Request for Proposal

"TENDER FOR PURCHASE OF HARDWARE, SOFTWARE ,TOOLS AND SETTING UP OF CYBER FORENSIC TRAINING LAB IN SIKKIM POLICE UNDER THE CCPWC SCHEME."

(Bidders are requested to attach only relevant documents with the technical bid.)

Tender Reference: 01/CB-CID/19

Dated: 24th December 2019

OTHER IMPORTANT DATES

1.	Start download of tender document	24th Dec 2019
2.	Start Date of submission of bid at 9.00 AM	26th Dec 2019
3.	Bid submission closing date till 5.00 PM	24th Jan 2020
4.	Tender opening date.	27th Jan 2020

Crime Investigation Department

Sikkim Police

Sikkim Police Headquarters, Gangtok

Contact Address:

Director General of Police.

Sikkim Police Headquarters, Gangtok.

Phone:03592-202087

E-mail: spcid@sikkimpolice.nic.in

DISCLAIMER

This Request for Proposal (RFP) contains brief information about the project, qualification requirements and the selection process for the successful applicant (bidder). The purpose of this RFP document is to provide applicants (bidders) with information to assist the formulation of their bid application (the "application").

Whilst the information in this RFP has been prepared in good faith, it is not and does not purport to be comprehensive or to have been independently verified. Neither the CID/SIKKIM POLICE nor any of its officers or employees, nor any of their advisers nor consultants accept any liability or responsibility for the accuracy, reasonableness or completeness of the information contained in the RFP, or for any errors, omissions or misstatements, negligent or otherwise, relating to the proposed project, or makes any representation or warranty, express or implied, with respect to the information contained in this RFP or on which this RFP is based or with respect to any written or oral information made or to be made available to any of the recipients or their professional advisers and, so far as permitted by law and except in the case of fraudulent misrepresentation by the party concerned, and liability therefore is hereby expressly disclaimed.

The information ('Information') contained in this RFP document or subsequently provided to interested parties (the "applicant(s)), in writing by or on behalf of CID/SIKKIM POLICE is provided to applicant(s) on the terms and conditions set out in this RFP document and any other terms and conditions subject to which such information is provided.

Each applicant should perform their own due diligence to check the accuracy, reliability and completeness of the information in this RFP document and obtain independent advice from appropriate sources. Submission of bid application shall be deemed to have been done after careful study and examination of the RFP with full understanding of its implications.

The response to this RFP should be full and complete in all respects. Incomplete or partial bids shall be rejected. The applicant must quote for all the items asked for in this tender. Intimation of discrepancies in the RFP, if any, should be given to the office of the CID/SIKKIM POLICE immediately by the applicants. If CID/SIKKIM POLICE receives no written communication, it shall be deemed that the applicants are satisfied that the RFP document is complete in all respects.

This RFP document is not an agreement and is not an offer or invitation by CID/SIKKIM POLICE to any other party. The terms on which the project is to be developed and the right of the successful applicant shall be as set out in separate agreements. CID/SIKKIM POLICE reserves the right to accept or reject any or all applications without giving any reasons thereof. CID/SIKKIM POLICE will not entertain any claim for expenses in relation to the preparation of RFP submissions.

Contents

DISCLAIMER 2

1. Project Introduction 4

1.1. Background 4

1.2. Data Sheet 5

2. Scope of Work 6

3. Terms & Conditions 7

3.1. Accountabilities 7

3.2. Tender Fee 10

3.3. Earnest Money Deposit 10

3.4. Performance Security Deposit 10

3.5. Payment Terms 11

3.7 Selection Procedure 12

3.8 Pre Qualification Bid Criteria 14

3.9 Technical Evaluation Criteria 15

3.10 Penalty 15

3.11 General Terms and Conditions of the RFP 16

3.12 Language of the Bid 16

3.13 Period of validity of the Bid 16

3.14 Bid Due Date 16

3.15 Bid Currency 16

3.16 Contacting CID/SIKKIM POLICE 17

3.17 CID/SIKKIM POLICE right to Accept Bid and to Reject Bids 17

3.18 Lack of Information to Bidder 17

3.19 Fraudulent & Corrupt Practice 17

3.20 Disqualification 17

3.21 Termination 18

3.22 Risk Distribution 18

3.23 Award of Contract 20

3.24 Tender Document 21

3.25 Preparation of Bids 21

ANNEXURE-I: Technical Bid Formats 22

ANNEXURE-II: Financial Bid Format 24

ANNEXURE-III: Proposal Covering Letter 25

ANNEXURE-IV: Required Cyber Forensics Tool List 27

1. Project Introduction

1.1. Background

The Sikkim Police Crime Branch, Crime Investigation Department (CB-CID) is amongst the most important units of the Sikkim Police organization. The Crime Branch is primarily and chiefly concerned with matters pertaining to crime, investigation, prosecution and collection of criminal intelligence.

The CB-CID is a specialized branch which tackles the various crime related issues at micro level and therefore is structured into various cells, units and sections. One of the important cell which operates under this is the Cyber Crime cell.

In order to solve the various cyber crimes taking place in the State of Sikkim, a cyber forensic training lab is proposed to be setup at Sikkim Police Headquarters at Gangtok. This lab shall be used for capacity building in the field of Cyber forensics for select units of Sikkim Police. To setup the lab and start with the capacity building programs related to this field, appropriate tools related to Cyber forensics needs to be procured by Sikkim Police.

The objective of publishing this RFP (Request for Proposal) by Sikkim Police is to identify an efficient vendor to supply the appropriate cyber forensic training tools and to assist establish the aforementioned cyber forensic training lab and to provide training on those tools.

Bidders are required to submit quotations for supplying appropriate cyber forensic tools required to setup the training lab at Sikkim Police Headquarters, Gangtok. An indicative list of tools required to be supplied is attached in Annexure-IV.

