गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

सत्यमेव जयते

Standard Operating Procedure (SOP) for Audio - Visual Recording of Scene of Crime

Bureau of Police Research & Development

Ministry of Home Affairs

Government of India

NH-48, Mahipalpur, New Delhi - 37

PREFACE

With an eye on transparency and ease of justice, the use of technology is encompassed in New Criminal Laws through a transparent approach in streamlining evidence collection, redefining secondary evidence and improving admissibility of electronic Records thus making technology pervasive in New Criminal Laws. Use of Technology is now envisaged in all stages (from e - FIR to investigation to submission of documents to trials). Further, Compulsory Forensic examination in all cases where offence attracts punishment of seven or more years has been envisaged.

This SOP have been prepared by elaborate brainstorming with field practitioners as to fulfil their immediate felt need of handholding document. This SOP is a guideline for the functional and operational part of crime scene photography and videography to ensure the admissibility of the same in the court of law. The technical aspect including photographs taken by forensic experts, contents and analysis is only basic and not dealt with in great detail.

The stakeholders' initial documents on these topics produced by Delhi Police, Chandigarh Police and UP Police have been found to be useful in creating this document and credit is duly acknowledged.

Also since practice of new laws and inherent tendency of technology to upgrade very quickly, will throw new dimensions on understanding of the implementation of new laws, feedback is solicited which will be handy to upgrade these SOPs if required in the near future.

This SOP is a suggested guidelines which is being shared for use of police and enforcement units in states and central organizations, but the states and central police organisations can build upon this basic structure depending upon their peculiar needs and needs of special acts hinging on these procedural laws.

INDEX

	Subject	Page no.
	PART A **Commentary on Technology Ecosystem for Quality of Evidence**	5-24
1.	**INTRODUCTION OF THE NEW CRIMINAL LAWS**	6
2.	**OBJECTIVE:** • Fair and Speedy Justice • Ease of Justice	
3.	**TECHNOLOGY ECOSYSTEM:** • Electronic and Digital Eco-System in New Criminal Laws	7-9
4.	**TECHNOLOGY ECOSYSTEM- DETAILED DISCUSSION** • Revolutionizing Evidence Presentation: A Transparent Approach • Streamlining Secondary Evidence: A Futuristic Approach • Admissibility of Electronic Records (Sections 57 and 63 BSA)	10-24
	PART B **SOP: Audio Visual Recording of SOC**	25-75
A.	**Policy, Principles & Procedures of executing SOP:** • Policy • Principles • Basic Premise of Preparation & Photo / Videography • Methods for searching crime scenes	27-57

	• Basics of Photography & Videography • Overall Photography & Videography • Mid-Range photography & Videography • General Procedure to conduct search and seizure • Procedure for processing Scene of Crime • Videography Proper During Search Seizure • Specific Technology Procedures of Recording • Technological Procedures of Storage & Transportation • DO's & Don'ts by IOs for Recording Photographic & Video Evidences • Procedure of Audio/Videography of SOC in investigative Tree • Procedure of Audio / Videography of SOC along with Seizure of Digital Evidence	
B.	DOCUMENTATION • Drawing of Seizure Memo • Documentation & Follow up at police Station • Chain of Custody	58-61
C.	COST ESTIMATION • Costing & Budgeting	62
D.	PROPOSED APP BASED SOLUTIONS: E-SAKSHYA AND OTHERS	63-67
E.	AIDE-MEMOIR	68-69
F.	ANNEXURES	70-75

PART -A

Commentary on Technology Ecosystem of Quality of Evidence

COMMENTARY ON NEW CRIMINAL LAWS w.r.t. TECHNOLOGY ECOSYSTEM FOR QUALITY OF EVIDENCE

1. INTRODUCTION OF THE NEW CRIMINAL LAWS

- In December 2023, the Parliament of India passed three new criminal laws to replace and overhaul the existing criminal justice system in India.

- The three criminal laws will provide enhanced protection for the poor, marginalized, and vulnerable while also cracking down on organized crime, terrorism, and other offences.

2. OBJECTIVE

- **Fair and Speedy Justice**

  –To ensure speedy justice in a time-bound manner, evidence-based speedy trial and fair trial, which will reduce the burden on courts and jails?

  –To use forensic science in the scientific evidence collection from crime scenes and use of technology in the criminal justice system.

  –To increase the rate of punishment and to prevent cybercrimes.

- **Ease of Justice**

  To aid ease of Justice through simple, consistent, transparent, and accountable criminal justice procedures.

3. TECHNOLOGY ECOSYSTEM

Use of Technology is now envisaged in all stages of New Criminal Laws (from e - FIR to investigation to submission of documents to trials). Further, forensic experts have been mandated to visit the crime scene to collect forensic evidence in all cases where offence attracts punishment of seven or more years. It has been provided that in offences prescribing imprisonment for 7 years or more, police officer shall cause forensics expert to visit the crime scene to collect forensic evidence. States may from such date, as may be notified by them, as early as possible but not later than 5 years, shall make it compulsory.

Some of the highlights are as under:

a) A new definition of electronic communication 'for use of technology in investigation, trial and court proceedings and service of summons, notices, etc. has been introduced.

b) The definition of 'Documents' has been expanded to include an electronic or digital record on emails, server logs, documents on computers, laptop or smartphone, messages, websites, cloud locational evidence and voice mail messages stored on digital devices.

c) The definition of 'evidence' has been expanded to any information given electronically. This will permit appearance of witnesses, accused, experts and victims through electronic means. This will ease the process of trial, prevent delays in transporting accused from prisons to courts, and also help in preserving the trial process for future reference that may be necessitated during challenge in higher courts.

d) In the definition of primary document (Section; 57, BSA), new explanations (now total 7) have been added to cover the following:

   (i). Where an electronic or digital record which is created or stored, and if such storage occurs simultaneously or sequentially in multiple files, each such file is primary evidence.

   (ii). Where an electronic or digital record is produced from proper custody, it is sufficient to prove its contents unless it is disputed.

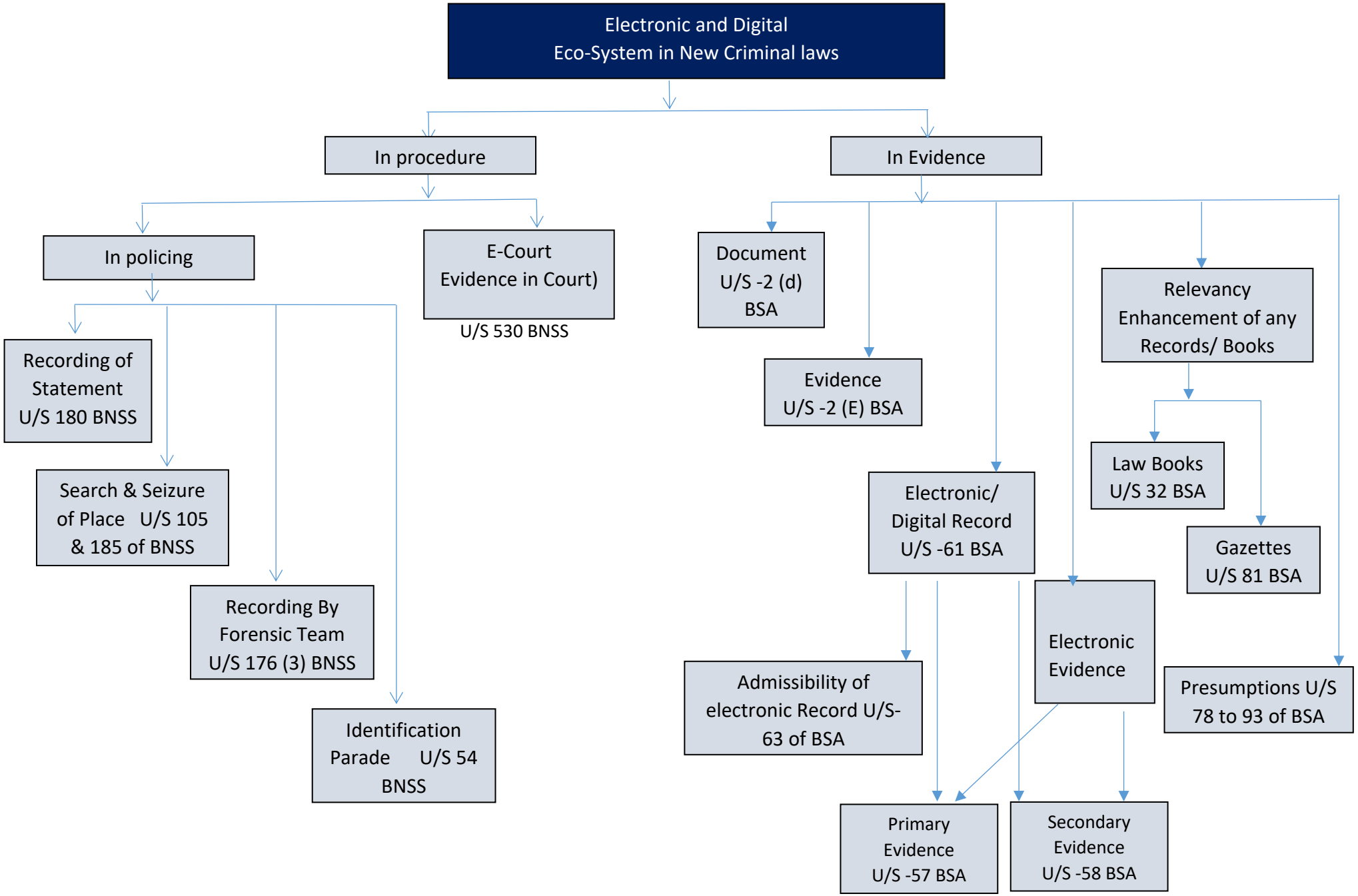
(iii) Where a video recording is simultaneously stored in electronic form and transmitted or broadcast to another, each of the stored recordings is primary evidence.

(iv) Where an electronic or digital record is stored in multiple in storage spaces computer resource, each such automated storage, including temporary files, is an primary evidence.

e) Scope of secondary evidence has been expanded. Now in addition to certified copies, copies made from original by mechanical processes, copies made from or compared with the original, counterparts of documents as against the parties who did not execute them and oral accounts of the contents of a document given by some person who has himself seen it, are included.

f) It has been permitted that accused (in custody) may be examined by a Magistrate through electronic means i.e. Video Conferencing/ VC facility available in the police station, court, prison or any other such place notified by the State Government. It has been provided that if the accused has been examined through VC, his signature on the statement shall be taken within 72 hours.

g) A provision has been made wherein the Magistrate may order specimen or sample without the person being arrested. Further there is no existing provision in CrPC for taking finger impression or voice sample which has been provided for in BNSS.


Electronic and Digital
Eco-System in New Criminal laws
In procedure
In Evidence
In policing
E-Court
Evidence in Court)
U/S 530 BNSS
Recording of
Statement
U/S 180 BNSS
Search & Seizure
of Place U/S 105
& 185 of BNSS
Recording By
Forensic Team
U/S 176 (3) BNSS
Identification
Parade U/S 54
BNSS
Document
U/S -2 (d)
BSA
Evidence
U/S -2 (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
Electronic
Evidence
Presumptions U/S
78 to 93 of BSA
Admissibility of
electronic Record U/S-
63 of BSA
Primary
Evidence
U/S -57 BSA
Secondary
Evidence
U/S -58 BSA

4. TECHNOLOGY ECOSYSTEM- DETAILED DISCUSSION

a). Revolutionizing Evidence Presentation: A Transparent Approach

Audio Video Recording of SOC

One of the Major change introduced in new criminal Laws is "recording of Crime Scene through any audio-video electronic means preferably mobile phone" The use of videography in crime scene investigation is a significant step towards improving the quality of evidence and strengthening the criminal justice system. By capturing the crime scene in a credible manner, it can help overcome issues of contradictory witness testimonies and allegations of tampering. The courts have rightly emphasized the need to adopt new technologies, while ensuring adequate safeguards. However, the effective implementation of this directive requires proper training, resources, and coordination among the investigating agencies.

1. Considering the risk of manipulation of evidence, the mandatory inclusion of audio-video recording in search and seizure proceedings is an important inclusion in BNSS. In BNSS Section.105*, the scope of audio - video recording during search and seizure includes, among others, the process of preparing a list of seized items and the signature of witnesses. Transparency in search and seizure proceedings is likely to deter against fabrication of evidence and ensure the presence of independent witnesses in these proceedings.

2. Section.105 requires that this audio video recording be submitted before the District Magistrate, Sub - divisional Magistrate or Judicial Magistrate of first class 'without delay'.

3. In BNSS Section.176(3)*, the requirement for videography of the process of collection of forensic evidence is another move towards greater transparency and accountability in evidence gathering, and a safeguard against irregularities and manipulation.

4. Audio - video recordings have the potential to strengthen the quality of evidence and steps have to be taken to prevent its alteration, modification and transposition, through direct intervention or unintended corruption of a digital record. Appropriate guidelines will have to be formulated for adopting procedures to maintain authenticity and accuracy of electronic evidence.

Recording Of Statements:

Section. 176 (1) provides an option of audio - video recording of any statement made during police investigation. The scope of this proviso is wide enough to include disclosure statements of accused before the police, besides the statements of other witnesses (audio - video recording for which is already permitted under s.161 CrPC, retained in Section.180 BNSS.) This is an important safeguard to deter against torture and coercion of the accused during custodial interrogations.

The investigating officer may also record the statement of such witnesses by audio-video electronic means as he deems fit in the interest of the investigation. The audio-video clips will be part of the case diary.

