Scheme for Notifying Examiner of Electronic Evidence Under section 79A of the Information Technology Act 2000

Government of India

Ministry of Electronics & Information Technology

(MeitY)

Version 2.0

Table of Content

1. About the Scheme for notifying forensic laboratories as "Examiner of Electronic Evidence"

CHAPTER XIIA of the Information Technology Act, 2000 empowers the Central Government under section 79A to notify any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence for the purposes of providing expert opinion on electronic form evidence before any court or other authority specified by notification in the Official Gazette. The *Explanation* clause of section 79A further articulates that the "Electronic Form Evidence" means any information of probative value that is either stored or transmitted in electronic form and includes evidence, digital data, digital video, cell phones, digital fax machine etc.

a) In line with the above requirement, MeitY had formulated a scheme for notifying the 'Examiner of Electronic Evidence' in January, 2017. The objective of the scheme is to ascertain the competence of all the desiring Central Government or a State Government agency and to qualify them to act as 'Examiner of Electronic Evidence" as per their scope of approval through a formal assessment / audit process. Once notified, notified Central, State Government agencies can act as the "Examiner of Electronic Evidence", and provide expert opinion of digital / electronic evidences before any court.

b) The scheme was prepared based on best practices of International Standards and Guidelines (**Refer Annexure - I**). The assessment / audit process of applicant laboratory/organizations/ bodies includes assessment of the technical skilled professional manpower in digital forensics, licensed tools and equipment, adequate laboratory infrastructure including support infrastructure, availability of suitable environment including existence of a proper quality management system; to carry out examination of digital/ electronic evidences.

2. Eligible Organizations:

Digital/Cyber forensics science Laboratories / Organizations of any Department, body or agency of the Central Government or a State Government / UT seeking to be notified as an "Examiner of Electronic Evidence" as mandated under section 79A of Information Technology Act 2000 and other related acts/ regulations, can apply to Ministry of Electronics & Information Technology (MeitY), Government of India by submitting an application form as prescribed in the **Annexure – II.** Scheme is not for individual expert to be notified as Expert Examiners rather for labs to be notified as 'Examiner of Electronics Evidence' in line with 79A of IT Act.

3. Scope Areas / Activities under the Scheme

The scope of notification under this scheme may apply any one or more following areas of activity of the applicant's laboratory / organization.

1. Computer (Media) Forensics
2. Mobile Devices Forensics
3. CCTV Forensics
4. Drone Forensics
5. Digital Video / Image Forensics
6. Digital Audio Forensics
7. Digital Device Specific Forensics
8. Digital Equipment / Machines Forensics (having embedded firmware)
9. Network Forensics
10. Cloud Forensics
11. Any other (please specify)

While applying for notification the scope areas must be specified the candidate labs. The specific technical details of activities must be mentioned. The exclusions if any also need to be described.

A laboratory already notified for some areas, also may seek notification for additional areas as scope expansion as and when the capabilities for the enhanced scope are acquired.

4. Requirements & Criteria for notification :

The Laboratories / Organizations / Bodies seeking notification as "Examiner of Electronic Evidence" as provisioned under Section 79A of Information Technology Act 2000, should have the following in place:

4.1 Legal status :

Should be a department, body or agency of the Central Government or a State Government mandated for the purpose of providing expert opinion on electronic form of evidence before any court or other authority (through examination of electronic/ digital evidences).

4.2 Infrastructure :

Should have the suitable and adequate:

a. Physical Premises and laboratory space
b. Physical and logical security of the laboratory facilities
c. Work Environment and Climate
d. Fire, Electrical Hazard safety etc.
e. Support services such as HVAC, UPS, Power backup, Electrical earthling etc.
f. Tools and Equipment (licenced)
g. Safe and secure (Fire resistant) storage and handling facilities for electronic evidence artefacts

4.3 Manpower Resources:

Should have manpower resources :

a. Minimum two number of regular technical/scientific manpower with expertise (at least 1 year of work/job experience) in scope areas / activities for which the applicant laboratory is seeking the notification including one reporting and reviewing officers as detailed in Annexure IV.
b. With adequate skills (technical, analytical, examination, forensics etc) and continual up gradation of skills through training (on current and advance technical topics, tools, equipment required for analysis, examination and forensic purposes) in last 5 years in the technical subjects/topics in the areas seeking the notification.