1.2. Data Sheet

Sl. No.	Item	Details
1.	Project Name	Selection Of Firm For Setting Up Of Cyber Forensic Training Lab
2.	Bid Inviting Authority	DGP/SIKKIM POLICE, Sikkim Police HQ, Gangtok–737101, Sikkim
3.	Contact person of the bid	Superintendant of Police/CID, Sikkim Police HQ Email: spcid@sikkimpolice.gov.in
4.	Tender Reference with Date	Ref No: 01/CB-CID/19 Date:24th Dec 2019
5.	Submission of Queries and Bid.	Address for submission of queries and Bid: SP-CID OFFICE, Sikkim Police HQ, Gangtok
6.	Publication of Corrigendum (if any) on website on the basis of Pre-Bid queries	All corrigendum issued by CID/Sikkim Police in this respect will be given without disclosing the name of interested bidders.
7.	Cost of tender Document (non-refundable)	Rs.20,000/- (Rupees Twenty Thousand only) in the form of a Demand Draft/Pay Order/ Account Payee Banker's Cheque drawn on any Nationalised/Scheduled bank in favour of "Director General of Police, Sikkim Police", payable at Gangtok.
8.	Earnest Money Deposit (EMD) (refundable)	Rs. 3,70,000/- (Rupees Three Lacs Seventy Thousand only) in the form of a Demand Draft on any Nationalised/Scheduled bank in favour of "Director General of Police, Sikkim Police", payable at Gangtok. The validity of the EMD is 90 days. Bid security shall be refunded to the successful bidder upon signing of contract/agreement with client. For unsuccessful bidders, the bid security shall be refunded after end of the overall bid process.
9.	Performance Security Deposit	5% of the Contract Value in the form of Demand Draft on any Nationalised/Scheduled bank in favour of "Director General of Police, Sikkim Police", payable at Gangtok.
10.	Last date and time of submission of Bid	24th January 2020
11.	Date and Venue for opening of bid	27th January 2020, Conference Hall, Head Quarter,Sikkim Police, Gangtok at 11:00 am .

Note:

* No financial information should be submitted under technical bid.

*The bidder shall bear all costs associated with the presentation and submission of the tender and CID/SIKKIM POLICE will, in no case, be responsible or liable for those costs, regardless of the conduct or the outcome of the bidding process.

2. Scope of Work

The minimum specified Scope of Work that needs to be undertaken by the bidder for supply of equipment and setup of the lab and support during the course of the project is given below and the work is to be performed as per the specifications and conditions mentioned in different parts of this document. Any further amendments issued in this regard and the Contract is to be signed and adhered by the Bidder respectfully.

1. Supply of appropriate Cyber Forensic tools along with the requisite software required for setup of Cyber Forensic training lab:

   An indicative list of the requirements is as below. For detailed list of tools required to setup training lab along with the individual quantities please refer **Annexure-IV**:

Sr. No	Name of items
	Basic Cyber Forensic Tools
1.	CDR Analysis Software (Academic Version)
2.	Disk Forensic Tool /Live Forensic/Network Forensic /Memory Forensic/ Registry Forensic and Remote Forensic Tool
3.	Mobile Forensic Tool
4.	SATA/IDE Write Blocker
5.	Pen Drives
6.	Card Readers
7.	Smart Phones
8.	Hard Disk
9.	Social Media Analysis Tool
	Other Cyber Forensic Tools
10.	Hardware Disk Imaging and Drive Wiper Tool
11.	Steganography Detection tool
12.	GPS Forensic
13.	Password Recovery Tool
14.	Video Forensic and CCTV analysis
15.	Data Recovery from Damaged hard disk
16.	Malware Analyzer
17.	Training Laptops with extra wireless keyboard and mouse.
18.	Trainer Laptop (Windows 10 Pro OS).
19.	Workstation for Practical .
20.	Smart Podium .
21.	LED Touch Screen 85'' and More
22.	Portable digital evidence seizure kit for IO's.
23.	Multi Function Printer
24	Digital Pointer
25.	Furnishing and Renovation of existing cyber lab.
26.	Biometric and card controlled door access system.
27.	Electric work and Networking with all necessary equipments

2. Setting up of the Cyber Forensic Training lab

3. Training the nominated Sikkim Police personnel on the installed Cyber Forensic tools with necessary certification and focus on hands-on practice.

4. Provide maintenance and support for the installed hardware and tools in the lab for minimum 3 to 5yrs.

3. Terms & Conditions

3.1. Accountabilities

(i) Payment of money as advance & balance amount will be made as per mutually agreed upon conditions between Sikkim Police & vendor. This will be subject to quality and performance of the work executed under the supply order.

(ii) The supply, installation & commissioning will be done within a mutually agreed upon stipulated time frame w.e.f. the date of awarding the work order. Failure to adhere to the specified time frame will incur a penalty which will be decided at the time to stipulating the above time frame.

(iii) The rates shall be inclusive of GST, freight & other applicable taxes etc. Including any unforeseen liability that may be incurred for satisfactory & proper installation of hardware, peripherals, software and other equipment required for the project.

(iv) The total installed & commissioned solution in Sikkim Police HQ should have a minimum of three years warranty with scope of extension of warranty to five years starting from the date of commissioning and handing over the fully completed lab to CID, Sikkim Police. Support and maintenance which will include repair & replacement of faulty parts during routine operations.

(v) The hardware & software supplied against this work order must include all the modules, sub modules and items required for installation, smooth performance and crash recovery of the software such as installation kit, CDs, Software Manuals, hardware sub-systems etc.

(vi) Vendor shall guarantee that the equipment quoted and supplied shall not be obsolete or proclaimed as 'End of Sale' by the Original Equipment Manufacturer (OEM) during the warranty period & that the equipment shall be supported with necessary spares during the warranty period and beyond. The model should not be nearing its life cycle end where the OEM is already planning a market release of a newer version in the next six months or a year.

(vii) Vendor shall supply complete set of technical/operations & maintenance manuals as applicable along with the delivery. The cost of such manuals supplied will be included in the cost of the system.

(viii) Supply of unauthorized /pirated /sub-standard /Refurbished /Used or Old hardware /peripheral /software /equipment detected at any date during or after warranty shall be notified to the vendor in writing. Such equipment or items shall be replaced forthwith by vendor at its own cost. Any penalty or litigations arising out of such supplies shall be the responsibility of the vendor.

(ix) Software Updates, License, Service Packs & Patches: All relevant and applicable Software, Operating Systems etc. Shall be updated at the time of installation with all the released patches and service packs. The above shall be applicable during the guarantee/warranty period free of any additional cost.

(x) Vendor shall clearly specify & highlight recurring expenses on licenses of commercial COTS or any other item procured for the project including justification of the product procurement viz-a-viz any similar freeware or open source alternative if available.

(xi) Vendor shall explicitly mention the OEM or Distributors of the schedule of items quoted in the bid proposal. In the case of Distributors/Dealers the vendor should attach a valid Proof of Dealership/Distributorship of the supplier for the item procured.

(xii) Post receipt/pre-installation inspection of the supplied equipment will be done at CID Sikkim Police HQ, Gangtok at the time of delivery of the equipment by the officers of CID , any other officer nominated by the ADGP/CID & technical personnel too:

a) Inspect the goods against any physical damage on delivery
b) Check the goods delivered against the models ordered
c) Reject the items which are not delivered as per the contract or any subsequent modifications to the contract, in terms of make & model
d) Submit a duly signed inspection report to the nodal officer for further action

(xiii) **Support & Maintenance**: The client support & maintenance for the tools supplied should be effective & prompt with response time of maximum 24 hours to resolve the reported issue, failure to do so will be recorded with due diligence incurring a penalty of Rs. 1000/- per day of delay on the vendor.