In all cases punishable under sections 64 to 71, sections 74 to 79 and section 129 of the BNS, 2023, the investigating officer will get the statement of the victim recorded by a Magistrate authorized under section 183 of the BNSS, 2023, as far as practicable, by a woman Magistrate and in her absence by a male Magistrate in the presence of a woman.

In all offences punishable with imprisonment for ten years or more or with imprisonment for life or with death, the investigating officer will preferably get the statement of the relevant and important witnesses recorded by the authorized Magistrate. Where the person making the statement is temporarily or permanently, mentally of physically disabled, the Magistrate will take assistance of an interpreter or a special educator in recording the statement. The statement will also be recorded through audio-video electronic means, preferably mobile phone. The recorded statements will be entered in the case diary by the investigating officer.

Consistent with the CrPC, the BNSS retains the mandatory requirement for videography of police statements, and audio - video recording of statements before the Magistrate for certain vulnerable

victims with physical or mental disabilities, under Cls.173 (1) and 183 (6), respectively.

Sec. 230 of BNSS requires the accused and victim (if represented by a lawyer) to be supplied with the police report and all necessary documents, including statements and confessions.

Forensic Expert at Scene of Crime-BNSS

- BNSS Sec. 176 (3) On receipt of every information relating to the commission of an offence which is made punishable for seven years or more, the officer in charge of a police station shall, from such date, as may be notified within a period of five years by the State Government in this regard, cause the forensic expert to visit the crime scene to collect forensic evidence in the offence and also cause videography of the process on mobile phone or any other electronic device:
- Provided that where forensic facility is not available in respect of any such offence, the State Government shall, until the facility in respect of that matter is developed or made in the State, notify the utilization of such facility of any other State.

Report of police officer on completion of investigation- Chain of custody

- Sec 193 (3) (i) As soon as the investigation is completed, the officer in charge of the police station shall forward, including through electronic communication to a Magistrate empowered to take cognizance of the offence on a police report, a report in the form as the State Government may, by rules provide, stating –

  (a) the names of the parties, (b) the nature of the information; (c) the names of the persons who appear to be acquainted with the circumstances of the case; (d) whether any offence appears to have been committed and, if so, by whom; (e) whether the accused has been arrested; (f) whether the accused has been released on his bond or bail bond; (g) whether the accused has been forwarded in custody under section 190; (h) whether the report of medical examination of the woman has been attached

- where investigation relates to an offence under sections 64, 65, 66, 67, 68, 70 or section 71 of the BNS, 2023;

(i) the sequence of custody in case of electronic device

(ii) the police officer shall, within a period of ninety days, inform the progress of the investigation by any means including through electronic communication to the informant or the victim

Supply of report and other documents by electronic communication shall be considered as duly served

SUMMARY OF VIDEOGRAPHY PROVISIONS IN NEW LAWS				
#	**Particulars**	**Relevant Legal Provision**	**Legal Mandate**	**Place of Recording or capturing**
1.	Videography recording of scene of crime	**BNSS Sec 176 Procedure for investigation** .. (3) On receipt of every information relating to the commission of an offence which is made **punishable for seven years or more**, the officer in charge of a police station **shall**, from such date, as may be notified within a period of five years by the State Government in this regard, cause the forensics expert to visit the crimes scene to collect forensic evidence in the offence and **also cause videography of the process on mobile phone or any other electronic device.**	Mandatory	Crime Scene
2.	Recording of Search and Seizure	**BNSS Sec 105- Recording of search and seizure through audio-** **Video electronic means.** The process of conducting search of a place or taking possession of any property, article or thing under this Chapter or under section 185, including preparation of	Mandatory	Place of search from where recovery in made

		the list of all things seized in the course of such search and seizure and signing of such list by witnesses, **shall be recorded through any audio-video electronic** means preferably mobile phone and the police officer shall without delay forward such recording to the District Magistrate, Sub-divisional Magistrate or Judicial Magistrate of the first class. **BNSS Sec 85- Search by Police**. ... Provided that the search conducted under this section **shall be recorded through audio-video electronic means preferably by mobile phone**. (*Chapter-Proclamation and attachment*) **BNSS Sec 185- Search by Police officer**. ..2) A police officer proceeding under sub-section (1), shall, if practicable, conduct the search in person: Provided that the search conducted under this section shall be recorded through audio-video electronic means preferably by mobile phone.		
3.	Information cognizable cases-FIR For sexual offences where victim is mentally or physically disabled	**BNSS Sec 173- Information in cognizable cases. .. Provided further that-** (a) in the event that the person against whom an offence under section 64, section 65, section 66, section 67, section 68, section 69, section 70.	Mandatory	Residence of victim/any place

		Section 71. section 74, section 75, section 76, section 77, section 78, section 79 or section 124 of the BNS, 2023 is alleged to have been committed or attempted, is temporarily or permanently mentally or physically disabled, then such information shall be recorded by a police officer, at the residence of the person seeking to report such offence or at a convenient place of such person's choice, in the presence of an interpreter or a special educator, as the case may be; **b) the recording of such information shall be video graphed.**		
4.	Recording of statement by police for offence of Rape	**BNSS Sec 176- Procedure for investigation….** Provided further that in relation to an offence of rape, the recording of statement of the victim shall be conducted at the residence of the victim or in the place of her choice and as far as practicable by a woman police officer in the presence of her parents or guardian or near relatives or social worker of the locality and such statement **may also be recorded through any audio-video electronic means including mobile phone.**	Optional	Residence of victim/any place of choice of victim
5.	Examination of witness by police	**BNSS See 180- Examination of witnesses by police.** …(3) The police officer may reduce into writing any statement made to him in the course of an examination under this	Optional	Police station or any other place

		section; and if he does so, he shall make a separate and true record of the statement of each such person whose statement he records: Provided that statement made under this sub-section **may also be recorded by audio-video electronic means:**		
6.	Orders for custody and disposal of property	**BNSS Sec 497-Order for custody and disposal of property** **Pending trial in certain cases.** ...(3) The Court or the Magistrate shall cause to be taken the photograph and if necessary, videograph on mobile phone or any electronic media, of the property referred to in sub-section (1).	**Photograph mandatory** Videography optional	Any place

b). Streamlining Secondary Evidence: A Futuristic Approach

The scope of secondary evidence broadens under BSA 2023, incorporating copies made through mechanical processes.

Two new forms introduced in the schedule expedite the authentication and appreciation of digital evidence, addressing challenges under previous statutes.

The most significant change in BSA is the introduction of evidentiary nature and admissibility of electronic evidence. The proposed changes include expansion of the definition of primary evidence to include copies of electronic or digital files.

- Scope of secondary evidence has been expanded in section 58. Secondary evidence now also includes - oral admissions, written admissions, and evidence provided by a person who is skilled in examining certain documents, which being technical or voluminous cannot be conveniently examined.

- Section 61 brings parity in the admissibility of electronic/digital record and other documents. Now, electronic or digital records will have the same legal effect, validity and enforceability as other documents.
- Section 62 & 63 of the BSA provide a comprehensive framework for the admissibility of electronic records as evidence. This section outlines the requirements for submitting a certificate for establishing the authenticity of an electronic record. Such a certificate is to be signed by the person in charge of the computer or communication device. Furthermore, a separate certificate provided in the schedule to BSA mandates the signature of an expert, whose endorsement serves as proof for any statements contained within the certificate. Once signed, the certificate serves as evidentiary support for the matters it asserts.

c). Admissibility of Electronic Records (Sections 57 and 63 BSA)

Similar to s.65B IEA, Cl.63 BSA provides a specific procedure for the admissibility of electronic records. Cl.2 (d) BSA which replaces s.3 IEA, defines documents to also include 'electronic or digital records'.

Cl.62 BSA, which replaces s.65A IEA, states that electronic records must be proved as primary evidence, unless mentioned. Newly introduced Cl.61 BSA, prescribes that the admissibility of electronic records cannot be denied on the basis of their nature as electronic records and their legal effect, validity and enforceability shall be at par with paper records. This will bring in a much - required change in the Evidence Law by treating electronic evidence as good as the physical evidences currently being dealt by courts.

Obviously, proper safeguards have to be built so that the legal sanctity of electronic evidence is maintained. Attention may also be provided towards building institutional and infrastructural capacity for its effective and mandatory implementation. This will include strengthening infrastructural facilities across States/UTs, providing the necessary gadgets collection - transmission - storage of electronic evidence, training of manpower in this regard, etc.

Guidelines will have to be framed by respective States / UTs to ensure high standard for the quality of the equipment, as well as to establish systems and infrastructure regarding the safe and secure

storage and transfer of electronic evidence, besides ensuring that it is protected from being leaked, deleted or corrupted.

- **BSA Sec 63 (4). (Section 65-B OF IEA)**

(4) In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things **shall be*** submitted along with the electronic record **at each instance where it is being submitted*** for admission, namely:

(a) Identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) Giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer or a communication device referred to in clauses (a) to (e) of sub-section (3);

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) **and an expert*** shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule. **(*-New additions)**

For Legal Commentary & case laws of Supreme Court High Courts regarding Admissibility of electronic evidence Click Here :

Or copy the link for assessing the document:

https://drive.google.com/file/d/1Tepq6I11PaYm5yrnDWwabupBpM22s6GG/view?usp=share_link

Note on CERTIFICATION of Audio - Video content as to satisfy the mandatory provisions of BSA:

There are two categories of evidences which require certification by experts.

- **First category:** Digital recordings after implementation of new laws:
  - Audio video recording of statements of victim and witnesses, u/s 180 BNSS (Preferable)
  - Audio video recording of search and seizure. (Mandatory)
  - Audio video recording of other procedural compliances like identification parade, property disposal.(Preferable)
- **Second category**: Various digital devices are routinely seized during course of investigations like mobile, social media accounts, emails, computers, CCTV cameras and so on.

Now in departure of earlier 65-B the new section 63(4) introduces two new underpinnings viz. "a certificate **shall be** submitted along with the electronic record **at each instance** where it is being submitted" for (a) Identifying the electronic record containing the statement and describing the manner in which it was produced; and (b) Giving such particulars of any device involved in the production of that electronic record

Hence now each audio-video recording as part of procedural compliance and investigative compliance and each seizure of relevant digital evidence requires certification, doubly by the handler (or manager) and by an expert.

The clarity on certificate providers is as such:

1. **Owner/Handler or Operator/ First responder/ Manager:**

According to 63(4) (c)BSA: *"and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate)"*

The Part (A) of the format of certificate – **'to be given by party'** - as specified by BSA explicitly refers to certificate giver of this part to be the owner/ handler or operator/first responder/manager. In videography and photography done by first responders (police team), the videography may have been done by constable and certificate can be given by head- constable of the same first responder team which routinely manages the audio-video recording of polices station or can even be given by records head-mohrir of police station under whom the record is downloaded and archived. But the chain of custody form should clearly mention the change of hands and reasons there-of.

Similarly the case for the seizure of digital evidence, **'the party'** or giver of certificate of Part -A of 63(4)(c) would be the owner/operator/handler or manager or person in-charge of communication /computer device in contention.

2. **Expert:**

As per section 63(4) of BSA:

*"an expert **shall be evidence of any matter** stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule".*

Certificate of Part -B of 63(4) (c) **can be signed by a person occupying responsible official position and evidence to the chain of events and stated to the best of his knowledge and belief**. For example SHO of police station who was evidence to the chain of events is best to ascertain the authenticity on his knowledge and belief. If first responder recorded the video, the forensic team in-charge can also be made to give part B certificate.

Certificate must relate to

- Identification of record, the manner in which it was produced
- Particulars of device

The above expert **should not be confused with** 'expert' defined in Sec **39 (2) BSA** which states that **'When in a proceeding'**, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion ofthe Examiner of Electronic Evidence referred to in

section **79A of the Information Technology Act, 2000**, is a relevant fact.

Explanation. —For the purposes of this sub-section, an Examiner of Electronic Evidence shall be an expert.

So, the first responder/ SHO can submit the record of Audio-video documentation in mirror copy along with chain of custody of primary evidence giving proper certifications as mandated in BSA along with them. The expert in this case could be responsible officer of sufficient seniority who is either himself evidence of the whole process or who can state to the best of his knowledge and belief that affirmation of the handler as to continuity & authenticity of it. The burden of proof in case of contention will be on defense to mount a challenge and prove the violation of authenticity and the at that time, court can seek opinion ofthe Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000 and check all the hashing and chain of custody provided by responder.

3. **Digital Forensic Experts – where from?**

It is pertinent here to examine **section 329 BNSS** which is captioned as – "**Reports of certain Government scientific experts.**"

Section 329 (1) of BNSS states that – "Any document purporting to be a report under the hand of a Government scientific expert to whom this section applies, upon any matter or thing duly submitted to him for examination or analysis and report in the course of any proceeding under this Sanhita, may be used as evidence in any inquiry, trial or other proceeding under this Sanhita."

Section 329 (4) (g) of BNSS states that - "This section applies to the following Government scientific experts, …(g) **any other scientific expert specified or certified, by notification, by the State Government or the Central Government for this purpose.**"

This section is a empowering provision for solving much of the problem in the context of experts.

Since the volume of certification shall increase and IOs/SHO's are also engaged in law and order duties, States may, using above stated enabling provisions of BNSS, design norms of cadre of digital forensic experts, for the purpose of compliance of certification of Part-B of 63(4)(c) and court proceedings thereafter, who can be of sufficient experience and responsibility and be made to experience these events of digital evidencing, as part of definition of expert, by making them

station at police stations if they are on lien from other technical departments.