4.4 Documented Information:

a. Laboratory Quality Manual / Handbook
b. Laboratory (Standard Operating Procedures) including
    i. Case acceptance
    ii. Handling of electronic exhibits and chain of custody
    iii. Security, storage and preservation of electronic exhibits
    iv. Examination/ analysis of electronic exhibits
    v. Reporting of electronic exhibits
    vi. Operation / handling of Tools / Equipment
    vii. Capacity management, Change management, maintenance of Tools and equipment
    viii. Training of laboratory manpower resources
    ix. Internal audit and management reviews
    x. Risk assessment
    xi. Any other relevant procedure

4.5 Global Standards & Guidelines : (Refer Annexure I)

Should follow and practice latest updated global standards and guidelines including following Standards:

a. **ISO/IEC 17025** (General requirements for the competence of testing and calibration laboratories).
b. **ISO/IEC 27037** (Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence),

Reference Standards:

a) **ISO/IEC 27041** (Information technology - Security techniques - Guidelines on assuring suitability and adequacy of incident investigative methods)
b) **ISO/IEC 27042** (Information technology - Security techniques - Guidelines on for analysis and interpretation of digital evidence)
c) **ISO/IEC 27043** (A Standard on Information technology - Security techniques – Incident investigation principles and processes within which forensics generally occur)

d) **ISO/IEC 27038** (Information technology - Security techniques – Specification for digital redaction)

e) **ISO/IEC 27040** (Information technology - Security techniques – Storage Security)

f) **ISO/IEC 30121** (A Standard on Information technology – Governance of Digital Forensic Risk Framework)

5. Procedure for Application, Assessment, Evaluation and Recommendation for Notification

The organizations/ laboratories seeking notification at 'Examiner of Electronic Evidence', should have an established laboratory quality management system in line with the requirements of current version of the ISO/IEC 17025 standard, best practices as given in the ISO/IEC 27037 Guideline standard.

5.1 Application: The Application form as prescribed in **Annexure II** of this scheme (duly filled) along with applicable quality system documentation and Statuary Declaration and Indemnity (duly signed and stamped), need to be submitted to:

The Group Coordinator (Cyber Security)
Ministry of Electronics & Information Technology (MeitY)
Govt of India, 6 CGO Complex, Lodi Road, New Delhi -110003

An online portal for automation of the end-to-end application, assessment, and pre-assessment process with a dashboard for the Scheme of 79A of the IT Act, 2000 to notify 'Examiners of Electronic Evidence' is under preparation and would be made available in due course for submission of application forms.

5.2 Stage – I - Assessment

a. Application review: Within 14 working days from the receipt of application, an acknowledgement conforming the receipt of the application will be communicated to the candidate lab. The preliminary assessment of submitted application and

documents will be carried out. The findings / gaps found during the preliminary assessment will be communicated to the applicant organization / lab prior to conducting on-site Stage-I Assessment. During this desktop evaluation MeitY may call/ have a meeting with the applicant organization's representative, to discuss and understand the laboratory's management system requirements for the applied scope of areas.

b. Stage I visit: Stage-I assessment may be done through on-site visit and /or virtual meeting to gain first-hand information/understanding about the context of operation, processes, size, complexity, and applicant lab's readiness. Objective to the Stage - 1 assessment is to ascertain that the policies, rules, manual, guidelines, standard operating procedures are defined as per the scheme and the standards referred in various Annexures. The gaps and / or issues observed will be reported as Stage-I assessment report. Stage – I assessment report will be communicated to candidate labs within 4 to 6 weeks from the acknowledgement date. The identified gaps need to be corrected by candidate labs in prescribed time frame as mentioned in report before proceeding to stage II assessment. Assessment team will evaluate the submission of candidate lab within 10 working days from the receipt of the response.

c. The Stage - I assessment duration is normally one or two days. The findings of Stage - I assessment is reported and documented as Stage I assessment report and used for planning /conduct of Stage II assessment.

5.3 Stage II - On-Site Assessment Visit:

Stage-II assessment will be completed within 4 to 6 weeks from the closure of stage – I findings. The objective of stage II assessment is to ascertain the implementation of applicant laboratory's documented policies, rules, manuals, procedures, adoption of best practices and ability of laboratory to meet the scheme assessment criteria. It includes verifying records for ascertaining the effectiveness of the implementation of the policies/ procedures, documented information, technical aspects, competency of manpower in digital forensics, availability of upto date licensed tools and equipment,

availability of suitable environment to carry out such examination as also the availability of a proper quality management system and reasonable experience to demonstrate their overall competency in applied scope of areas.

