptable standard)
(Hash report to be enclosed with the certificate)

(Name, designation and signature)

Date (DD/MM/YYYY): _____
Time (IST): _____hours (In 24 hours format)
Place: _____

XYZ
Joint Secretary & Legislative Counsel to the Govt. of India

Section 63(2) of BSA says about following conditions:

- At the time of the creation of the electronic record, the computer that produced it must have been in regular use,
- The kind of information contained in the electronic record must have been regularly and ordinarily fed in to the computer,
- The computer was operating properly; and,
- The duplicate copy must be a reproduction of the original electronic record.

Procedures of storage, certification and transportation

- Procedure for issuance of Certificate of Part A of Section 63 (4)(c): -

a. In case of audio-video recording(s) done on a Mobile phone, the police officer/ operator, should apply hashing software through app/web-based tool on the mobile itself and generate the hash value, note it down and transfer the recording to the expert in the police station, on to the local designated desktop - via Cable or Bluetooth or other default file transfer methods. Police officer shall produce a Part-A certificate of section 63(4)(c) to the officer in charge of the police station/investigation unit as his part of execution is complete.

Cont.

b. If the police officer/ operator does not have the hashing tool or app or is not confident of hashing techniques, he/she can take the help of the designated expert of the police station. Mention this entire process in the chain of custody form along with the name of the hashing software used. Also, mention whether the hashing was done by the police officer/operator independently or with the help of an expert in his/her presence. It is also advisable to take screenshots of the hash value in order to avoid human errors.

Cont.

c. In case a digital camera/ recording device with a detachable memory card is used, the officer/operator shall hand over the standalone recording device/ camera's memory card to an expert in the headquarters/police station by placing the memory card in an evidence envelope with identifying case information and sealed. This sealed envelope will then be delivered to the expert.

Procedure for issuance of Certificate of Part B of Section 63 (4)(c)

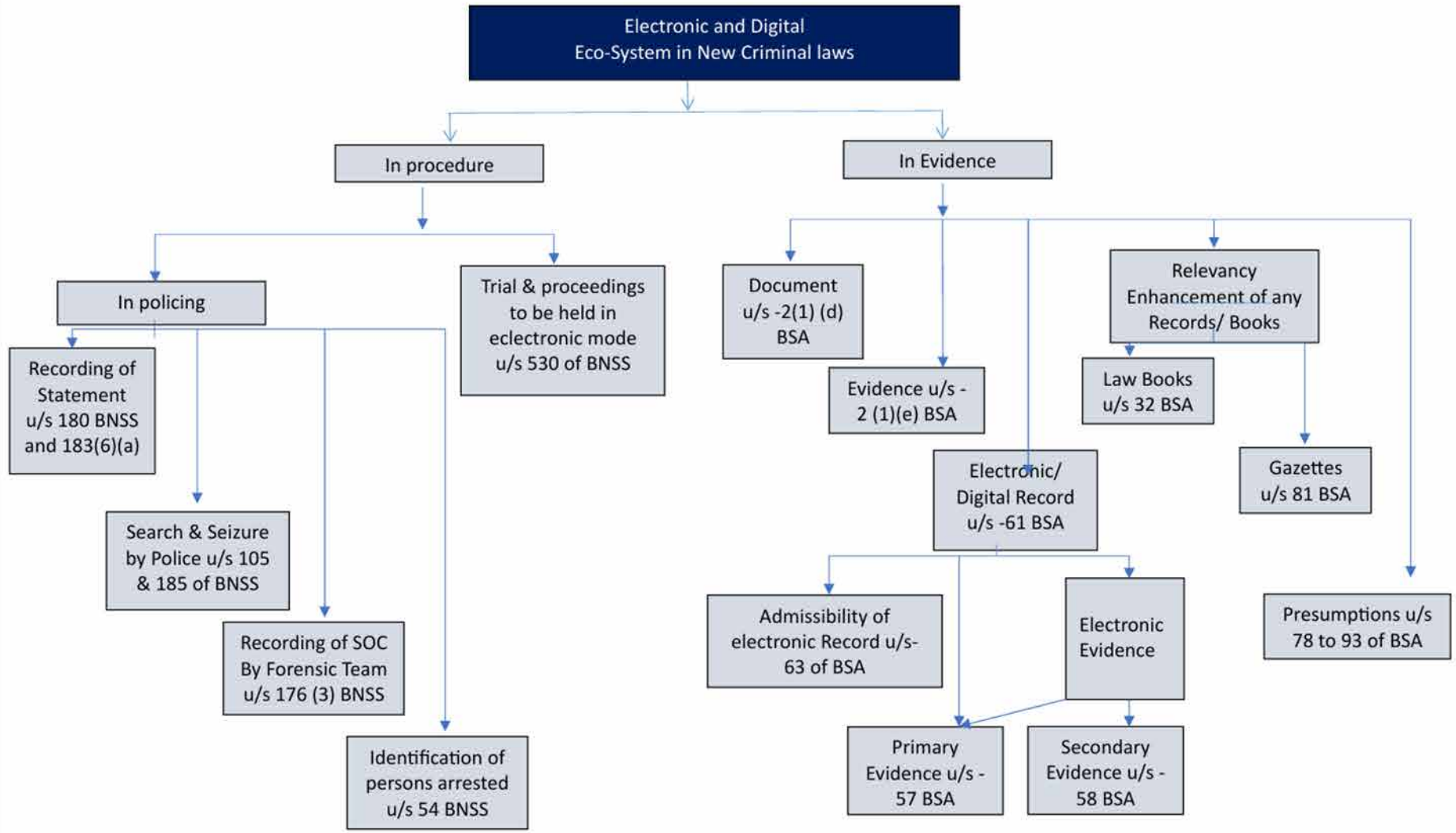
- The expert will now transfer the recording obtained from the first responder/ police officer to the designated computer/device. The digital audio-visual recording(s) transferred on the hard disc of the desktop will become the “master negative.” The master negative Hard Disk or storage device shall serve as the permanent record because it should not be altered once written/stored.
- Having copied the image, final hashing should be done at this stage. Transfers should be depicted in the chain of custody forms with the expert signing it duly.
- The files on the master negative hard disk or storage devices should be copied, without opening, onto another pen drive or storage device which becomes the ‘working record’, the “negative duplicate or mirror image.” This mirror image with both certificates A & B has to be supplied to the magistrate.
- Any enhancement of digital image files should be documented by the expert/evidence specialist and recorded on a separate pen drive or storage device.