The State Governments can notify the training and certification course which the police officers have to undergo in order to be qualified as a forensic expert for the purposes of section 176(3) of BNSS. All scientific officers trained in forensic evidence collection will be treated as forensic experts for the purposes of section 176(3) of BNSS. They can subsequently, if deemed fit, come up with a standardized exam for these Digital Forensic Experts. Whoever clears this exam will be notified as "Expert".

Alternatively, under MHA, the task to assess through a certification exam post basic/primer training of selected digital experts can be undertaken by joint certification by BPRD-NLU or BPRD-NFSU curated certification course on the lines of audit certifications.

These Digital experts should be then equipped with standardized hardware and software. They will seize the digital data and give certificates as an expert. They can handle and seize the digital data in prescribed form. They can also be tasked to do preliminary processing like creating image of digital device and provide it to the IO for investigation purpose. They can also assist IO in cases where digital data analysis is important.

The above mechanism will get operational in parts or whole of any state as notified by the State Government, but not later than 30.6.2029.

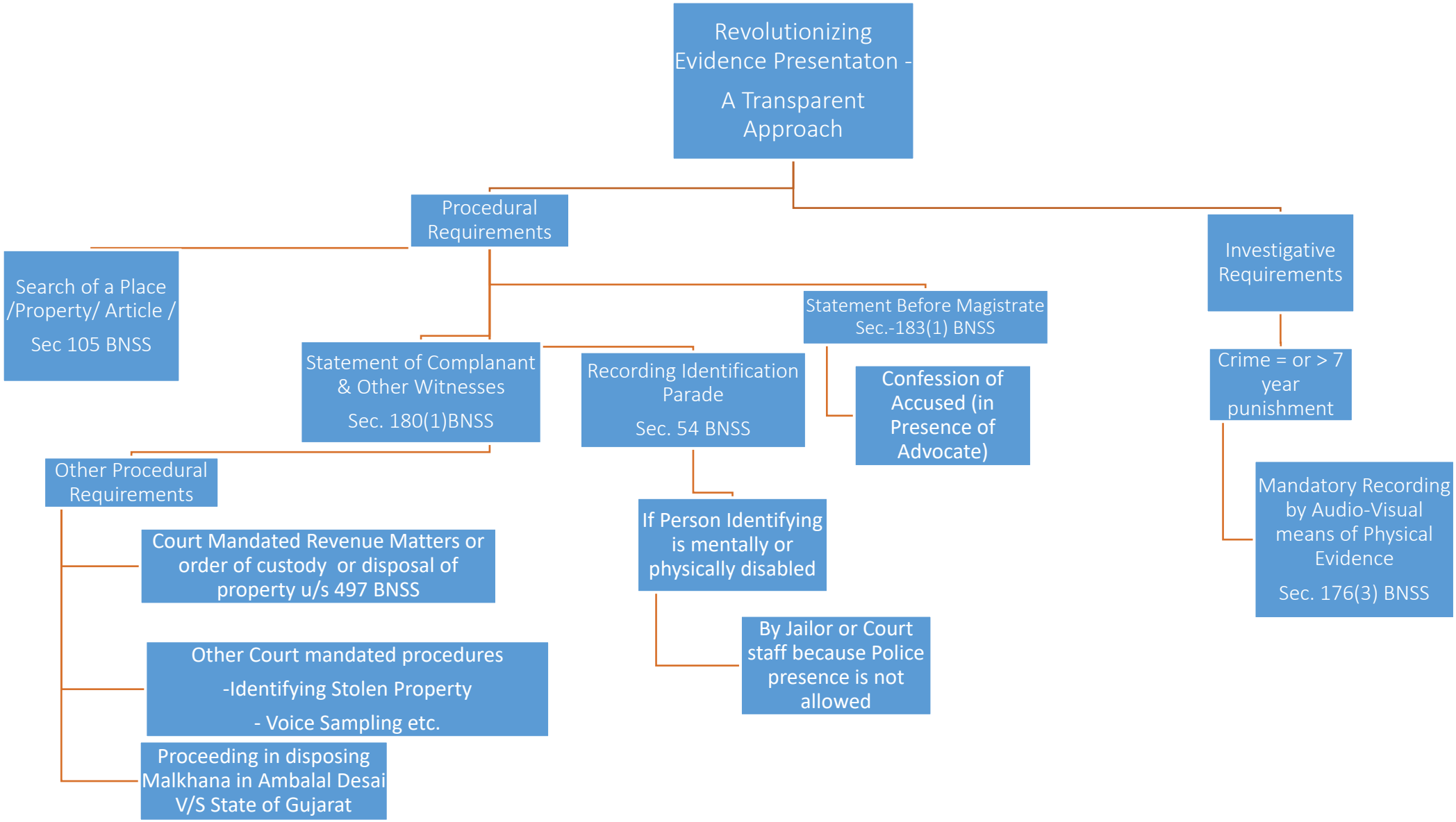
4. Future of evidence generation:

Since the overall demand of experts is very high for practical implementation there will always be gaps, NIC is coming up with standard software and standard process to capture audio/video and generate hash report with time stamp (e-Sakshya) This application will have inbuilt system for generating certificate in the prescribed format. Block chain technology is being used to ensure data integrity and trustworthiness. MEITY may issue a notification that photo/video captured through this standardized software/application may not require external certification and system generated report will be

sufficient for the purpose of 63(4) BSA. In this regard, the **e-sakshya** can rather being standalone application, can in future, be dovetailed in already existing portals of National Cyber Forensic Laboratory (NCFL) of I4C or CCTNS.

.

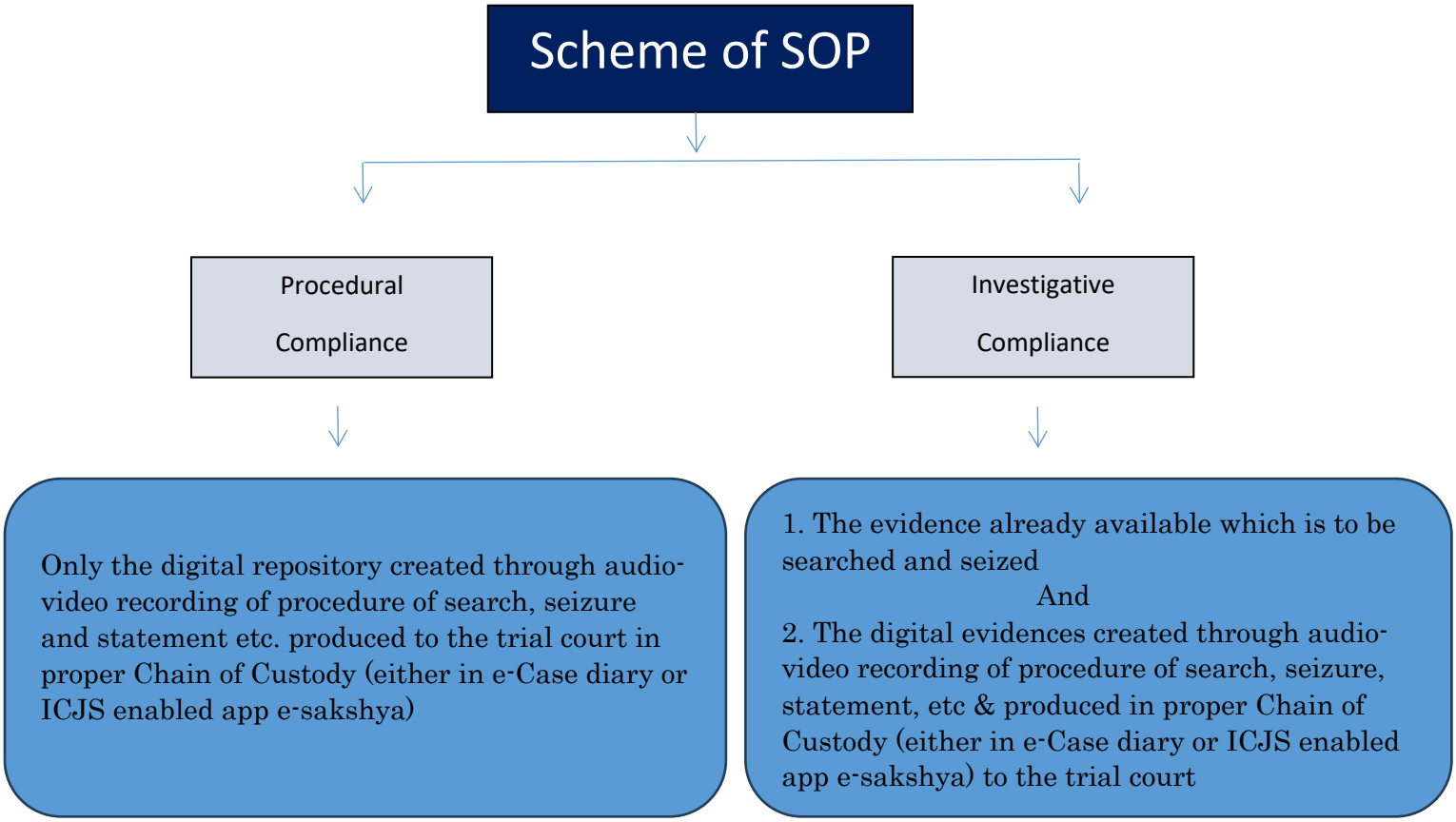
****


Revolutionizing Evidence Presentaton -
A Transparent Approach
Procedural Requirements
Investigative Requirements
Search of a Place /Property/ Article /
Sec 105 BNSS
Statement of Complanant & Other Witnesses
Sec. 180(1)BNSS
Recording Identification Parade
Sec. 54 BNSS
Statement Before Magistrate Sec.-183(1) BNSS
Confession of Accused (in Presence of Advocate)
Crime = or > 7 year punishment
Mandatory Recording by Audio-Visual means of Physical Evidence
Sec. 176(3) BNSS
Other Procedural Requirements
Court Mandated Revenue Matters or order of custody or disposal of property u/s 497 BNSS
Other Court mandated procedures
-Identifying Stolen Property
- Voice Sampling etc.
Proceeding in disposing Malkhana in Ambalal Desai V/S State of Gujarat
If Person Identifying is mentally or physically disabled
By Jailor or Court staff because Police presence is not allowed

PART - B

SOP: Audio Video Recording of SOC

The Standard Operating Procedure (SOP) consist of two parts, first pertaining to general procedures of Videography in Police Procedures: and the second relating to Standing Operating Procedure for Videography in investigative compliance & seizure of electronic and digital devices found as part of investigation.



A. Policy, Principles & Procedures of executing SOP

POLICY:

The photographs and video-graphs are universally accepted best practices and was essential for the appreciation of the scene of crime and evidence by the Hon'ble trial court. It is accepted that there is limited strength of forensic science experts in the districts, they are stationed at the district headquarters and hence they are unable to reach all scenes of crime and even if they reach the scene of crime the delay causes disturbance of scene of crime. Therefore, the scene of crime via videography and photography for appreciation by the trail court, preferably, should be done by the first responder itself. Specific and expert photography for better erudition of the evidence should be done by the forensic science experts who have to undergo a distinct training. In some scenarios the forensic experts can conduct and document all videography if in interest of investigation considering qualitative cost benefit analysis.

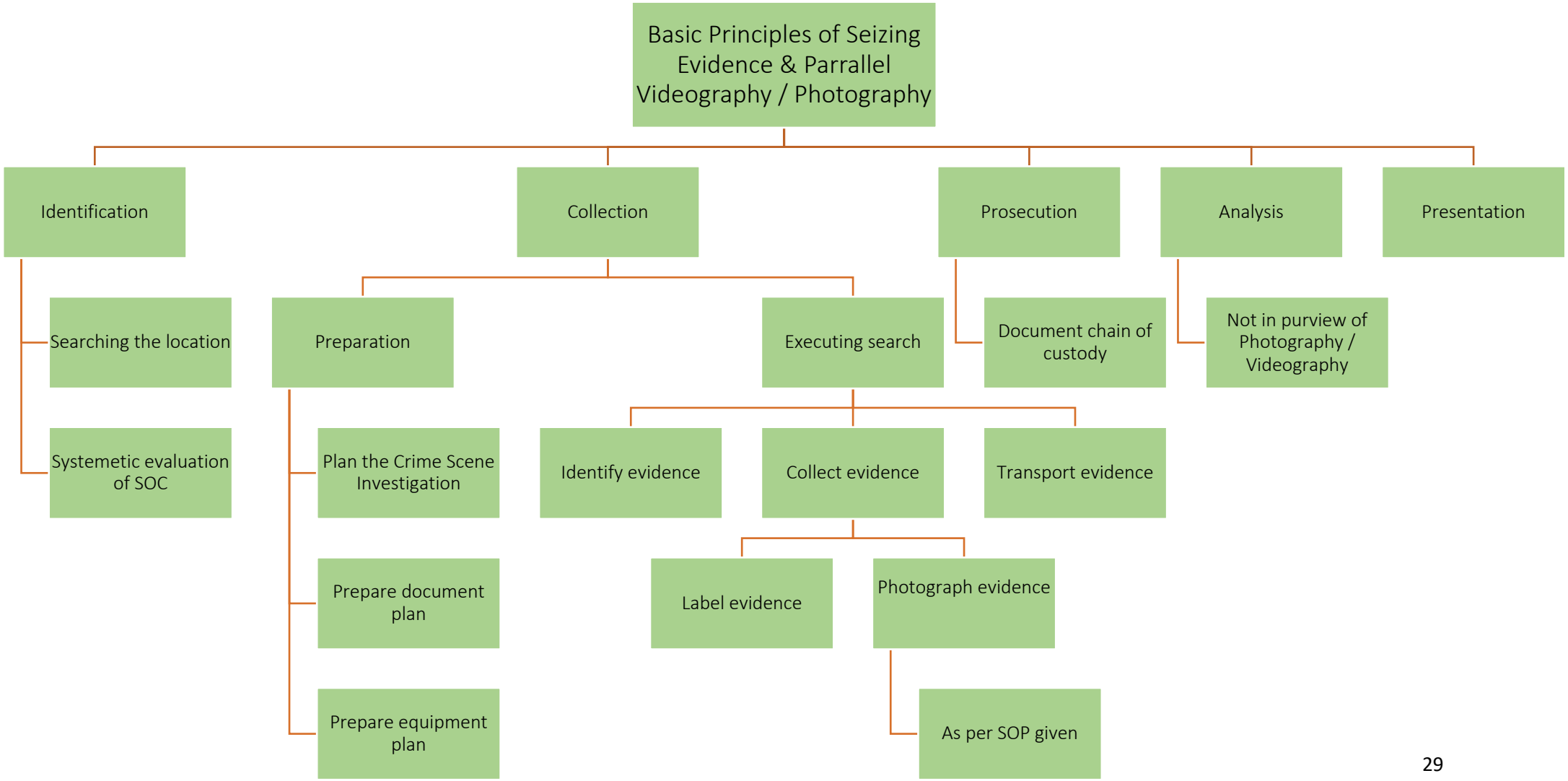
Police IOs are the first responders in any crime scenario. They must have access to simple technology along with appropriate training to inspire confidence in them to preserve and record the scene of crime authentically and faithfully. Once this initial important response is ensured, the detailed videography / photography may be ensured, if required, by the specialized forensic evidence collection teams. The availability of simple instructions for videography/ photography ensures the appropriate immediate response of the I0 and appreciation and collection of evidence.