The duration of assessment depends upon the scope of areas and complexity of process. Normally one scope area required maximum two man-day of assessment. The finding of Stage-II assessments is documented as Stage-II assessment report along with its recommendations. The gaps / non-conformances/ issues, if any, are reported to laboratory as Stage II report, for taking necessary corrective/ preventive actions.

Corrective Actions / Preventive Action**:** The applicant laboratory will be required to take corrective action for observed gaps / non-conformances/ issues reported during the assessment, within the prescribed time (generally 4 to 6 weeks or as assigned by the assessment team in its report). The evidences of corrective actions shall be submitted to assessment team leader, for review and acceptance. On acceptance of closure of gaps by assessment team, the case will be forwarded to Stage III committee within 4 week from receipt of corrective actions from candidate lab.

5.4 Stage III : Review by Higher level of committee

A Stage-III is a higher level of committee constituted by MeitY, reviews the findings of the assessment team and recommendation of the assessment team in respect of applicant's laboratory and the scope of the notification. This is an independent review carried out by high level committee consisting of members independent of persons directly involved in assessment process. The case is presented by cyber security division scientist to Stage III committee.

Upon recommendation of Stage III committee and after seeking formal approval from the Secretary, MeitY, the applicant laboratory is notified for the relevant scope of areas as 'Examiner of Electronic Evidence'.

Any delay of more than one year in closing the gaps / non-conformances/ issues reported during the assessment by candidate labs would require re-assessment.

5.5 Stage I-III : Timelines of report

- Assessment Team after conduction of each audit stage i.e. Stage-I & Stage-II and receipt of Corrective Action/Preventive Action (CA/PA) from the lab should prepare & submit a duly signed Non-Conformity (NC) Closure report. This needs to be ensured by Lead Auditor. The verification criteria of each checkpoint should be clearly and unambiguously defined and any recommendation/NC against this point shall be based upon objectively verifiable evidence.

- After closing all the NCs raised in stage-II assessment, the assessment team shall clearly propose to Stage-III Committee that the respective lab may be empanelled for the specified scope or not based on the objective verifiable criteria for recommendation.

6. Notification and Validity

A gazette notification is issued based on satisfactory assessment, independent review by Stage III committee and approval of recommendations by competent authority as detailed in previous section.

A notification declaring the applicant laboratory/organization as **"Examiner of Electronic Evidence"** along with scope will be issued in the Gazette of India. A notified Laboratory/organization will continue to remain notified unless the approval of the lab is withdrawn for the reasons as stated in de-notification process.

7. Surveillance and De-notification

7.1 Surveillance assessment:

A laboratory once notified, shall be responsible to ensure continued compliance to the requirements of this scheme. MeitY will conduct regular surveillance assessments. As part of surveillance assessment, the notified laboratory/ organization need to submit the requisite annual information indicated in the Annexure III, in the beginning of each Calendar year i.e. during January of each year latest by 31st January.

Further, MeitY shall be conducting the onsite surveillance assessments at an interval of 3 years from notification date / previous assessment in most cases depending on

review of yearly data and in only those cases where there is significant change have taken place as reported by lab, the surveillance audit may be carried out on yearly basis. In case of any major changes in the laboratory/ organization infrastructure, location, equipment/tools and management structure, laboratory shall report the same to MeitY immediately. Upon review, surveillances can be scheduled earlier than 3 year planned surveillances. The surveillance would typically be of 2 man-days.

7.2 De-notification :

Any of the following conditions, if noticed may lead to de-notification of the laboratory:

i. If the laboratory quality management system completely breaks down.
ii. If the laboratory fails to submit itself for annual information.
iii. If the minimum number of regular technical/scientific manpower falls below two as detailed in Annexure IV.
iv. The major observations of the Hon'ble courts causing serious apprehension on the laboratory's competence/ impartiality of operations
v. In case of any major change in the management / organizational structure which casts apprehension on the laboratory's impartiality and confidentiality of operations
vi. A laboratory may get de-notified only for a part of its notified scope, if any of above conditions stated above are applicable, in that particular area.