Transport of audio-video recordings

- Section 105 BNSS mandates that the record of audio-video recording should be produced to the concerned court as soon as it is done.
- Transfers should be depicted in the chain of custody forms with the responder & evidence expert signing them duly.
- The expert, data manager, or designated officer at the Police Station will transfer the mirror images (preferably all recorded in the last 24 hours) in a secure storage device to the designated desktop of the Magistrate along with memos and chain of custody forms.

Important Apps

- E-Sakshya app: With this, investigating officers can record videos and take photographs of crime scenes as needed. These recordings and photographs can also be downloaded for use by prosecutors and defense advocates.
- Nyaya Setu: This will connect the Police, Medical, Forensic, Prosecution and Prison authorities. It will provide the police with all the information related to the investigation on a real-time basis.
- E-summon app: The Courts will electronically send summons to police stations and the concerned person to whom the summons is to be sent.
- Nyaya Shruti app: This will enable the Court to hear witnesses via Video conferencing


Electronic and Digital
Eco-System in New Criminal laws
In procedure
In Evidence
In policing
Trial & proceedings to be held in eclectronic mode u/s 530 of BNSS
Recording of Statement u/s 180 BNSS and 183(6)(a)
Search & Seizure by Police u/s 105 & 185 of BNSS
Recording of SOC By Forensic Team u/s 176 (3) BNSS
Identification of persons arrested u/s 54 BNSS
Document u/s -2(1) (d) BSA
Evidence u/s - 2 (1)(e) BSA
Relevancy Enhancement of any Records/ Books
Law Books u/s 32 BSA
Gazettes u/s 81 BSA
Electronic/ Digital Record u/s -61 BSA
Admissibility of electronic Record u/s- 63 of BSA
Electronic Evidence
Presumptions u/s 78 to 93 of BSA
Primary Evidence u/s - 57 BSA
Secondary Evidence u/s - 58 BSA

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____

Submitting Officer: (Name/ID#) _____

Victim: _____

Suspect: _____

Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Locati**

Final Disposal Authority

Authorization for Disposal

Item(s) #: _____ on this document pertaining to (suspect): _____
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

☐ Return to Owner ☐ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: _____ Signature: _____ Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ ID#:_____
in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____ Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian _____ ID#:_____ to
Name _____
Address: _____ City: _____ State: _____ Zip Code: _____
Telephone Number: (_____) _____
Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: _____ Date: _____

Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

Challenges

- Authentication & Tampering
- Issues with issuing Certificate
- Privacy & Data Protection
- Lack of awareness & technical, legal experts
- Jurisdictional problems relating to Cyber evidence

Thank you!