PRINCIPLES:

The state units & central police organisations will strengthen the overall ecosystem of evidence collection via audio-video recording by adhering to broad principles outlined below:

- Securing the scene of crime & preparation of recording evidence
- Use of Smartphones until specialized cameras/audio video devices are selected for capturing evidence.
- Securing and storage of data/ evidence
- Quality and resolution of the data/ evidence for appropriate forensic analysis
- Secure portals for transferring the evidence for storage (and till that time that this is in place, adequate hardware requirements of investigative units)
- Storing the evidence as permanent record in order to ensure authenticity and prevent manipulation.
- Production and admissibility of evidence
- Funding the endeavour for hardware & software on a sustained basis forensic facilities,

BASIC PREMISE OF PREPERATION & PHOTO/ VIDEOGRAPHY



Methods for searching crime scenes:

- The investigating officer must adopt an orderly process to access the crime scene so that any material evidence is not left out. Any one of the following crime scene search patterns may be adopted as per need (Figure 1).:

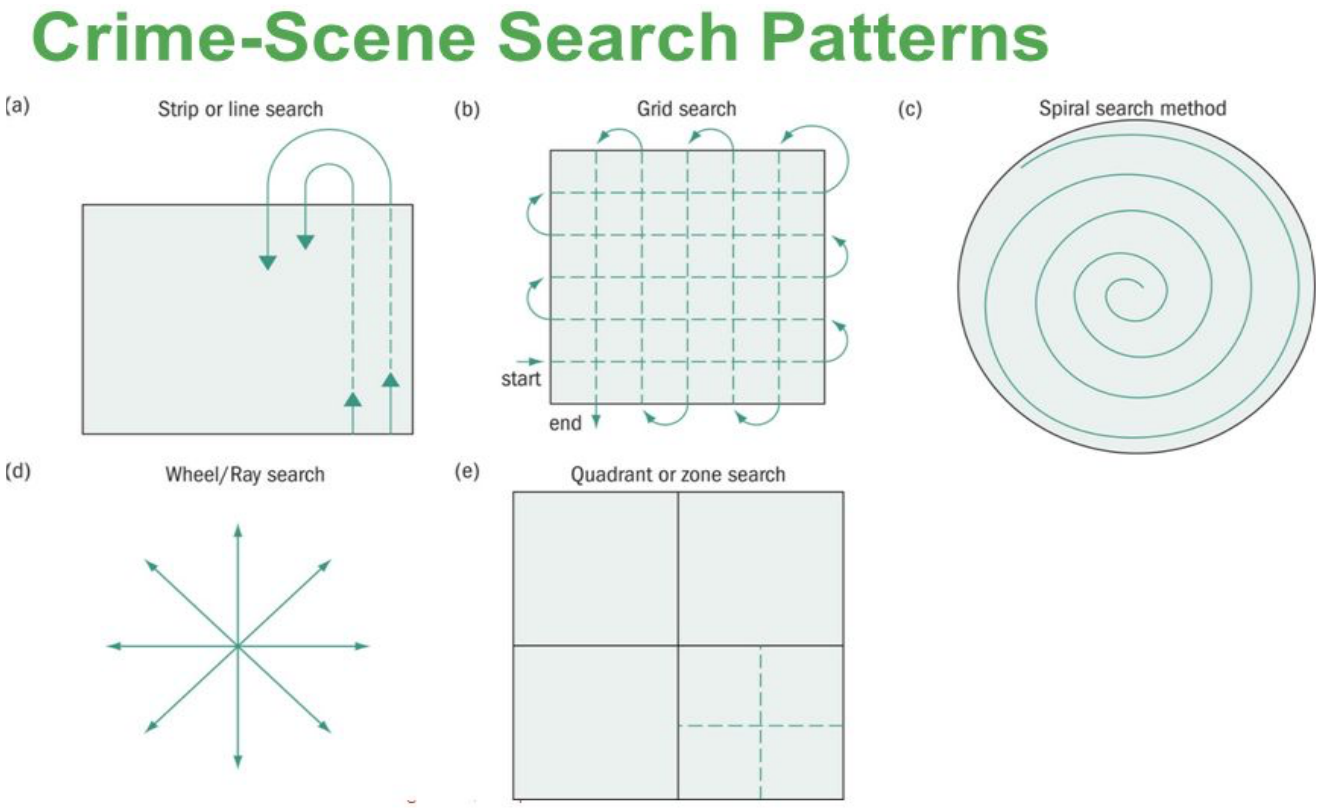
i. **Line or Strip Method**: Walk a path from one end of the crime scene to the other side of the room/area and then return in the direction from where you first started. Useful for large and outdoor scenes.

ii. **Grid method**: Best for large crime scenes such as fields. It is basically a double line search where searcher moves from one end of the area to the other.

iii. **Wheel or Ray method**: Best for small and circular crime scenes. The searchers gather at the center and proceed outward along radii.

iv. **Spiral method:** It is best used where there are no physical barriers (outdoor scenes). The searcher examines the area for evidences in an ever-widening circle, from the position of center or core of crime scene and then moves in an outward direction.

v. **Zone method:** Most effective in houses of buildings. The area is divided into four quadrants / squares and then examined using previously described methods.



Basics of Photography & Videography

Photographing and videotaping a crime scene is nothing but a part of the documentation of the crime scene. It comes in the first part of crime scene management. These are also considered as the supporting evidences in the court. Forensic photography is an organized approach to the processing of the scene of the crime. Photography and videotaping is the prior step before touching or handling anything from the crime scene. The photographs and videotapes taken from the crime scene are submitted to the court with a report under section 63 (4)(C)of BSA.

Overall Photography & Videography

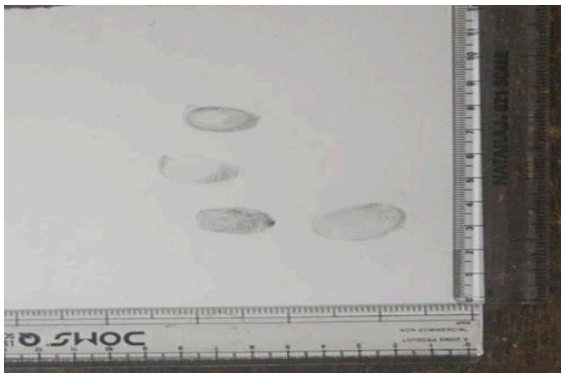
Wide angle/ wide range or overall photography / Videography will cover the whole crime scene, which include the scene as well as the surrounding area. Sometimes in case of outdoor crime scenes, wide angle photographs are taken with drone cameras which can also be used to take videos. Wide-angle lenses start with 35 mm focal lengths and provide greater depth of field. It is an accurate depiction of the scene.

Mid- Range Photography & Videography

The medium range will give the relation and location of the evidences that is the relation of each and every individual piece of evidence with others. This orientation shot will give information like how the evidences are related to its surroundings. It also gives us a fair and authentic depiction of what the scene is.

Close-up photography & Videography

Close-up photographs and recordings are the photographs and recordings that show more genuinely. This will maintain the integrity of objects and subjects. In such photographs and recordings , we are taking two shots. One with a scale or ruler to know the actual measurements and the other without scales. So, the defence can't allege that the scene was altered or the evidence is burying anything important. Apart from these, close-up photography is also called macro photography because the size of the subject/object on the negative is larger than the live size according to the reproduction ratio.



PROCEDURES:

1. GENERAL PROCEDURE TO CONDUCT SEARCH SEIZURE

Search & Seizure: Search, Seizure are one of the most important part of police investigation, particularly, search may provide ample evidence relating to crime under investigation. Search is useful in finding out the suspect or accused that may be absconding and may result in his or her apprehension for questioning or arrest, whatever the case may be. The search of his person, property and premises may result in finding incriminating evidence which could prove to be very useful in the investigation of the case. Investigation includes all the proceedings under the BNSS for collection of evidence by a police officer or by any person (other than a Magistrate) who is authorized by a Magistrate in this behalf.

a) The search should be conducted in the presence of independent witnesses who may or may not be government officials. In case no witnesses are available Police officials can also be cited as witnesses during the search. These witnesses also referred as Panch Witness should append their signatures on the seizure memo.

b) In certain cases, the search is conducted based on the disclosure made by the accused person in custody and based on his disclosure and pointing out, there can be recovery of incriminating documents, articles, arms and ammunitions and other materials. Seizure memo with respect to such articles recovered at the instance of the accused are admissible evidences, thus, should be prepared carefully.

2. PROCEDURE FOR PROCESSING SCENE OF CRIME

Basics of Audio-visual Recordings

1. Preparation

- Verify that the audio-video recording equipment is operational.
- Inform all parties present about the recording process.
- Use a tripod or stabilizer to prevent shaky footage.
- No one else other than who has to witness the statement is present in that area during the process of videography
- For recording statement of the subject/witness setup close-up frame
- Quality of videography/photography shall be given proper attention that may also be used for comparison purposes or to calculate precise measurements including but are not limited to latent prints, exemplars/standards, other ridge detail impressions, bloodstains, bullet strikes, transfer patterns, tool marks, bite marks, pattern injuries, and tire or footwear impressions

2. Safety procedure:

- Ensure that there is no immediate threat to other responders; scan area for sights, sounds, and smells that may present danger to personnel (e.g., hazardous materials such as gasoline, natural gas). If the situation involves a clandestine drug laboratory, biological weapons, or radiological or chemical threats the appropriate personnel/agency should be contacted prior to entering the scene.
- Approach the scene in a manner designed to reduce risk of harm to officer(s) while maximizing the safety of victims, witnesses, and others in the area.
- Survey the scene for dangerous persons and control the situation. Notify supervisory personnel and call for assistance/backup.

3. **Securing the crime scene:**

- In order to protect and prevent unwanted access to crime scene by the people with curiosity or malicious intentions, a perimeter must be established by police line tape.
- In order to prevent contamination of the scene or any other evidence, the officer must prevent anyone from entering into the crime scene.
- The investigating officer needs to wear gloves and protective clothing to reduce the possibility of contaminating the evidence themselves.
- Control the flow of personnel and animals entering and leaving the scene to maintain integrity of the scene.
- Maintain the privacy and confidentiality of scene of crime. Do not allow the media and press personnel.

4. **Preliminary Survey:**

- Do an overall survey of the crime scene
- Evaluate and establish a path of entry / exit to the scene to be utilized by authorized personnel.
- Evaluate initial scene boundaries.
- Conduct scene "walk-through" and initial documentation.
- Identify and protect fragile and / or perishable evidences.
- Prepare preliminary documentation of the scene as observed.
- Ensure that all evidences that may be compromised are immediately documented, photographed and collected.
- Identify the origin of the incidence and reconstruct the sequence of events. The sequence of events should not contradict with the statement of witnesses.

5. Contamination control:

Contamination control and preventing cross contamination at scene of crime is essential to maintain the safety of personnel and the integrity of evidence.

- Limit scene access to people directly involved in scene processing.
- Strictly follow established entry / exit routes at the scene.
- Use personnel protective equipment to prevent contamination of personnel and to minimize scene contamination.
- Disposable device should be used for the collection of biological evidence materials.

6. Sketching of scene of crime:

- The crime scene sketch should generally be rough sketch, however in cases of heinous crime sketches must be to scale also, distances should be measured accurately and nothing of important should be left out of the sketch map.
- The exact position of one or two permanent fixture should be provided which will be helpful in ascertaining its distance to the major articles, exhibits, marks such as blood stains, track marks of vehicles etc.
- The compass point must be indicated and the north point should be obtained by means of a compass.
- The title, case reference, date, time, name and signature of investigation officer should be mentioned in the corner of the sketch.
- The photographs should include dead body (if present) to show locations, injuries and condition.
- Each piece of evidence should be photographed to illustrate where it was found to establish relationship of evidences to the victim.
- Photographs of evidences should be taken from straight above eliminating potential distance distortions.