(xiv) **Training**: The training on the cyber forensics tools setup at the lab would be imparted to officials and personnel for successful operations of the response system should be well designed, adequate, thorough and intensive with focus on hands-on practice, the training shall be conducted by experienced trainers for the required duration for trainees to be fully conversant with the system and their individual roles. Also there will be training of trainers for 5 officers with necessary certification (preferably OEM certification)

(xv) Training shall be followed by hand holding of staff for adequate duration in the initial phase of real time operation by which time the candidates for future should be identified.

(xvi) **Buyback/Up-gradation facilities**: Due to rapid changes in technology during relatively short span of time OEMs constantly launch newer versions of products which include hardware, software and peripherals. In cases where the supplied items are in fairly good condition and better versions are launched by the OEM the vendor should accordingly intimate CID, Sikkim Police on time about the newer versions and solicit upgrading existing equipment and technology with the latest versions which should have tangible benefits over the existing ones not limited to just superficial aesthetics and minimal add-ons. The vendor should assist in buy back offers where possible with the OEMs.

(xvii) Existing Equipment, Software Peripherals etc.: Substantial amount of cyber forensics equipment, software peripherals etc. are in possession of the CID/Sikkim Police. Most of these haven't been used even once and in absence of any trained personnel or user manuals have remained unopened in their containers. The vendor should inspect all these equipment, software etc. And assist CID/Sikkim Police to make proper use of them (for training purposes) or if thoroughly obsolete and of no practical use dispose them off in a proper manner.

(xviii) **EXPERIENCE**: The Vendor should have executed such work under CCPWC scheme of MHA for at least one State/UT Police and more than 3 years experience in the cyber forensics field. Experience certificates from clients where the vendor has supplied similar equipment and solutions should be furnished to CID/Sikkim Police.

(xix) Dispatch of Documents: Copy of the Delivery Challan, bill along with customer/user certified Installation/Commissioning Report needs to be maintained.

(xx) It is the vendor's responsibility to ensure that the Project Manager (PM)/ or any other authorized person in full knowledge of the project and the matter under discussion is available to meet with SP/CID provided that the meeting relates to the work proposed and/or the objectives proposed.

(xxi) It is the Vendor's responsibility to ensure that all objectives proposed and all deliverables proposed are achieved and disclosed prior to the agreed end-date of the project.

(xxii) It is the Vendor's responsibility to ensure any information it possesses relating to CID/Sikkim Police that is not available in the public domain be treated with the utmost confidentiality and discretion.

(xxiii) Where the Vendor feels the need to disclose confidential information to a third party, it is their responsibility to ensure that it does so with the explicit permission of CID/Sikkim Police.

3.2. Tender Fee

Tender document fee of Rs.20,000/- (Rupees Twenty Thousand only) in the form of Demand Draft in favour of "Director General of Police, Sikkim Police", payable at Gangtok should be submitted along with the Technical bid.

3.3. Earnest Money Deposit

(i) An earnest money deposit (EMD) of INR Rs. 3,70,000/- (Rupees Three Lacs Seventy Thousand only) in the form of Demand Draft in favour of "Director General of Police, Sikkim Police", payable at Gangtok, shall have to be submitted by the bidders' along with the bid. The EMD shall be furnished in Indian National Rupees (INR) and should be valid for a period of minimum 90 days.

(ii) Any bid not secured in accordance with above mentioned clause, shall be rejected by the Purchaser as being non-responsive, without any further correspondence. Unsuccessful bidders' EMD will be discharged / returned after end of the overall bid process.

(iii) Earnest Money Deposit furnished by selected Bidder shall be refunded after signing of contract and submission of Performance Security Deposit. The EMD can be forfeited if a Bidder withdraws its bid during the period of bid validity specified by the Bidder on the Bid Form or during the bid process, if a Bidder indulges in any such deliberate act that would jeopardize or unnecessarily delay the process of bid evaluation and finalization, or if any information is found wrong / manipulated / hidden in the bid.

(iv) The decision of the Purchaser regarding forfeiture of the EMD shall be final & shall not be called upon question under any circumstances. No interest will be paid on the EMD.

3.4. Performance Security Deposit

(i) The successful bidder shall at his own expense deposit with the CID/SIKKIM POLICE, within fifteen (15) working days of the date of notice of award of the contract or prior to signing of the contract whichever is earlier in the form of Demand Draft on any Nationalised/Scheduled bank pledged in favour of "Director General of Police, Sikkim Police", payable at Gangtok.

(ii) This Performance Security Deposit will be for an amount equivalent to 5% of contract value. All incidental charges whatsoever such as premium; commission etc. with respect to the performance security deposit shall be borne by the bidder. If the accepted Bidder fails to furnish the Performance Security Deposit within the above said period, the EMD remitted by him will be forfeited to the SIKKIM POLICE and his tender will be held void. The Performance Security Deposit furnished by the Bidder in respect of his tender will be returned to him at the end of the contract period subject to submission of all reports to satisfaction.

(iii) If the Bidder failed to act up on to the tender conditions or backs out when his tender is accepted, his Performance Security Deposit mentioned above will also be forfeited to the CID/SIKKIM POLICE.

3.5. Payment Terms

Sl. No.	Milestone / Deliverable	Payment
1.	**Completion of delivery of the cyber forensic tools**	**40% of contract value**
2.	**Successful setup of Cyber Forensics Lab**	**30% of contract value**
3.	**Successful completion of training of all nominated Sikkim Police personnel**	**30% of contract value**

3.6 Procedure for submission of bids

a) It is proposed to have a Three Cover for this tender:

Pre-Qualification Bid – (2 copies) in one cover

Technical Bid - (2 copies) in one cover

Commercial Bid - (2 copies) in one cover

b) Pre-Qualification Bid, Technical Bid and Commercial Bid of the Tender shall be covered in separate sealed covers super-scribing "Pre- Qualification Bid", "Technical Bid", "Commercial Bid". Each Bid shall also be marked as "Original" and "Copy". Please Note that Prices shall be indicated only in the Commercial Bid. And if price will be indicated in the Pre-Qualification Bid or Technical Bid, that Bid is liable to be rejected.