The de-notification shall be published in gazette of India and same will be communicated to the concerned laboratory / organization's Head and also to the Secretary of concerned Ministries /State/ Union Territory. A de-notified laboratory, if wishes to get re-notified, need to re-apply as a fresh applicant and has to undergo the complete cycle of assessment.

8. <u>Procedure for Scope change / expansion.:</u>

The laboratories/ organization seeking scope change (for notified areas), expansion or addition of new scope areas, need to apply in the prescribed application format and need to undergo for the complete assessment process i.e. (Stage I, II and III) as listed in SL No. 5 above. Only in case of Minor changes (editorial changes), Group Coordinator, Cyber Security Group, MeitY, can decide to waive off the stage I and II assessment.

9. Complaints and Appeals

Laboratories/ organizations are free to complain against the findings of assessment or decision on notification / de-notification by writing to the Group coordinator, Cyber Security Group, MeitY. In case the laboratory/ organization is not satisfied with the decision of Group coordinator Cyber Security Group, MeitY; the laboratory may appeal to the Secretary MeitY, who's decision shall be final and binding on all.

10. Fee / Modalities

Serial Number	Stages of Application, Assessment and Notification	Fee Details
1	Application	Nil
2	Stage I (Off site Desktop Assessment), Stage I Onsite Assessment and Stage II Onsite assessment	Nil
3	Issue of Notification / De-notification	Nil
4	Surveillance Assessment / Additional surveillances	Nil
5	Scope Modification / Addition / New Scope	Nil
Note	1. The applicant laboratory/ organisation to provide the travel tickets by air / train/ bus to the assessment team. (as per the entitlement of the officers prescribed by Govt of India) with validation and confirmation from CSD Division, MeitY. 2. The applicant laboratory/ organisation also to provide the Local *Trav*el, boarding and lodging and complete logistics to the assessment team. (as per the entitlement of the officers prescribed by Govt of India) 3. In case, if an external technical subject matter (specific area of forensics), is deputed as part of assessment team, the applicant laboratory needs to provide the travel tickets (Economy class air) and arrange his/her stay/local logistics (boarding and lodging) with validation and confirmation from CSD Division, MeitY.	

Annexure I

List of Standards / Guidelines

a) **ISO/IEC 17025** (General requirements for the competence of testing and calibration laboratories).

b) **ISO/IEC 27037** (Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence)

Reference Standards:

a) **ISO/IEC 27041** (Information technology - Security techniques - Guidelines on assuring suitability and adequacy of incident investigative methods)

b) **ISO/IEC 27042** (Information technology - Security techniques - Guidelines on for analysis and interpretation of digital evidence)

c) **ISO/IEC 27043** (A Standard on Information technology - Security techniques – Incident investigation principles and processes within which forensics generally occur)

d) **ISO/IEC 27038** (Information technology - Security techniques – Specification for digital redaction)

e) **ISO/IEC 27040** (Information technology - Security techniques – Storage Security)

f) **ISO/IEC 30121** (A Standard on Information technology – Governance of Digital Forensic Risk Framework)

ANNEXURE – II

Application Form for

Notification of Department / Body / Agency of the Central Government or a State Government as an

Examiner of the Electronic Evidence

Note **(Kindly go through the instructions before filling up the Application form)**

1. *Strikeout whichever is not applicable and Application form should be filled up in capital letters.*
2. *Kindly attach a separate sheet, if the space provided is insufficient.*
3. *If the rows provided in any of the tables are insufficient, the same may be increased as per requirement.*
4. *Authorised Signatory is required to put signatures on all the pages of the form and the documents being submitted along with the form.*
5. *MeitY may seek more information as and when required and may request for technical presentation at MeitY.*
6. *Any information found to be incorrect then the application would be rejected immediately.*

1. Laboratory Name

_____

2. Full Address

_____

_____

P
I
N

3. Contact Number (s), website, email (with STD Code)

   _____

4. Department's / Agency's profile & information brochure, if any, kindly attach: Attached / Not Attached:

   _____

5. Name of the Contact Person:

   _____

6. Designation:

   _____

7. Mobile

   _____

8. Phone:

   _____

9. E-Mail ID:

   _____

10. Electronic Evidence Examination related activities are being carried out since (mm/yy) : __ / ___.

11. **Scope of Areas** which require the notification as Examiner of electronic evidence under the scheme :

Sl.	Area of Digital Forensic Investigation	Mark tick '✓' in case applicable or else mark cross 'X'	Brief about the applicable Scope of Area (Pls provide the detailed scope clearly specifying the capabilities limits, exclusions if any, such as files, formats etc. , use a separate addition sheet if required)
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

12. Detailed **Organisation Chart as** relevant to the scope of areas applied. (Parent Ministry / Department and its relation with the applicant laboratory).