3. VIDEOGRAPHY PROPER DURING SEARCH SEIZURE

- **Never talk while shooting the video** and capturing the photographs on the crime scene.
- Ensure that **audio of recorder is off** & also turn off mic devices available with the officials present at the crime scene.
- Begin recording before entering the premises.
- Include a clear introduction with the date, time, location, case details, and warrant details. As far as possible, the latitude-longitude and time of recording should be recorded along with the video. The video-recording so made shall be part of the case diary.
- Clearly announce the commencement of the search and seizure operation.
- Capture a 360-degree view of the area to document its initial condition.
- Document the search process methodically, covering each room or area in sequence.
- Focus on capturing the entire search process, including a detailed walkthrough of the area being searched.
- Capture close-ups of seized items, showing their condition and any identifying marks.
- Clearly narrate the discovery and seizure of items, ensuring they are visible in the recording.
- Record the preparation and signing of the seizure list by witnesses.
- Ensure continuous recording from start to finish without unnecessary interruptions.
- End the recording with a summary of the search seizure operation.

Post-Recording

- Review the recording for accuracy and completeness.
- Securely store and backup the recording.
- Label the recording with date, time, location, case details, and a brief description of the content.

4. SPECIFIC TECHNOLOGICAL PROCEDURES OF RECORDING

1. Only departmentally approved and issued digital cameras/ Audio video recorder will be used for official criminal investigation purposes. A departmentally approved camera should have a minimum of 3.0 megapixels (3.2 MP gross), on camera viewer, close up capability, flash and a sterilize removable image memory card or device of at least 8 to 16 MB.
2. At the beginning of each tour of duty, it shall be the responsibility of the officer to ensure that
   a. The issued digital camera/ Audio video recorder is in proper working order,
   b. The camera/ Audio video recorder has a clean image memory card or device and that the camera battery or batteries are fully charged. The officer should also have a 90-degree evidence ruler which gives white, grey and black vertical and horizontal planes to be used when taking close-up photographs/Videos of injuries;
   c. The camera date stamp is correctly set and that the date stamp set so that it will not be printed on the digital images, and
   d. The camera set at "automatic" for exposure, flash and focus. Compensation may be necessary because of the skin pigmentation of the individual being photographed. The storage control should be set at "best quality."
3. In taking digital photographs/Videos, the officer should take a number of photographs/Videos. When taking photographs of injuries, the officer should have the camera at a 90- degree angle to the injury.
   a. The photographs/Video should include the following:

      (1) A photograph/Video of the general scene or if an individual, a full frame photograph/Video of the person;

      (2) A photograph/Video showing the relationship of the injury to the subject's body, and

      (3) A close-up photograph/ video of the injury, with and without the evidence ruler in the photograph/Video.

b. The officer taking digital photographs at the crime scene should view the photographs on the camera's LCD view screen to determine if the photographs effectively document a victim's injury or the crime scene.

c. The officer at the scene should not delete any digital images which are photographically faulty. Digital images that are relevant for investigative or trial purposes can be printed at a later time.

d. The digital photographs/ Video shall not be viewed with any device that would enable editing of the digital images, such as a memory card reader or a computer.

e. The officer should record the camera's/ Audio video recorders assigned numbers for the images taken for a particular crime scene or case.

f. The officer should note in the officer's incident report that photographs/ Video had been taken of the victim and of the scene.

5. TECHNOLOGICAL PROCEDURES OF STORAGE & TRANSPORTATION

1. At the conclusion of the officer's tour of duty, the officer shall:

   a. Turn in the camera's memory card to the appropriate officer or unit in headquarters by placing the memory card in an evidence envelope with identifying case information and sealed. This sealed envelope will then be delivered to the evidence specialist.

   b. Download the unaltered images into a computer file which has limited access. The writing software approved by the department should not permit re-writing or alteration of recorded images.

2. The evidence specialist, or the designated officer, will copy, **without opening,** the digital images/ Video onto a Hard Disk or Pen drive or storage devices which will become the **"master negative."**

   a. The Pen drive or storage devices shall be **write-once-read-**

many times (WORM). This master negative Disk or Pen drive or storage devices shall serve as the permanent record because it cannot be altered once written. This master negative disk or Pen drive or storage devices should be placed in a secured location or on designated desktop and not become part of the investigative case files.

b. The files on the master negative Pen drive or storage devices should be copied, **without opening**, onto another Pen drive or storage devices which becomes the working record, the **"negative duplicate or mirror image."**

c. A separate hard disk or Pen drive or storage devices should be created from the negative duplicate Pen drive or storage devices for each criminal case or investigation. The officer should confirm that the digital images were correctly transferred to a Pen drive or storage devices.

3. The **hashing** should be done at this stage, while transferring data from mobile/ audio-video recorder to dedicated computer/hard disk or storage device, using various tools and softwares (mentioned ahead) of primary & negative/mirror image and documented. **Transfers should be depicted in chain of custody forms with responder & evidence expert signing duly.**

   Hashing is a fingerprinting of any digital data present in non-volatile medium and it may be done in respect of any file, folder or complete media which contains data. Hashing is mathematical algorithm applied on a particular data to generate an alpha-numeric string of characters of fixed length and it will remain same of same data but any slightest change in data will change the hashing value entirely which can be easily noticed on comparison.

   Hashing is done of primary evidence i.e. original media as well as mirrored copy of the media to prove that both are having absolutely same data by matching the hash value. **When seizing digital evidence/device simultaneously, hashing should be done through write blocking devices to make it alter proof or any accidental data tampering due to mishandling**.

   Different hashing algorithms are as follows:

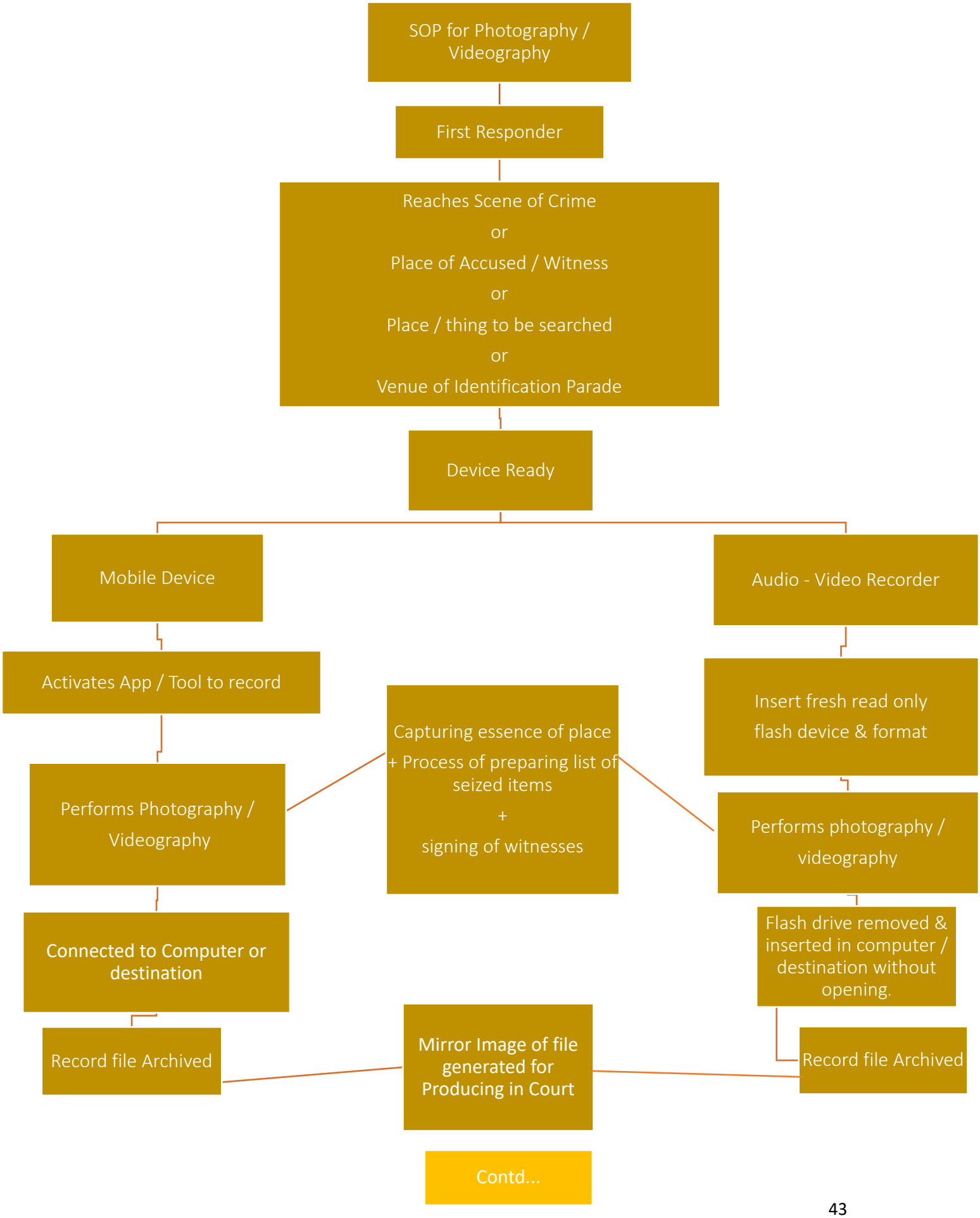
   - MD5 (Message Digest 5) - once widely used but now considered less secure due to potential collisions.

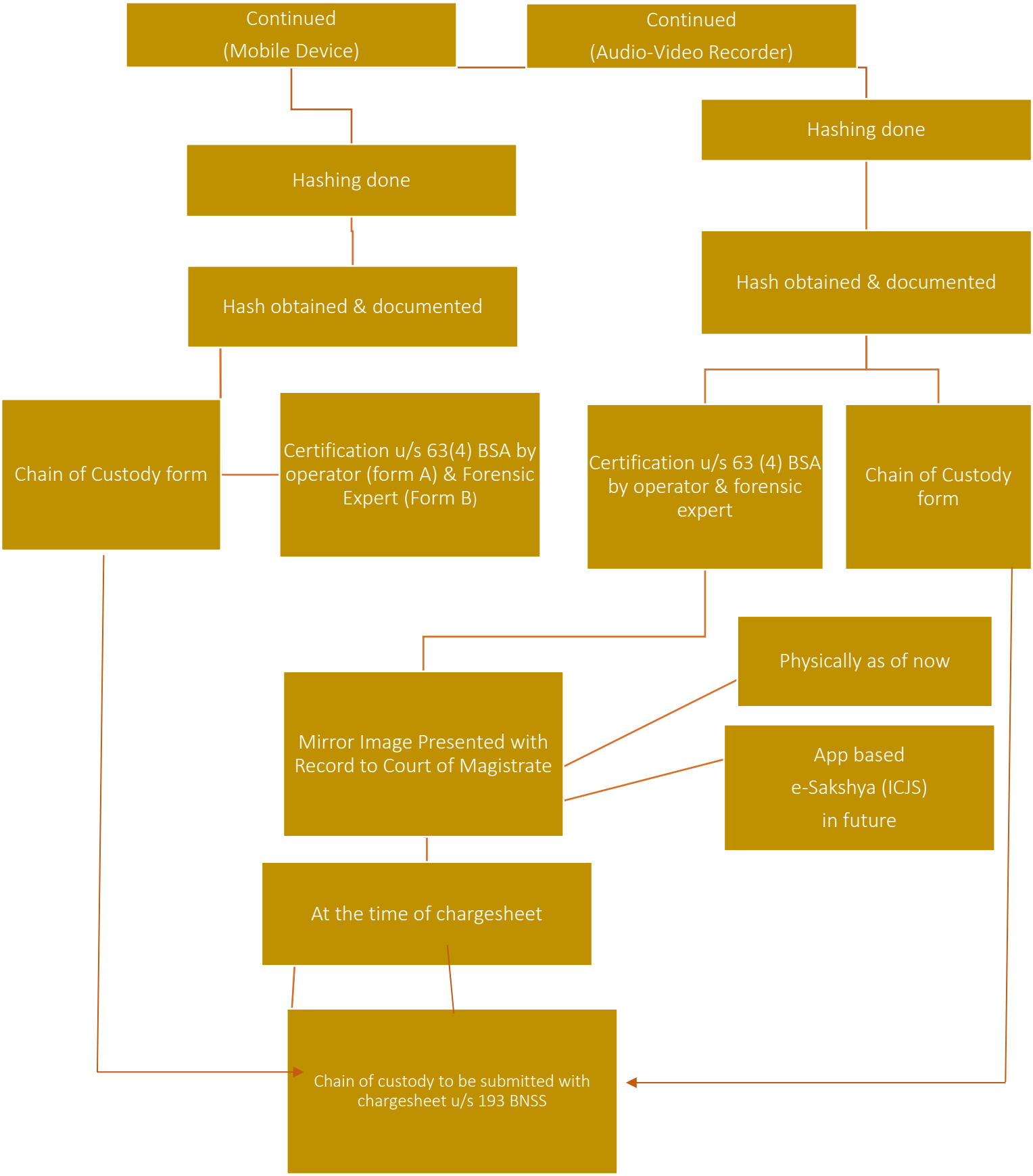
- SHA-1 (Secure Hash Algorithm 1) also facing security concerns and phasing out.
- SHA-2 family (SHA-256, SHA-384, SHA-512)- widely used, secure, and recommended for most applications.
- SHA-3 (Secure Hash Algorithm 3) - newer, more efficient, and designed for future security needs.