c) The three envelopes containing Pre-qualification Bid, Technical Bid and Commercial Bid shall be put in another single sealed envelope clearly marked "**Selection Of Firm For Setting Up Of Cyber Forensic Training Lab**" These envelopes are to be superscripted with Tender Number and the wordings "DO NOT OPEN BEFORE 11.00 AM **on 27/01/2020** "

d) The cover thus prepared shall also indicate clearly the name, address, telephone number, E-mail ID and fax number of the Bidder to enable the Bid to be returned unopened in case it is declared "Late".

e) Each copy of the tender shall be a complete document and shall be bound as a volume. The document shall be page numbered and appropriately flagged and must contain the list of contents with page numbers. Different copies must be bound separately. Any deficiency in the documentation may result in the rejection of the Bid.

f) As part of the Bid, Bidder shall also provide the Pre-Qualification Bid and Technical Bid in Soft Copy (PDF Format), in the form of a non rewriteable CD (Compact Disc) as follows:
   i. Two (2) copies of CD each containing the Pre-Qualification Bid and Technical Bid - The CDs containing Bids shall be sealed along with the hard copies of the respective Bids
   ii. All CDs submitted by the Bidder must be in sealed covers. The sealed covers as well as the CD media must be duly signed by the Bidder using a "Permanent Pen/Marker", shall be super-scribed with "Technical Bid- Soft Copy (PDF Format) / Pre-Qualification Bid -Soft Copy (PDF Format)" (as the case may be) and shall bear the name of the Bidder
   iii. Bidder must ensure that the information furnished by him in respective CDs is identical to that submitted by him in the original paper Bid document. In case of any discrepancy observed by the State in the contents of the CDs and original paper Bid documents, the information furnished on original paper Bid document will prevail over the soft copy
   iv. Bidder must ensure that Pre-Qualification and Technical Bid CDs do not contain any Commercial items / prices

g) If the outer envelope is not sealed and marked as indicated above, State will assume no responsibility for the Bid's misplacement or premature opening
h) The Tender should be signed on all the pages by the Bidder's authorised signatory and should be affixed with the bidder's Seal.
i) The representative participating in the bid process should carry a letter of authorisation on the company letter head.

3.7 Selection Procedure

Only the bidders fulfilling the Pre Qualification Bid Criteria as per Clause 3.8 and scoring 35 marks or above in the Technical Evaluation criteria as per Clause 3.9 are allowed to participate in the Commercial Bid. The envelopes marked "Pre Qualification Bid" shall be opened first. The envelopes marked "Financial Bid" shall be kept sealed and shall be opened only after evaluation of technical bid.

Evaluation of Bid:

For financial evaluation, the total cost indicated in the Financial Bid including all Taxes will be considered.
The Lowest financial bid will be allotted a financial mark of 100 marks. The financial marks of other Bidder(s) will be computed by measuring the respective financial bids against the lowest financial bid.

$$\text{Financial Marks (MF)} = \frac{\textit{Lowest Financial Bid Amount}}{\textit{Bidder's Actual Financial Bid Amount}} \text{ X } 100$$

Combined and Final Evaluation:

The composite mark is a weighted average of the Technical and Financial Marks. The ratio of Technical (MT) and Financial mark is 80:20 respectively. The Composite Mark will be derived using the following formula:

Composite Mark= (MT X 0.8 + MF X 0.2)

Thus, the composite mark shall be out of a maximum of 100 marks. The responsive Bidder(s) will be ranked in descending order according to the composite marks, which is calculated based on the above formula. The highest-ranking Bidder as per the composite mark will be selected in this tender.

3.8 Pre Qualification Bid Criteria

The bidders must enclose the following documents inside the pre qualification bid envelope:

Sl. No.	Criteria	Documents required
1.	The Bids shall be submitted by only the Bidder; no consortium is allowed in this Bid	Declaration in this regard needs to be submitted
2.	The bidder should have been in existence as a cyber forensics firm /company for the last 3 years (as on 1st December 2019).	Registration of firm, trade license, GST registration and professional tax clearance certificate.
3.	The Bidder should have the financial statement audited by the Chartered Accountant for the last financial year i.e 2018-2019	Copy of audited profit and loss account/balance sheet/annual report of the last financial years viz.2018-2019
4.	The bidder should have executed such work for at least one State/UT Police	Work Orders to be enclosed.
5.	The bidder should have a well established office in India.	The address proof of the office, website and salary certificates of the cyber forensics knowledgeable personnel along with their Curriculum Vitae as per format 2 of Annexure I should be submitted
6.	Bidder should NOT be under a declaration of ineligibility for corrupt and fraudulent practices issued by the tendering authority.	Self declaration certification to be submitted
7.	The Bidder shall furnish, as part of its Bid, an Earnest Money Deposit (EMD) of Rs.3,70,000/-Three Lac Seventy Thousand. and TENDER FEE of Rs 20,000/- (Twenty Thousand only) in the form of a DD in the favor of "Director General of Police, Sikkim Police", payable at Gangtok." No Bank Guarantee would be entertained for the same.	The EMD shall be denominated in Indian Rupees.

Note:

(i) The tender fee and EMD to be submitted in original as mentioned in this RFP
(ii) Bidders must provide supporting documents for the eligibility criteria as mentioned against each criterion and in the same order.
(iii) Bidders shall provide its proposal covering letter as per format of Annexure-III, organizational details as per Format 1 of Annexure-I.

3.9 Technical Evaluation Criteria

The eligible bidders shall be evaluated based on the following criteria and technical mark shall be awarded to the bidders. The bidder needs to score at least 35 marks or above out of a total of 50 marks to be able to qualify for commercial/financial bid opening.

S. No.	Clause	Marks scored
1.	Presentation on the experience of the vendor and specific expertise in the field of Cyber forensics	10 marks
2.	Presentation on the cyber forensic tools proposed to be supplied for setting up of the lab	10 marks
3.	Innovative technologies/uniqueness of the proposed solution	10 marks
4.	Presentation of the training methodology for imparting knowledge of the system to the nominated Sikkim Police officials and certification.	20 marks

3.10 Penalty

Penalty will be deducted in the case of bidder not meeting the Project timelines as per clause 1.2. The modalities of penalty are as mentioned below.

Delay vis-à-vis Project Timelines	Penalty
Delay of 1 week	5% of the contract value
Delay of 2 weeks	10% of the contract value
Delay of 3 weeks	20% of the contract value
Delay of more than 3 weeks	30% of the contract value
Delay of more than 5 weeks	50% of the contract value

3.11 General Terms and Conditions of the RFP

The following general terms and conditions shall apply:

(i) This RFP may be cancelled without assigning any reasons, thereof, at any time.