13. Copy of the order/notification establishing the digital forensic lab.

14. Network diagram and cyber security practices to safeguard digital assets and data.

15. "**Quality System Manual" or equivalent document (as available) :**

Reference Number and current version and date : _____/_____/_____

16. Whether **"Quality System Manual" or equivalent document** address the scope of areas (applied for notification) [Please indicate details]_____

17. Do the **Quality System** have following SOPs(Standard Operating procedures) corresponding to each the scope areas as :

- Case Acceptance
- Handling of exhibits and chain of custody
- Security and preservation of exhibits
- Analysis / examination of exhibits
- Electronic Evidence Analysis Reporting
- Tools and Equipment operation, handling and maintenance
- Training (Internal)
- Internal audit and management reviews
- Risk assessment
- Any other procedure

(The SOPs may not be separate for each of the above listed activity)

18. Lab Details:

(i) Area exclusively allocated to Electronic Evidence Laboratory (Range Recommended is 48-64 square feet per Experts):

(ii) No. of Fire-Resistant Cupboards / Safes for exclusively reserved for storage of original electronic exhibits:

(iii) No. of Work desks in rooms / cabins for digital forensics related work:

(iv) Power Backup and other infrastructure details including Heating, Ventilation and Air Conditioning (HVAC):

(v) Infrastructure available for storage and archival of exhibits.

19. Number of Expert Opinions provided by the Department/Agency related to electronic evidence in last three years:__

20. Details of Accreditations / Recognitions (International / National) Received (Enclose Certificates):……..

S.No	Details of the Accreditations / Recognition (National / International)		Validity Upto
	Accreditations / Recognition Agency	**Scope Relevant to Electronic Evidence**	
1.			
2.			
3.			

21. Detailed information of persons involved in examination and/ or reporting of digital forensic cases including who is reporting officer and reviewing officers scope wise:

A. Area of Scope 1: e.g. Mobile Forensics

S. No.	Expert's Name, Designation including Role & Functions within the organisation	Working with the organisation since (Year & Months)	Highest Academic Qualification with main subject(s)	Relevant Professional Qualification (including training)	Total experience (in years) of handling cases of digital forensic examination	Total experience (number of cases) of handling in digital forensic examination	Whether Experts is regular/ Contractual (Attach details) (P/C)	Whether Security clearance of Experts is received (Attach details) (Y/N)
1.								
2.								
3.								

B. Area of Scope 2 : e.g. Computer Media Forensics

S. No.	Expert's Name, Designation including Role & Functions within the organisation	Working with the organisation since (Year & Months)	Highest Academic Qualification with main subject(s)	Relevant Professional Qualification (including training)	Total experience (in years) of handling cases of digital forensic examination	Total experience (number of cases) of handling in digital forensic examination	Whether Experts is regular/ Contractual (Attach details) (P/C)	Whether Security clearance of Experts is received (Attach details) (Y/N)
1								
2								
3								

Repeat above table for any other scope being claimed.

22. Proficiency Testing (Inter / Intra/ External) details in last 3 years

Sl. No.	Scope and Details of Testing	Details of examination	Date of Testing	Nodal Laboratory / Proficiency Testing Provider (if PT provider is Accredited please provide the details)	Performance details	Corrective Action Taken (if any)
1						
2						
3						

23. List of forensic Tools including Toolkits and Equipment being utilised during the examination of the electronic evidence:

S. No.	Name of the Forensic S/w Tool / H/w Tool/ Toolkits and Equipment including version	Whether the tool / toolkit is freeware or commercial	Validity of License (date of Purchase and Date till when updates/amc will be provided) of Commercial S/w Tool	Functions of the Tool (in brief)	Mechanism for renewal of S/w Tool License
1.					
2.					

STATUTORY DECLARATION and INDEMNITY

The information stated herein as well as in the annexed documents is true to the best of my knowledge & belief and nothing has been concealed or falsely stated.