Following tools are available for hashing (only indicative, not exhaustive):

- Hash Check: Open-source, cross-platform tool with support for various hash algorithms and file formats.
- Hash Tab: Windows tool that integrates with the Explorer context menu to easily hash files.
- Hash My Files: Multi-platform tool with advanced features like batch hashing, comparing hash values, and generating reports.
- MD5 Hash Generator: Generates various hash values for online text input.
- SHA-256 Online: Simple web tool for hashing files uploaded from your device.
- Cyber Chef: Multi-purpose online toolset with a hashing module for various algorithms and encodings.

4. Once the master negative disk or Pen drive or storage device has been created, it shall not be removed from the custody of the appropriate department or officer. If a Pen drive or storage device is to be reviewed beyond the custody of the appropriate agent, a new Pen drive or storage device should be made from the negative duplicate Pen drive or storage device, such as for the investigating officer, prosecutor, defense attorney, etc.
5. Any enhancement of digital image files should be documented by the evidence specialist and recorded on a separate Pen drive or storage device.
6. The evidence specialist or data manager or trained '*Head Mohrir*' (crime record Munshi as is known in certain PS) **will transfer the mirror image in pen drive or storage device to the designated desktop of Magistrate** along with memos and chain of custody forms.


SOP for Photography / Videography
First Responder
Reaches Scene of Crime
or
Place of Accused / Witness
or
Place / thing to be searched
or
Venue of Identification Parade
Device Ready
Mobile Device
Audio - Video Recorder
Activates App / Tool to record
Insert fresh read only flash device & format
Capturing essence of place
+ Process of preparing list of seized items
+
signing of witnesses
Performs Photography / Videography
Performs photography / videography
Connected to Computer or destination
Flash drive removed & inserted in computer / destination without opening.
Record file Archived
Mirror Image of file generated for Producing in Court
Record file Archived
Contd...


Continued
(Mobile Device)
Continued
(Audio-Video Recorder)
Hashing done
Hash obtained & documented
Hashing done
Hash obtained & documented
Chain of Custody form
Certification u/s 63(4) BSA by operator (form A) & Forensic Expert (Form B)
Certification u/s 63 (4) BSA by operator & forensic expert
Chain of Custody form
Physically as of now
Mirror Image Presented with Record to Court of Magistrate
App based
e-Sakshya (ICJS)
in future
At the time of chargesheet
Chain of custody to be submitted with chargesheet u/s 193 BNSS

6. DO's & DON'T's by IO's for Recording Photographic & Video Evidences

1. Use the safe route when moving through the scene, avoid disturbing the scene.
2. It is important to caliber time and location of the camera before starting recording.
3. The whole episode of recording must be without any break. Also, all team members of first responder team or forensic team should maintain silence during videography and avoid any chatter or loose talk which could be then used by defense to counter the investigative sanctity. Same is also expected of witnesses present there.
4. Ensure proper lighting arrangements while conducting search

    a. Take photographs and video of the crime scene before and after the alteration.

    b. Take a complete set of pictures including aerial, long - range, mid - range and close-ups.

    c. The photographs and video should include entry and exit routes, victims and evidences as far as possible.

    d. Take photograph and video of crime scene objects such as blood stains or fingerprints or footprints as soon as possible.

    e. Take photographs and video from exterior to the interior of the crime scene and from general to the specific focus.

    f. Close-up photography and recording is preferred when taking footprint, fingerprint, shoeprint, tyre track, injuries etc.

5. Take photographs and video with scale when appropriate.
6. To take spare blank memory cards.
7. Ensure maximum charging of battery of camera and connecting wires for direct charging/operating camera.
8. There should be starting and ending shot in the recording for describing the starting and ending point of recording.

9. If search to be prolonged then to the capacity of one memory card, then there should be two audio-video recording so that continuity may be maintained by recording the scene of crime as well as change of memory card may be capture with other spare device and that recording also shall be preserved with main memory card.

10. It is to be take on record that memory card was blank before any recording.

11. Process of recovery of evidences with closeup videography revealing the identifiable details of the recovered evidence should be done.

12. Process of preparing seizure memo and signing the same by the witnesses and concerned person also should be video-graphed.

    a. Detail of camera, date/time and description of storage media i.e. memory card should be mentioned in seizure memo which matches with the details generated by camera.

    b. Hash value of the individual image/ video footage to be mentioned in the panchnama.

    c. Ensure admissibility of the digital evidence, by following the procedures demanded by law including the certificate under Sec. 63(4)(c) of BSA and maintain the authenticity and data integrity through the hash values in different places of transmission and storage.

    d. 63(4)(c) certification does not require the owner of device but the person who actually manages the device regularly at the relevant time.

    e. Don't disturb the crime scene before taking photographs and Video.

    f. Don't submit unclear photographs and recordings to the court of law.

    g. Don't submit the digital evidence without certificate under Sec. 63(4)(c) of BSA

    h. Don't forget to mention the hash value of the individual photograph and video in the case diary.

Note: The above SOP is not exhaustive; the IO should try his level best to present the original crime scene to the competent court through every mode and tool possible including digital photograph and video footages.

Note on transport and production of Audio-video content to the relevant courts:

Section 105 BNSS mandates that the record of audio-video recording should be produced to the concerned court as soon as it is done.

Now the scenarios depending on the courts' outlook could be many:

a. Courts will definitely ask for certificates mandated by BSA and chain of custody form to be produced and may or may not insist on recorded video file as such because the copies of recorded file will be produced in pen drive/ Hard disk which would increase the movement of items from malkhana and as such courts do not have their own malkhanas. Some courts can ask for video files to be submitted along with certification & chain of custody for which a mirror file from the destination computer where recorded files have been downloaded / archived and hashed would be supplied to the court in storage device like pen drive etc. All original should therefore be stored in a designated/partitioned hard drive in desktop of police station in separate file which is not touched by anyone once it is hashed. I/o's/Responders can make a copy of files and store in more accessible part of computers. **Transfers should be depicted in chain of custody forms with responder & evidence expert signing duly.**

Explanation 6 of section 57, BSA —Where a video recording is **simultaneously** stored in electronic form and transmitted or broadcast or transferred to another, each of the stored recordings is primary evidence**. So during transferring video from mobile/audio-video recorder to destination computer, a mirror image is also produced , it can be submitted to the court with sufficient credibility.**

Hence the evidence specialist or data manager or trained Head Mohrir (crime record Munshi as is known in certain PS) **will transfer the mirror image in pen drive or storage device to the designated desktop of Magistrate** along with memos and chain of custody forms.

Remember that : *giving matching hash # value of original record as proof of evidence shall be admissible as secondary evidence.*

Importance is given to the integrity of a specific file and not to the entire storage medium.

b. Sec 39 (2) states that **'When in a proceeding'**, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion ofthe Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000, is a relevant fact.

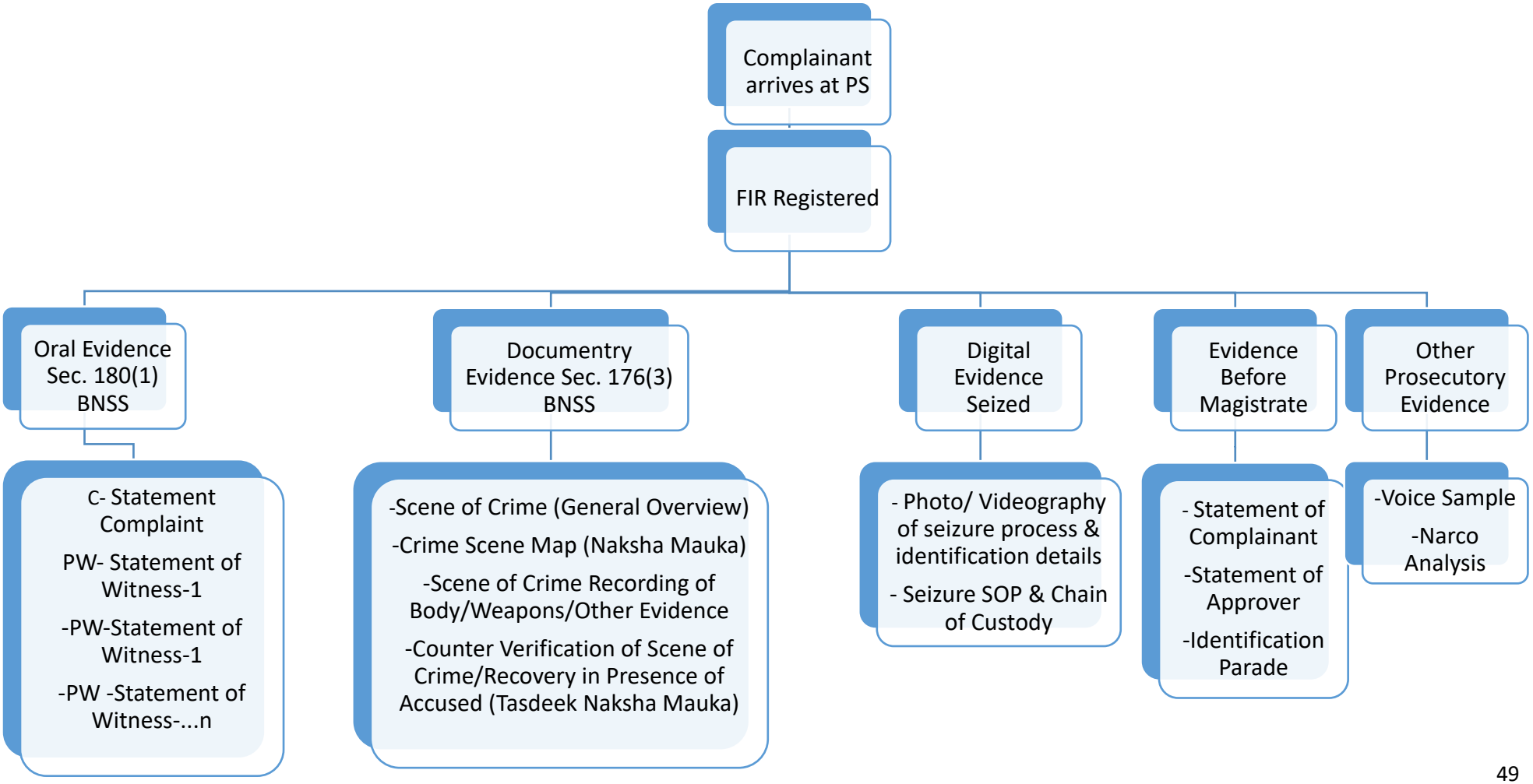
   Explanation. —For the purposes of this sub-section, an Examiner of Electronic Evidence shall be an expert.

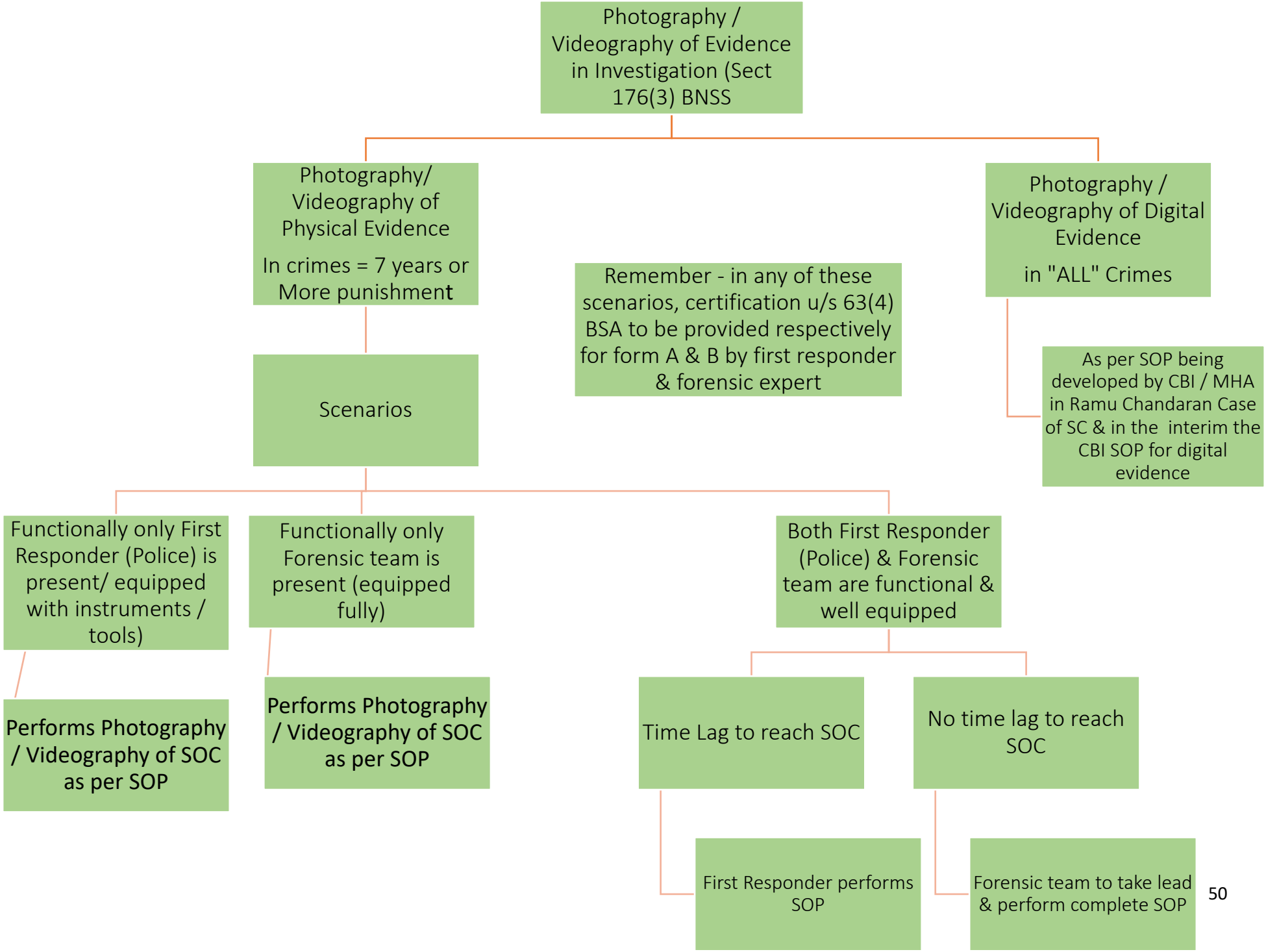
   So, the first responder/ SHO can submit the record of Audio-video documentation in mirror copy along with chain of custody of primary evidence giving proper certifications as mandated in BSA along with them. The burden of proof in case of contention will be on defense to mount a challenge and prove the violation of authenticity and the at that time, court can seek opinion ofthe Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000 and check all the hashing and chain of custody provided by responder.