(ii) If any date mentioned in this RFP is declared as a public holiday, the schedule shall be shifted to the next working day.

(iii) The undersigned reserves the right to cancel any or all of the bids without assigning any reasons thereof.

(iv) The undersigned reserves the right not to award the bid to the bidder selected on the basis of the selection procedure without assigning any reason.

(v) In case of any dispute, the jurisdiction of the Courts of Law at **Gangtok** would apply.

(vi) A delay of more than 3 weeks in executing the task to be treated as material breach & the contract may be terminated with a notice of 7 days.

(vii) Arithmetical errors in the Financial Bid will be rectified on the following basis:

a. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and will be considered for future calculations.
b. If there is a discrepancy between words and figures, the amount in words shall prevail
c. If the bidder does not accept the correction of errors, its bid will be rejected and its EMD may be forfeited.

3.12 Language of the Bid

The bid prepared by the bidder, as well as all correspondence and documents relating to the Bid exchanged between the bidder and CID/SIKKIM POLICE shall be in English.

3.13 Period of validity of the Bid

The bid shall remain valid for 180 days from the date of submission of Proposal being specified. Bidder should ensure that in all circumstances, its Bid fulfils the validity condition. Any bid valid for a shorter period shall be rejected as non- responsive.
In exceptional circumstances, CID/SIKKIM POLICE may solicit bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing or by Fax. Bid Security shall also be suitably extended. A bidder granting the request is neither required nor permitted to modify the bid.

3.14 Bid Due Date

The Bid Due date is mentioned in the schedule of events. The Technical Committee, CID/SIKKIM POLICE may, in exceptional circumstances and at their discretion, extend the deadline for submission of proposals by issuing an Addendum/Corrigendum online through the website. However, till such communication is received by the bidders, bidders may not assume any change in the schedule.

3.15 Bid Currency

Prices for services offered shall be quoted in Indian National Rupees only.

3.16 Contacting CID/SIKKIM POLICE

Bidder shall not approach CID/SIKKIM POLICE officers beyond office hours and or CID/SIKKIM POLICE office premises, from the time of the Bid opening to the time of finalization of successful Bidder.

Any effort by a Bidder to influence CID/SIKKIM POLICE officers in the decisions on Bid evaluation, Bid comparison or finalization may result in rejection of the Bidder's offer. If the Bidder wishes to bring additional information to the notice of the CID/SIKKIM POLICE it should do so in writing.

3.17 CID/SIKKIM POLICE right to Accept Bid and to Reject Bids

1. Prior to expiration of the period of Bid validity, CID/SIKKIM POLICE will notify the successful bidder in writing that its Bid has been accepted.
2. CID/SIKKIM POLICE will issue Letter of Intent (LOI) to successful bidder.
3. Within 7 days of receipt of such LOI, the successful bidder shall give its acceptance to the CID/SIKKIM POLICE. After the receipt of Acceptance letter from successful bidder CID/SIKKIM POLICE shall issue Work Order (WO) and sign an agreement with the successful bidder within 30 days.
4. The CID/SIKKIM POLICE has the right to reject any or all of the bids without giving any reasons what so ever prior to the awarding of the contract.
5. In case of the single bid received or in case of single bidder qualifying for the opening of the technical bid, CID/SIKKIM POLICE reserves the right to accept or reject the single bid.

3.18 Lack of Information to Bidder

The bidder shall be deemed to have carefully examined RFP document to his entire satisfaction. Any lack of information shall not in any way relieve the bidder of his responsibility to fulfil his obligation under the bid.

3.19 Fraudulent & Corrupt Practice

"Fraudulent Practice" means a misrepresentation of facts in order to influence a Bidding process or includes collusive practice among bidders (prior to or after Bid submission) designed to derail the fair practices by CID/SIKKIM POLICE and to deprive the CID/SIKKIM POLICE of the benefits of free and open competition.

"Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value, pressurizing to influence the action of a public official in the process of project execution. CID/SIKKIM POLICE reserves right to reject the bidder for award if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for, or in executing bid process.

3.20 Disqualification

CID/SIKKIM POLICE may at its sole discretion and at any time during the evaluation of Bids, disqualify any bidder, if the bidder:

1. Submits the Bids after the response deadline.
2. Make misleading or false representations in the forms, statements and attachments submitted as proof of the eligibility requirements
3. Exhibits a record of poor performance such as abandoning works, not properly completing the contractual obligations, inordinately delaying completion or financial failures, etc. in any project in the preceding three years.

4. Submits a Bid that is not accompanied by required documentation or is non-responsive.

3.21 Termination

1. Termination for Default: If the bidder fails to carry out the award / work order in terms of this document within the stipulated period or any extension thereof, as may be allowed CID/SIKKIM POLICE without any valid reasons acceptable to CID/SIKKIM POLICE may terminate the contract after giving two months notice, and the decision of CID/SIKKIM POLICE on the matter shall be final and binding on the bidder.
2. In case of unavailability of sufficient funds or discontinuation of the project the CID/SIKKIM POLICE reserves all rights to cancel Agreement after the payment of completed and ongoing work under the project.
3 CID/SIKKIM POLICE can terminate the Agreement with a notice of 45 days if the bidder becomes bankrupt and/or becomes insolvent. CID/SIKKIM POLICE in such cases of termination will ensure payment of all services rendered and materials supplied under the Agreement.

3.22 Risk Distribution

Force Majeure	1. For the purpose of this Article, Force "Majeure" means any cause, which is beyond the control of the vendor or CID/SIKKIM POLICE as the case may be, which such party could not foresee or with a reasonable amount of diligence could not have foreseen, and which substantially affect the performance of the Contract, such as:- - War / hostilities - Riot or civil war/commotion - Earth Quake, Flood, Fire, Tempest, Epidemics, Lightning or other natural physical Disaster, Quarantine restricts and Freight embargoes - Restrictions imposed by the Government or other statutory bodies, which is beyond the control of the Bidder, which prevent or delay the execution of the order by the vendor. 2 If a Force Majeure situation arises, the Bidder is required to promptly notify CID/SIKKIM POLICE in writing of such condition and the cause thereof within a period of three (3) days from the date of happening of such an event requiring invocation of this force majeure article. Unless otherwise directed by CID/SIKKIM POLICE in writing, the vendor will continue to perform its obligations under this supply order as far as is reasonably practical and shall seek all reasonable alternative means for performances of this order
Notice Of Force Majeure Event	As soon as practicable and in any case within 7 days of the date of occurrence of a Force Majeure Event or the date of knowledge thereof, the Party which is rendered wholly or partially unable to perform any of its obligations under this Agreement because of a Force Majeure Event ("the Affected Party") shall notify the other party of the same, setting out, inter alia, the following in reasonable detail: a. The nature and extent of the Force Majeure Event; b. The estimated Force Majeure Period; c. The nature of and the extent to which, performance of any of its obligations under this Agreement is affected