And

MeitY will not be responsible for any mishandling of evidence, negligence in forensic investigation or harm caused to any party because of any misrepresentation of its notification, name and logo by the intermediary or any other interested party. The notified Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence will indemnify MeitY against any misuse of MeitY Name and Logo. For any misuse of MeitY name and logo, the notified organizations themselves will be held responsible. MeitY will take necessary actions for such cases. The notified organisations will not use the Name of MeitY and its Logo, to promote their interest in any manner in any programme not connected / related or being undertaken for MeitY.

Place: Signature of Authorised Signatory with Organisation's Seal

Date:

List of Enclosure(s):

1. Application form
2. Department's / Agency's profile & information brochure as required in point No. 4
3. Detailed Organisation Chart as required in point No. 11
4. Quality Manual as required in point No. 12
5. Network diagram and cyber security practices in point 13.
6. SOPs as required in point No. 17
7. Lab's infrastructure Details as required in point No. 18
8. Accreditation Details and certificates as required in point No. 20
9. Expert's details as required in point No. 21
10. Proficiency Testing details as required in point No. 22
11. Tools Detail as required in point No. 23
12. Any other (Please specify)

Send scanned copy of form and enclosures through email to MeitY

Annexure III

(List of Documents to be submitted **annually i**n the beginning of each calendar year latest by 31st January.)

a. Addition / deletion of scope of activities
b. Addition/deletion of skilled staff
c. Details of licensed tools/software
d. Validity / updation of tools and Technology
e. Number of cases referred to by the prosecuting agency/court (details along with case title)
f. Number of cases handled and reports filed before the court
g. Number of times, examiner appeared before the court as an expert (give case title)
h. Observation including any strictures passed by the Courts
i. Number of cases pending, nature and reasons of pendency /
j. Number. of refused due to lack of requisite skills
k. Proficiency Testing details during the period
l. Self-declaration w.r.t continued compliance to ISO/ IEC 17025 & iso 27037.

The above list is indicative and minimum required to be submitted every year or as specified by MeitY.

All such documents submitted to MeitY to be marked as confidential.

Annexure - IV

Minimum Qualification /Experience / Training for investigation of Digital Forensics cases at the applicant Forensic Labs

1. **Technical Assistant / Technical Officer:**

   B.E/B.Tech/M.Sc /M.Tech/M.E./M.S. in Science or Engineering in relevant area (Computer Science / Computer Application /IT/ Electronics / Forensic Science) from a recognized University.

   +

   Minimum 6 Months training in the relevant area of Digital Forensics / Computer Forensics from a reputed Govt recognised Institute (may include on the job training)

   Or

   B. E / B. Tech with specialization in Information Security and/or Digital Forensics / Computer Forensics or Higher Degree (M. Tech/M.E./M. S / Ph.D.) with specialization in Information Security and/or Digital Forensics / Computer Forensics or Higher Degree from a recognized University.

   +

   Minimum 3 Months training in the relevant area of Digital Forensics / Computer Forensics (may include on the job training)

Desirable: Qualified Forensic Aptitude and Caliber Test (FACT) / FACT+ in Digital Forensics/Computer Forensics/Cyber Forensics.

2. **Reporting Officer (Permanent Officer in Government Service):**

B.E / B.Tech / M.Sc or higher (M.Tech/M.S./M.E./PhD) in Science or Engineering in relevant area (such as Computer Science / IT / Computer Application / Electronics / Forensic Science) from a recognized University.

+

Minimum of 1 years of experience in the relevant area of Digital Forensics / Computer Forensics

+

Minimum 3 Months training in the relevant area of Digital Forensics / Computer Forensics (may include on the job training)

Or

Graduate in Science or Engineering from a recognized University.

+

Domain Expertise (including Banking/ income Tax, etc.) of at least 7 years should have prepared and signed at least 100 forensic reports in domain of Digital Forensics.

+

Minimum 3 Months training from Government Recognised institutes in the relevant area of Digital Forensics/Computer Forensics

Or

B.E / B.Tech with specialization in Information Security and/or Digital Forensics / Computer Forensics or Higher Degree (M.Tech/PhD) with specialization in Information Security and Digital Forensics / Computer Forensics or Higher Degree from a recognized University.

+

Minimum of 6 months of experience in the relevant area of Digital Forensics / Computer Forensics

+

Minimum 3 Months training in the relevant area of Digital Forensics / Computer Forensics

3. **Reviewing Officer**

One year experience as Reporting Officer.