c. The issue of transport and production will seize once the app based uploading and retrieving of audio-visual records will start on applications lie **e-Sakshya** or other state acts etc.(see note on app based recording)

C). PROCEDURE OF AUDIO/ VIDEOGRAPHY OF SOC IN INVESTIGATIVE TREE

General procedures & do's/don't s remain same as in search & seizure but functional & operative part corresponds as below:




Photography / Videography of Evidence in Investigation (Sect 176(3) BNSS
Photography/ Videography of Physical Evidence
In crimes = 7 years or More punishment
Remember - in any of these scenarios, certification u/s 63(4) BSA to be provided respectively for form A & B by first responder & forensic expert
Photography / Videography of Digital Evidence
in "ALL" Crimes
As per SOP being developed by CBI / MHA in Ramu Chandaran Case of SC & in the interim the CBI SOP for digital evidence
Scenarios
Functionally only First Responder (Police) is present/ equipped with instruments / tools)
Functionally only Forensic team is present (equipped fully)
Both First Responder (Police) & Forensic team are functional & well equipped
Performs Photography / Videography of SOC as per SOP
Performs Photography / Videography of SOC as per SOP
Time Lag to reach SOC
No time lag to reach SOC
First Responder performs SOP
Forensic team to take lead & perform complete SOP

PROCEDURE OF AUDIO/ VIDEOGRAPHY OF SOC ALONG WITH SEIZURE OF DIGITAL EVIDENCE

Common electronic devices that generate digital evidence may include

Device	Types of Potential Evidence
Digital/Video Camera/CCTV	• Pictures • Videos • Files stored locally or on media card
Cell Phone/ Smart phones	• Social media accounts • Text Messages or chats • Call Logs • Contacts • Applications used • Cloud based storage accounts. • App based information. • E-commerce and banking information. • Hidden or Encrypted data. • Videos, audio recordings, pictures. • Location Sharing • Google profiles and timelines • Crypto currency related details

Computer/Laptop	• Social Media accounts • Internet Search History • Documents • Email (Non-web-based) • Encrypted or hidden files. • Deleted files • Network connections • Crypto currency related details.
Game consoles and Toys	• Pictures • Videos • Documents • Microphone recordings
File Storage (Hard drive, thumb drive, optical media)	• Documents • Video/Audio files • Excel Sheets of Balance Statements, sales and financial data

Internet of Things (IoT)	• Usage logs • Network logs • AV Recordings • Even motor vehicles may carry considerable digital evidence.
Wearable Devices, Biometric Devices.	• Location • Apps used • Usage Logs • Biometric Data

a) Photographing the Set-Up

Photographing everything prior to seizure is an important first step. Some general photographs of the search site should be taken to document its pre-search condition and to serve as a reference during investigation. Documentation on how the system was configured may prove essential when the system is re-connected in the Forensic Laboratory. It should be ensured that pictures of close-ups of the front and back of all equipment and the way it is connected is taken. Special attention to switches on the back of certain equipment that must be in a certain configuration needs to be paid.

b). Collection & Preservation

- **Common storage places** where the first responder can find digital evidence include: -

  - Internal/External Hard Disk Drives (including SSD, NVMe drives etc.)
  - USB /Pen drive
  - Memory Cards
  - CD/DVD
  - MP3 Player
  - Computer/Laptop
  - Mobile Phone
  - Digital Camera
  - Smart Watch
  - Digital Video Recorder (DVR)
  - GPS Devices
  - Router etc.

- **Protected and hidden devices**

Sometimes digital evidence can also be found in electronic devices which are meant to prevent unauthorised access.

- Fingerprint based access control
- Access Card
- Digital signature certificate (dongle based)

Some smart criminal hide evidence in articles designed to disguise their true purpose such as –

- Pens (with USB concealed)
- Toys etc.

Important technical points for Digital Evidences

Purpose of any evidence being presented in criminal trial is to prove/disprove a relevant fact as well as to link the evidence with accused and victim. So while presenting digital evidence, it just not to prove some fact but also to establish source and destination of such evidential and digital artifact.

In respect of digital evidences, source and destination of evidential artifact are computer/digital devices which belong to the alleged or victim or witness of the crime. Each digital file/folder carries its identification details in its metadata while identification details of devices are in soft form as well as printed on devices also.

Please recall that section 63 (4) BSA require the identification of the record/data as well as description of the device producing such record. So, the metadata of the digital evidence and description of the producing device must be captured as part of evidence to produce in the court. Meta Data: Right click, go to property, you will find Meta data. It must also carry when go for images and photograph to avoid any morphing by using clone detection technique.

The ownership of any device is to be proved with the possession/recovery of device as well as knowledge of password of the device. In respect of any online account, ownership/possession is to be proved with user ID and password. It is further corroborated with locations, IPs of activities logs etc. of any online activities.

Generally android and other imaging tools capture the geolocation with time stamp of any photo taken by them.

Please Note:

A case captioned ***Ram Ramaswamy v Union of India*** is pending before the Supreme Court urging the Court to pass guidelines regulating seizure of electronic devices. Since the Government has formed a committee on this issue, which will be coming up with revised guidelines, Hon'ble' Supreme Court has directed in the interim order that: **"...for the time being at least the CBI manual will be followed by all the Central Government agencies."**

Hence while using BPRD's SOP on Audio-Video Recording, for concurrent seizure of digital evidence, central

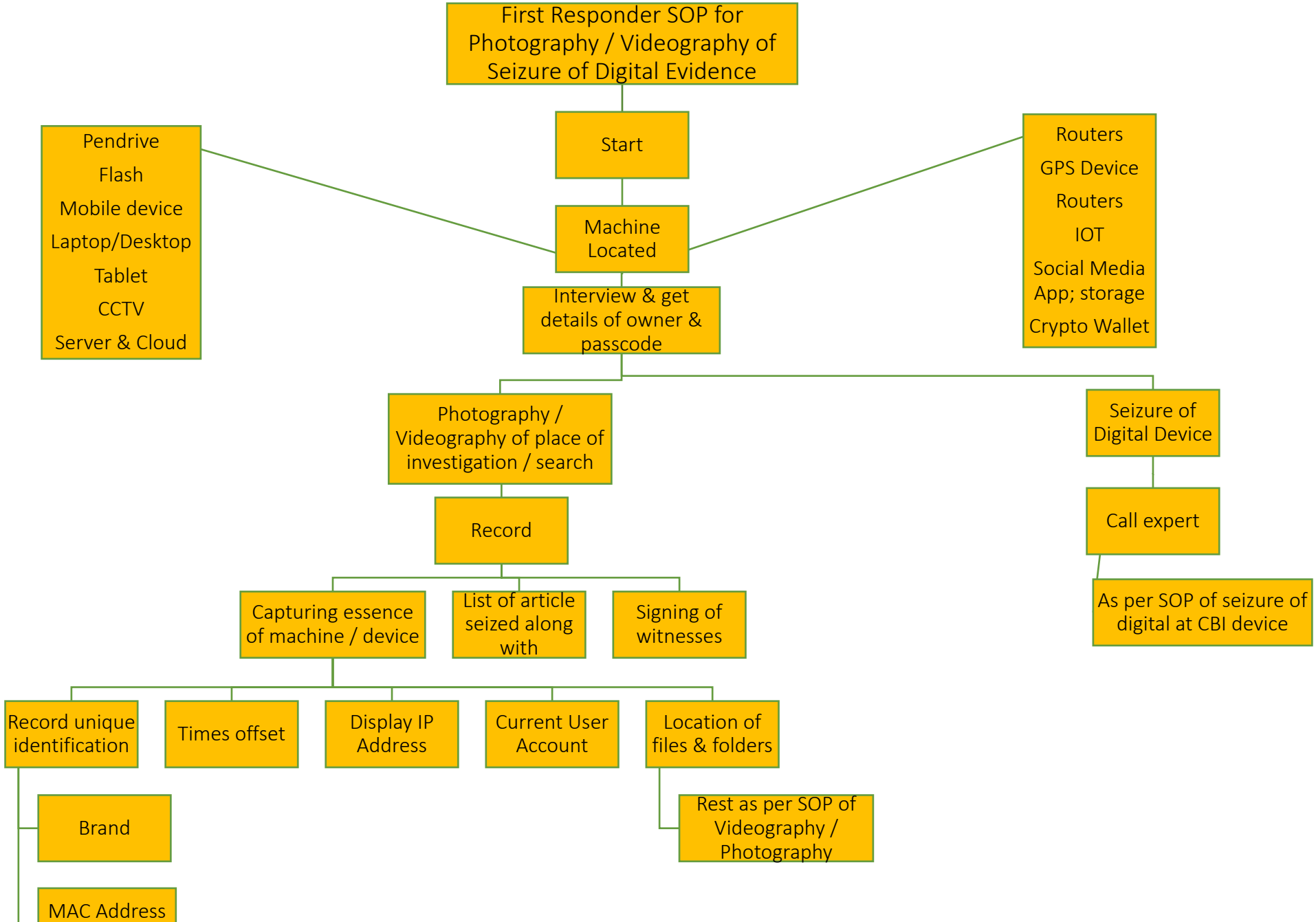
agencies can follow the CBI manual accounting the changes in the sections of NCLs.

Click Here For CBI Manual on Seizure of Digital Evidence or copy this link for assessing the manual

https://drive.google.com/file/d/1_DH4oygTD_Xb3i68XQuBBOrFy-1DhhaH/view?usp=share_link .

Detailed Note on Search & Seizure of Digital Evidence is shared below:

https://docs.google.com/document/d/18qrWC109Yp5PcQBx0C6kuliCbtUBnn0Y/edit?usp=share_link&ouid=114379320188171761637&rtpof=true&sd=true


First Responder SOP for Photography / Videography of Seizure of Digital Evidence
Start
Machine Located
Pendrive
Flash
Mobile device
Laptop/Desktop
Tablet
CCTV
Server & Cloud
Routers
GPS Device
Routers
IOT
Social Media App; storage
Crypto Wallet
Interview & get details of owner & passcode
Photography / Videography of place of investigation / search
Seizure of Digital Device
Call expert
As per SOP of seizure of digital at CBI device
Record
Capturing essence of machine / device
List of article seized along with
Signing of witnesses
Record unique identification
Times offset
Display IP Address
Current User Account
Location of files & folders
Brand
MAC Address
Rest as per SOP of Videography / Photography

B. DOCUMENTATION

1. DRAWING OF SEIZURE MEMO

After the completion of the search, the IO needs to take a call as to which articles/objects/documents/movable properties should be seized out of the recovered ones, keeping in view the evidentiary value of the same.

The search memo prepared should consist of a proper sketch of the place where search is being conducted and accurate and detailed markings should be made regarding the position of articles, material objects at the scene of crime. Wherever possible, the sketch should be drawn by a qualified draftsman. In all important cases detailed photograph and videography of the scene along with objects and useful clues should be made. The entire sequence of search should be explained and reduced in writing in the case diaries for easier understanding of senior officers and court.

The memo has to be drawn as per the Integrated Investigation Form-IV as prescribed by NCRB, which is annexed as Annexure-'C' (common in CCTNS parlance as IIF -2 Form).

Seizure memo contains the list of all articles seized by the search team from any premises or scene of crime and provides details of various items and articles along with their brief description. The seizure memo should indicate the composition of team, date and time of commencement and completion of search.

The seizure memo should be prepared in a detailed manner and the description of articles along with its colour should be indicated. In case of items which have serial no. such as mobile phones, electronic devices, computer, pen drives, laptop etc., their make along with serial no./model no. should be clearly indicated

All the seized items / properties/material objects/documents should be recorded in writing in the seizure memo duly attested by the officials, witnesses and a copy of the seizure memo may be served on the owner / occupant of the premises and signature of the said owner / occupant should be obtained on the said seizure memo.

The witnesses and the IO should append their signatures on the seized documents/seized articles.

The sample seal in triplicate has to be drawn and the seal with

which the article was sealed has to be handed over to the witness with an instruction to produce the same before the court at an appropriate time and to maintain the integrity of the chain of custody of the seized articles.

After completion of the search proceedings, the IO/search team shall deposit the seized items/documents/properties/ material objects into the Malkhana of the nearest

police station as warranted under Section 43B of the UA (P) Act by making proper entry in Malkhana Register to maintain the chain of custody.

The seizure shall be reported to the court having jurisdiction just after the search and permission of the said competent jurisdictional court, if any, be obtained for retention of the seized properties.