	by the Force Majeure Event; d. The measures which the Affected Party has taken or proposes to take to alleviate/ mitigate the impact of the Force Majeure Event and to resume performance of such of its obligations affected thereby; and e. Any other relevant information concerning the Force Majeure Event, and/ or the rights and obligations of the Parties under this Agreement.
Resolution of Disputes and Arbitration	If any dispute or confusion arises, the decision of the third party arbitrator should be abided by all the parties.
Acquaintance with local conditions	Each Bidder is expected to fully get acquainted on his own initiative with the local conditions and factors effecting the implementation before they Bid or submit proposal in response to this RFP. CID/SIKKIM POLICE shall not entertain any request for clarification regarding such local conditions. Neither any change in the time schedule of the contract nor any financial adjustments arising thereof shall be permitted by the CID/SIKKIM POLICE on account of failure of the Bidder to know the local conditions / factors.
Statutory and Regular Approvals	The Bidder shall be responsible for obtaining approvals for any statutory and regulatory requirements from any or all authorities to fulfil the Bid conditions. Further, the Bidder shall be responsible to get required documentation completed for participating in the Bid.
Confidentiality	Any information pertaining CID/SIKKIM POLICE or any other agency involved in the Bid, or matters concerning CID/SIKKIM POLICE that comes to the knowledge of the Bidder in connection with this Bid, will be deemed to be confidential and the Bidder will be fully responsible for confidentiality of all the information held in trust, as also for all consequences of its concerned personnel failing to observe the same. The Bidder shall ensure due secrecy of information and data not intended for public distribution.
Limitation of Liability	The liability of the CID/SIKKIM POLICE for its obligations under the Agreement Signed shall in no case exceed the total value of the Contract.
Failure to Agree with the Terms and Conditions of the RFP	Failure of the successful bidder to agree with the Terms and Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event CID/SIKKIM POLICE may award the project to the next best value Bidder or call for new Bids.
Notices	1. Any notice given by one party to the other pursuant to this contract shall be sent to the other party in writing by registered post or by telex, email or facsimile to the other party's registered office address. 2. A notice shall be treated as effective when the same is delivered to other party in the address provided for

	communication.
Patent Rights	The Bidder shall indemnify the CID/SIKKIM POLICE against all third party claims of infringement of patent, trademark or industrial design and intellectual property rights arising from the use of equipment's and services or any part thereof.
Taxes and Duties	1. All payments will be subjected to tax payment/deduction at source as applicable/required at the prevailing tax rates. 2. CID/SIKKIM POLICE shall not pay any increase in duties, taxes and surcharges and other charges on account of any revision, enactment during the period of validity of the Bids and also during the contract period. The decision of CID/SIKKIM POLICE in this regard will be final and binding and no disputes in this regard will be entertained.
Change orders	1. The CID/SIKKIM POLICE may at any time, give written order to the bidder to make changes for additional functionalities specifically required, but not falling within the general scope of the current RFP/Agreement. If any such change causes an increase in the cost of, or the time required for, the bidder's performance of any provisions under the Contract, the vendor should notify CID/SIKKIM POLICE in terms of the person month efforts required for executing the change requests, CID/SIKKIM POLICE will examine the efforts estimate & agreed efforts will be compensated in terms of person month charges. 2. Any claims by the bidder for adjustment under this clause must be asserted within 90 working days from the date of the bidder's receipt of the CID/SIKKIM POLICE change order.

3.23 Award of Contract

Award of Contract	1. CID/SIKKIM POLICE will award the contract to successful bidder whose bid has been determined to be responsive and has obtained maximum score during bid evaluation in terms of Composite marks. 2. CID/SIKKIM POLICE shall consider placement of Letter of Intent to the selected bidder, that bidder shall give his acceptance and conformity within 7 days of issue of Letter of Intent. 3. The selected bidder shall need to execute an agreement with CID/SIKKIM POLICE within fifteen (15) days from the date of the issue of Letter of Intent. In the event of the failure on the part of the successful bidder to sign the agreement within the above stipulated period, the EMD shall be forfeited and the acceptance of the contract shall be considered as cancelled.

3.24 Tender Document

Bidder is expected to examine all instructions, forms, terms, specifications, and other information in the Tender Document. Failure to furnish all information required by the Tender document or to submit a Bid not substantially responsive to the Tender Document in every respect will be at Bidder's risk and may result in the rejection of its Bid.

3.25 Preparation of Bids

1. Bidder should take into account any corrigendum published on the tender document before submitting their bids.

Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid. Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that need to be submitted. Any deviations from these may Prime to rejection of the bid.

(Sd/-)
DGP, Sikkim Police

ANNEXURE-I: Technical Bid Formats

Format 1: General Information about the Bidder

S. No.	Particulars	Details
1.	Name of the bidder	
2.	Address of the bidder	
3.	Constitution of the bidder	
4.	Name & designation of the contact person	
5.	Telephone No.	
6.	Email of the contact person	
7.	Fax No.	
8.	Website	
9.	Certificate of Incorporation	
10.	No. of years in Cyber Forensics business	
11.	No. of employees having experience in the field of Cyber Forensics	
12.	Technical Certifications obtained	
13.	Income Tax Registration/ PAN Card No.	
14.	Goods & Service Tax (GST) Registration No.	

Format 2: Curriculum Vitae of the Cyber Forensics resources

S. No.	Particular	Details
1.	Name	
2.	Position	
3.	Date of Birth	
4.	Educational Qualification	
5.	Certifications / Trainings	
6.	No. of years of relevant experience	
7.	Key Projects / Responsibilities handled	

Format 3: Project Experience

S. No.	Name of the Project	Department Name & Address	Brief Scope of Work	Project Value (in INR)	Project Period (From – To / Ongoing)	Page Ref. of Supporting Documents in the Technical Bid
1.						
2.						

ANNEXURE-II: Financial Bid Format

Financial Bid Format:

S. No.	Item	Total Price *(in lakhs)*	Total Price in words
1	Setup Cyber Forensics Training Lab		
2	GST		
3	Grand Total		

Note:

(i) The amount quoted shall be inclusive of all taxes, training charges and AMC for minimum three years.

(ii) Income tax will be deducted at source from the payments made as per the law applicable in India.