2. DOCUMENTATION & FOLLOW UP AT POLICE STATION

- The investigating officer shall maintain documentation as a permanent record.
- The police officer will, as per procedure below, without delay, but not later than 48 hours, send to the Magistrate copy of the list of seized items with the signature of the witnesses and video- recording of the search and seizure process.

i. On completion of the search and seizure operation, the police officer will bring the audio-video electronic device which was used for recording to the Police Station.

ii. At the Police Station, the AV recording will be transferred to the local designated desktop - either directly through device insertion or via Cable or Bluetooth. Mention of this will be made in chain of custody form & Hashing will be done.

iii. The downloaded file will be named in a manner so that the relevant metadata of FIR Number, police station, date and serial number of the video related to the offence is captured therein. The standard format will be

FIR No_.....ddmmyy_....SNo……

iv. The police officer will make an entry in the general diary regarding the downloading of the video wherein the file name (as explained in (iii) above) will be linked to the FIR number, Police Officer ID, Date and Time of recording, Latitude-Longitude and any other remarks, if any.

v. The AV recording will be scanned for any virus before any further processing.

vi. The AV recording will then be deleted from the police officer's smartphone or audio-video recorder, making space for more recordings to be made in the future.

vii. The following day, the designated data manager of the police station will transfer all such recordings of the last 24 hours on a portable storage devise and proceed to download all the recordings on the storage device of the Magistrate.

- The notes and reports should be done in a chronological order and should include no opinions, no analysis or no conclusions but just facts.

3. CHAIN OF CUSTODY

"Proper custody" means the record was maintained in a secure and reliable system with appropriate access controls and audit trails. (Kindly refer Sec. 8[1] with explanation, Sec. 93 of the BSA)

BSA Explanation to Sec 80 & 81

Documents/Electronic Records are said to be in proper custody if they are in the place which, and looked after by the person with whom such document is required to be kept; but no custody is improper if it is proved to have had a legitimate origin, or if the circumstances of the particular case are such as to render such an origin probable

Chain of custody of electronic evidence is imperative. Hashing of digital evidence collected should be ensured to ascertain integrity of digital evidence seized. Once packed and sealed in front of the witnesses, a clear record of chain of custody should be kept in writing for each package till it is handed over to the CFSL for forensic examination. The package should normally be sent for forensic examination to the CFSL without undue delays.

Document the chain of custody

- Name and signature of each person, including internal staff, who take possession or transport the evidence.
- Date of transfer.
- Evidence's label or serial number.

Chain of Custody Form

Case Details

FIR No	Police Station	Name of I.O.	Date of Seizure	Time	Place

Device Details

Item No.	Device Type	Make	Model	Device Serial No.	Description	Remarks

Chain of Custody Documentation

Item No	Received From	Received By	Reason	Date/Time	Sign. of Receiver	Remarks

C. COST ESTIMATION

Volume of videography work

According to the Crime in India report for 2022 published by the National Crime Records Bureau, a total of 58.24 lakh IPC and SLL crimes were reported in India. It is estimated that 20% of these crimes involve punishments of seven years or more, and seizures occur in 35% of cases. Consequently, it is estimated that 11.64 lakh crimes will require crime scene photography and videography as per Clause 176 of the BNSS, and 20.38 lakh crimes will involve seizures.

Costing & Budgeting

The states will have to cater to needs of police stations for additional burden of audio-video recording as mandated in New Criminal Laws. This can be made granular as following:

1. Minimum number of Audio Video recorders at police stations at some minimum ratio say 5 recorders per PS considering 5 I/Os at simultaneous work.(This will be a need till state migrates fully to **e-sakshya** facility)
2. One dedicated desktop for Evidence Specialist/ data manager/ /Information assistant **(Whatever term states use as per norms of the delegation, recruitment or training for the Digital Forensic Expert)** at each police station.
3. Dedicated vehicle for digital forensic experts/ first responders to reach scene of crime. (This can be catered through additional vehicle/s with driver of existing 112-ERSS Mechanism and can be made stationed at control rooms).
4. A dedicated room with work stations for forensic teams and first responders to store and collect their equipment and transfer their files to desk station.
5. Storage facility at data centers for parallel storage, if states go for it, till states fully integrate to e-sakshya facility.

States can budget accordingly to the needs stated above to cater to the implementation of NCLs.

D. Proposed App based solutions: e-Sakshya and others.

The advent of technology by way of smartphone which is in fact a small computer in itself that has an operating system, RAM, input and output devices and is connected to internet and a network and which is easily carried in almost everyone's pocket offers a handy tool in achieving the above objective. Almost everyone is using applications like WhatsApp to send Videos and photographs to their near and dear ones and police officers are one of them. Some police officers are using WhatsApp for understanding the scene of crime remotely.

It is also worthwhile to mention that technology enables us to record certain data (called the metadata) in the file itself. We are proposing the usage of metadata to record critical investigation information as metadata in the files. The metadata will automatically record the latitude and longitude, date and time from the GPS and will have the crime number and other details that has to be manually entered by the user.

The smartphones being powerful pocket computers are capable to make complicated calculations in split seconds. We are using the smartphones to calculate the hash values of each file.

While using smartphones with good resolution cameras to record the evidence with the help of sophisticated software with geo-tagging and time-stamping. These; photos/ videos and their meta-data would immediately be provided with a Hash value and sent to secure servers for storage as permanent record and for later retrieval for investigation purposes.

For this, Android/ iOS/ MS based application' supported by a web application has been developed by many central/state units previously and now with the advent of New Criminal Laws, NCRB through the **'e-Sakshya'** is adding cloud based audio/video recording application to be dovetailed in CCTNS-2.0.

The app can be installed on any android smartphone that has an inbuilt. GPS as the time and date stamp and latitude and longitude are extracted in real time from the GPS data and is embedded in the metadata. Each file (whether photograph or video) has the data of photographs and videographs with associated metadata stored in the file itself. The HASH value of each individual photograph/video is also calculated in real time and embedded in the metadata and the file(s) will immediately sync to the server or can be emailed to a specific email id. Even the address of the server and the email id are stored in the metadata.

The tool thus addresses the authenticity of the photograph/video by way of storing the crime' details in the metadata; calculating the hash values and even printing them on the individual photo/video and sending them to the secure server thus maintaining the chain of custody. The tools will be extremely easy to use, secure and foolproof.

eSakshya@ICJS

A Process Recording (Videography/Photography) Platform for Criminal Justice System

Provided at

Prepared for

State and Central Investigating Agencies

By

MHA Informatics Division

Step by Step Guide for testing and onboarding on eSakshya Platform

1. ICJS Nodal Officer of a District of any State/ UT will create Police Station wise authorised users to access the eSakshya Mobile Application on ICJS platform. **(Annexure A in detailed User Manual)**

2. Authorised users of Police Station can
   a. download eSakshya Mobile Application from mSeva Mobile App Store.
   b. install eSakshya mobile app on mobile phone. (**User Manual at Annexure B**)
   c. test the eSakshya mobile app thoroughly.
3. ICJS Nodal Officer of State / UT will upload UAT certificate of eSakshya based on the testing feedback of the mobile app from authorised users of police stations. **(Annexure C Section II in detailed user manual)**

4. Onboarding Process for Go Live on eSakshya Platform:

   a. **Registration for Sakshya Locker (Annexure D in detailed user manual):**
      - **Registration of State/UT:** Nodal Officer of State/UT will register in API Setu Portal (https://apisetu.gov.in/) by submitting Basic Details, Organizational details and completing the Sign-Up process.
      - **Sakshya Locker Agreement:** Sakshya Locker team of NeGD will share the draft agreement, payment and other formalities.
      - **Generation of Client ID and Secret Key**: Subsequent to the singing of agreement, Nodal Officer of State/UT will generate Client ID and Secret Key.
   b. **Sharing of Client ID and Secret Key**: Nodal Officer of State/UT will update the Client ID and Secret Key received from API Setu platform with ICJS**. (Annexure C Section I in detailed user manual)**
   c. Issuance of Go Live Certificate (Annexure C Section III in **detailed user manual**)
      - Nodal Officer of State/UT will upload Go Live Certificate on ICJS to go online as per the mutual readiness.

d. **Confirmation of Go Live**: ICJS will confirm the go live of eSakshya Platform for a State/UT.

For Detailed Information on **e-Sakshya please see:**

https://drive.google.com/file/d/1YP9c-Q76nG9DxOT6AMv2-9O2pzGSOMHn/view?usp=share_link

****

E. Aide-memoir

1. Audio-Video Recording of Scene of Crime / Statement of witness

- Device to be used: camera or phone
- Calibre time/date and set the location on before starting the recording
- Where to Store of the Recording: external Memory card/Storage device alone or Cloud storage or both (parallel storage)
- Set a path of the input file preferably to the removeable media/MMC Card or the cloud server as per protocol
- The whole episode of recording without a break to ensure continuity
- Proper arrangement of lighting for recording
- Maximum charging of the recording device
- One location of SOC: Size of the file
- More than one location of SOC: Size of the file
- Process of recovery of evidence with close-up videography
- Process of preparing seizure memo and signing the same by the witness
- Process of calculation of hash value of the recorded media to ensure authenticity and integrity.
- Details of the recording device, i.e., camera or mobile phone, date/time & description of storage device, i.e., memory card, hash value so calculated to be mentioned in seizure memo
- Admissibility of the AV Recording in the Court
- Proper custody (Section 81 & Section 93, BSA, 2023)

2) Certificate u/s 63 (4) (c) of BSA, 2023

- Certification does not necessarily require the owner of the device but the person who manages the device regularly at relevant times in the prescribed format as laid down in BSA schedule Part-A.

3) Search & Seizure of Digital Evidence

- Hardware: Computers, mobile devices, storage media, CCTV systems, network devices etc.
- Software: Operating systems, applications, firmware, malicious, etc
- Data: Documents, emails, images, audio/video files, logs, metadata
- Online evidence: social media, cloud storage, websites, internet activity logs

Annexure-A

THE SCHEDULE

[*See* section 63(*4*)(*c*)]

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: _____

Annexure -B

LIST OF ESSENTIAL ITEMS TO BE REQUIRED BEFORE SEARCH & SEIZURE

1. Copy of warrant / power delegation letter by the CIO.
2. Coordination among team members.
3. Stationery (papers A4/Legal, pens, pencils, scale, stapler, paper clips, File covers etc.)
4. Brass seal.
5. Sealing materials.
6. Investigation bags.
7. Packing clothes.
8. Needle.
9. Thread.
10. Slide glass.
11. Hand gloves.
12. Magnifier glass.
13. T orch.
14. Tarpaulin & ropes (if required as per ground situations).
15. Umbrella (in case of rainy climates).
16. Candles.
17. Match box.
18. Camera (for photo & videography).
19. Marker pen.
20. Hand bags or packing box (to bring seized articles from the scene of crimes or accused houses).
21. Envelopes.
22. Eye spectacles.
23. Glass jar to collect the evidence (as per requirement to see the kind of search).
24. Small plastic / fiber boxes (to collect the evidences if need).
25. Vehicles (as per requirement).

Annexure – C

IIF – IV PROPERTY SEARCH & SEIZURE FORM

(Search/Production/Recovery u/s 85/105/185 BNSS..... etc.)

1. District ..... P.S. ..... Year ..... FIR/G.D. No. ..... Date.....

2. Acts and Sections..... .....

3. Nature of property seized: Stolen/Unclaimed/Unlawful possession/Involved/Intestate.

4. Property seized/recovered:

(a) Date ..... (b) Time

(c) Place .....

(d) Description of the place .....

5. Person from whom seized/recovered:

Name ..... Father's/Husband's name .....

Sex ..... Age ..... Occupation .....

Address .....

Professional receiver of stolen property. Yes/No

6. Witness:

1. (i) Name ..... Father's/Husband's name ..... Age ..... Occupation..... Address.....

2. (ii) Name ..... Father's/Husband's name…… Age ..... Occupation ..... Address .....

7. Action taken/recommended for disposal of perishable property ...

8. Action taken/recommended for keeping of valuable property.....

9. Identification required. Yes/No

10. Details of properties seized/recovered (Use appropriate prescribed form(s) and attach).

(1) .....

(2) .....

(Attach separate sheet, if required)

11. Circumstances/grounds for seizure

12. The above mentioned were seized in accordance with the provisions of law in the presence of the above said witness/* and a copy of the seizure form was given to the person/ the occupant of the place from whom seized.

13. The following properties were packed and/or sealed and the signature of the above said witnesses obtained thereon or on the body of the property.

Sl. No	Property	Indicate whether signature obtained on the packet or on the body of the property

Signature of the person from whom seized (if present)

Witness-1

……..Signature

Witness-2

..... Signature

Specimen of the seal is given below

..... Signature of Investigating Officer

Name..... Rank ..... No .....

Place ..... Date .....

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

सत्यमेव जयते

NCRB Mobile App "NCRB Sankalan of Criminal Laws"

NCRB has launched a Mobile App "NCRB Sankalan of criminal Laws". This App is compilation of new criminal laws namely Bharatiya Nayaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam. It is available on Googleplay store as well as Apple App store. This App is useful for General Public, Court Officers, Advocates, Law Students as well as for Police Officers in enhancing their knowledge about the New Criminal Laws. This App serves as a comprehensive guide providing complete information about the new criminal laws at one place. It provides an Index linking all Chapters and Sections of the new laws and a corresponding chart for section wise comparison between old and new laws with a search and linking facility for quick information retrieval. The App is designed to work in offline mode also in absence of connectivity. With its user-friendly design, comprehensive content, and innovative features, the app empower susers to learn the new laws effectively.

NCRB
SANKALAN
of New Criminal Laws

https://ncrb.gov.in/uploads/SankalanPortal/Index.html