ANNEXURE-III: Proposal Covering Letter

COVERING LETTER for **"Selection of Agency for Setting up of Cyber Forensics Training Lab at Sikkim Police HQ"**

Date: Reference No.: RFP/……

[Bidders are required to submit the covering letter as given here on their letterhead]

To
The DGP
Sikkim Police
Police Headquarters
Gangtok – 737101, Sikkim

Dear Sir,

We …….. (Name of the bidder) hereby submit our proposal in response to notice inviting tender date …….. and tender document no. …….. and confirm that:

1. All information provided in this proposal and in the attachments is true and correct to the best of our knowledge and belief.
2. We shall make available any additional information if required to verify the correctness of the above statement.
3. Certified that the period of validity of bids is 180 days from the last date of submission of proposal, and
4. We are quoting for all the services mentioned in the tender.
5. We the Bidders are not under a Declaration of Ineligibility for corrupt or fraudulent practices or blacklisted by any of the Government agencies.
6. We are submitting our eligibility documents and technical bid documents along with the following:
    a. A soft format in form of a CD/DVD clearly hyper linking all the relevant scanned documents and highlighting relevant portions of the document for ease of evaluation. This is in addition to the paper documents in hard copy format to be submitted by the bidders and needs to be handed over along with bids.
    b. The hard copy format is also similarly indexed, flagged and highlighted at relevant places.
7. We, the undersigned, having carefully examined the referred RFP, offer to Propose for the selection as a Software developing firm, in full conformity with the said RFP.
8. We have read all the provisions of RFP and confirm that these are acceptable to us.
9. We further declare that additional conditions, variations, deviations, if any, found in our proposal shall not be given effect to.
10. We agree to abide by this Proposal, consisting of this letter, our Technical and Commercial Proposals, and all attachments, for a period of 180 days from the date fixed for submission of Proposals as stipulated in the RFP and modifications resulting from contract negotiations, and it shall remain binding upon us and may be accepted by you at any time before the expiry of that period.
11. Until the formal final Contract is prepared and executed between us, this Proposal, together with your written acceptance of the Proposal and your notification of award, shall constitute a binding contract between us.
12. We declare that we do not have any interest in downstream business, which may ensue from the RFP prepared through this assignment.
13. We hereby declare that all the information and statements made in this proposal are true and accept that any misrepresentation or misinterpretation contained in it may lead to our disqualification.
14. We understand you are not bound to accept any proposal you receive, not to give reason for rejection of any proposal and that you will not defray any expenses incurred by us in bidding.
15. Demand Draft: Draft No. _____ dated _____ drawn on _____ for Rs. 3,70,000/- is enclosed towards EMD.

16. Demand Draft: Draft No. _____dated ___ drawn on _____ for Rs. 20,000/- is enclosed towards RFP document cost.

Signature…….

In the capacity of……

Duly authorized to sign Proposal for and on behalf of……..

Date…….. Place…….

[*: Strike off whichever is not applicable]

ANNEXURE-IV: Required Cyber Forensics Tool List with Technical Specification (to be uploaded with Technical Bid.)

1. CDR Analysis Tool - Academic License (15 users)+ 1 pro license.		
Make:- Model :-		
Technical Specification		**Compliance (Y/N)**
1.	Should be an integrated solution to process various telecom logs and perform mufti-dimensional analysis like Tabular reports, Visual Link Analysis and GIS based Geo Analytics	
2.	Should be 15 Users License.	
3.	Should support Analysis of following types of telecom logs.	
a)	Individual CDRs/Billing Records	
b)	2G/3G/4G GPRS CDRs	
c)	IMEI Scans	
d)	Cell Tower/Mast Dumps	
e)	2G/3G/4G GPRS Cell Tower / Mast Dumps	
f)	ISD Dumps	
g)	Gateway Scans/Dumps	
4.	It should accept following formats and standardize all the formats from different service providers into one common format.	
a)	Text (comma, Tab, pipe etc.)	
b)	MS Excel (xls & xlsx)	
c)	HTML	
d)	MS Access for Subscriber Data	
5.	It should generate various point and click reports for CDR analysis like	
a)	It should show the relation between other party(s) and target(s) in single screen, and it should also generate the common numbers between them in single click.	
b)	It should show the relation between IMEI and Target(s) in single screen with common IMEI among them if any.	
c)	It should show the relation between Cell Id and Target(s) in single screen with common Cell Id among them if any.	
d)	It should show the relation between State/Telecom Circle and Target(s) in single screen with common State/Telecom Circle among them if any.	

e)	It should show the relation between Country and Target(s) in single screen with common Country among them if any.	
f)	It should show the relation between Total/Average Duration and Target(s)	
g)	It should show the relation between Call Type and Target(s)	
h)	Identification of calls where first and last pair of callers are same under sandwich call pattern	
i)	Identification of conference call (Call with in a call)	
6.	It should help in finding new number used by target when he/she discards his/her SIM card and Handset by analyzing the call patterns	
7.	It should allow user to remove duplicate records if one CDR has been imported multiple times in a case.	
8.	It should allow user to decode Roaming Cell Tower Information if available in target CDR / IMEI Scan	
9.	It should allow user to merge & unmerge multiple target numbers in to one target if IO comes to know that these numbers are being used by one target only.	
10	Should allow user to generate consolidated CDR briefing Excel reports for printing and producing to higher officers with information like	
a)	Summary Information about the target, its top other party, its top Day and Night Locations and Top Suspect List Matches	
b)	Frequency report for Other Parties of a Target No. with Call Type Distribution	
c)	Frequency report for IMEIs of a Target No.	
d)	Frequency report for Cell IDs of a Target No. With Day and Night Location Identification	
e)	Watch List/Suspect List Match Details	
f)	Common number and IMEI report if more then One Targets are under Investigation.	
11	Should allow user to search unknown numbers on social networking sites like True caller, etc.	

12	Should allow user to create Visual Link Charts of Data to identify numbers of interest.	
a)	It should allow Identification and creation of Clusters of Close Calling Numbers	
b)	It should allow to add other information available during investigations as and when available in the visual charts.	
c)	It should allow identification of common elements on visual charts.	
13	It should allow user to import and store the Cell ID Charts of various Telecom Service Providers, by which user can get all cell ids decoded for location-based analysis	
14	It should have unified filters to filter data based on investigation criteria like	
a)	Date & Time	
b)	Call Type	
c)	Target Number	
d)	Other Party	
e)	Cell ID	
f)	IMEI	
g)	City	
h)	State/Telecom Circle	
i)	Country	
j)	Day of week	
k)	Duration (equal to, between, Greater then & Less then)	
15	All filter combinations should be applicable on all reports simultaneously.	
16	In ISD Dump data analysis user should be able to create group of data on pre-selected countries for better concentrated analysis.	
17	In ISD Dumps It should provide facility for identifying the numbers who are calling in target country on the basis of	
a)	Frequency of Calls	
b)	SIM Change	
c)	Handset Change	
d)	Suspected Cell IDs etc.	
e)	Call of target in multiple countries of interest.	
18	Should allow Geo Analysis of ISD Dumps calls on map to identify hot spots of calls to/from country of interest.	

19	Should allow user to identify calls from ISD dumps to countries of interest from Various Geo-fence defined by users like Prison Area , Border Villages and other High Value locations	
20	In tower dump analysis it should identify the numbers and IMEI common between different locations	
a)	Identification of common Target Number, Other Party, IMEI, City, State & Country	
b)	Identification of uncommon Target Number, Other Party, IMEI, City, State & Country	
c)	Identification of those handsets who are using multiple SIM Cards	
d)	Identification of those SIM cards who are used in multiple handsets	
e)	Identification of those target numbers who are in touch with multiple other parties and vice versa	
f)	Identification of numbers who are target in one location and other party in other location.	
g)	Identification of those numbers who are present only during the incident period but neither before nor after the incident.	
h)	Identification of target numbers, other party and IMEI of current case with other stored case in database.	
i)	Frequency report on Day of week for Target Number, Other Party and IMEI	
j)	Frequency report on Call Type for Target Number, Other Party and IMEI	
k)	Frequency report on Country for Target Number, Other Party and IMEI	
l)	Frequency report on Hour of the Day(0-24) for Target Number, Other Party and IMEI	
m)	Frequency report on Location on the Basis of IMEI and IMSI to identify those IMEI and IMSI who were present in more than one towers on a Route Dump.	
n)	Identification of potential VOIP calls	
o)	Frequency report on Total Duration for Target Number	
p)	Frequency report on Average Duration for Target Number	
q)	Matching of Target Numbers, Other Party Number and IMEI with stored suspect/Watch list.	
r)	Identification of Target Numbers who has ported from one service provider to other.	

s)	One to One Call - Identification of those pairs of callers who are calling among them-self only.	
t)	New No. Analysis to identify those numbers or IMEI who might be present at scene at a particular time but not before and after that time.	
u)	Same Day Calls - Identify those numbers whose SIM got activated just on the date of call in the tower dump Group.	
21	User should be able to define that how many cell id are covering an incident Locations in an easy to use GUI	
22	In Gateway Dumps it should allow user to generate frequency based reports on the basis of Countries involved in the gateway dump.	
23	It should allow user to create cases , and add user to cases with access management	
24	It should allow administrator to permit access to users to specific modules by giving them individual permission for various modules.	
25	Should support storage of Subscriber Data and match the other party name and address from subscriber database in various Reports.	
26	Should allow maintaining a suspect list of Mobile no. IMEI and Cell IDs by importing from files or by Data Entry, the imported CDRs and Tower Dumps should be matched with suspect list for proactive investigation.	
27	Should allow user to bookmark the Number, IMEI and Cell ID with comments so that user can keep a track of all important findings in the case.	
28	Should allow user to identify the handset make model involved in the CDR and Tower dumps from IMEI	
29	Should allow user to see if any calls are made from any Geo-fenced location in a case.	
30	Should be fully compatible with the i2 Analyst Notebook.	
31	Should allow user to import data extracted from Mobile Forensic Tools like Cellebrite UFED, Micro-Systemation XRY etc. With the following features:	
a)	Common Number between various devices	
b)	Summary of Calls , SMS, chats.	
c)	Sand-witch Call Pattern from Call Logs	
32	Should allow user to geo-fence the area of interest like vital installations or scene of crime to identify calls made or received in that area automatically	

33	Should allow user to identify the how many cell towers from different service providers are covering an incident place or a location on a map.	
34	Should allow user to perform GIS based Geo Analytics like	
a)	Plotting locations of multiple targets on Maps for identification of potential meeting points.	
b)	Viewing Animated Movement of target from historical data on map.	
c)	Plotting day and night locations of multiple targets.	
d)	Measuring Distance between two locations	
e)	Calculating area with Radius of a Circle drawn on Map.	
f)	Facility to draw a buffer on a route of Road and Rail Network to Identify the Various Cell Tower Ids in the vicinity of the Road and Rail Line to create a Cell Tower Profile of entire route without visiting the Site.	
g)	Facility to use various base maps like Open Street Maps, Google Maps and Offline Maps without internet including offline satellite imagery.	
h)	Must have offline vector base maps of All over India Pre-configured to use directly.	
i)	Exporting Map as Jpeg Image	
35	Should allow field users to connect to central repository over secure VPN to search subscriber information and Cell Id Information remotely.	
37	Should allow creation of multiple users and Read Only case reviewers.	
38	Should provide regular updates within 15 days for new release during warranty period.	
39	IPDR analysis	
40	Maximum Size of DB supported by the tool in GB	
41	Client Server Setup	
42	Backup & Restore facility	

2. Disk Forensic Tool /Live Forensic/Network Forensic /Memory Forensic/ Registry Forensic and Remote Forensic Tool .		
Make:- Model :-		
Technical Specification		Compliance (Yes/No)
1.	Should have gallery view option to quickly reveal all photographs and graphics file stored on hard drives and other media.	
2.	Should have timeline view option to provide an easily to search adjustable, graphical calendar like display for file activity of particular interest.	
3.	Should contain Full Unicode support to allow users to search text and fonts from any foreign county and in any language	
4.	Should support acquisition Restart facility: continue a window acquisition from its point of interruption.	
5.	Should have inbuilt LinEn utility to acquire evidence via boot disk	
6.	Should have inbuilt WinEn utility to acquire RAM evidence	
7.	Should do image verification by CR and MD5	
8.	Should have Inbuilt support for writing scripts & should have pre-built scripts	
9.	Should Support more than 150 Filters and Conditions	
10.	Should Support combining filters to create complex queries using simple "OR" or "AND" Logic`	
11.	Should have Inbuilt Active Directory Information Extractor	
12.	Should be able to automatically rebuild the structure of formatted NTFS AND FAT volumes	
13.	Should support Recovery of deleted file/folders	
14.	Should have Inbuilt windows event log parser, Link file parser to search in unallocated space	
15.	Should have Inbuilt support for Compound (e.g., zipped) documents and file analysis.	
16.	Should support file Signature analysis	

17.	Should have native viewing support for 400 file formats	
18.	Should have built-in Registry Viewer	
19.	Should Meet the mentioned criteria for searching: Unicode index search, Binary search, Proximity Search, Internet and emails search, Active Code Page: keyboard in many language, Case Senstive, GREP ;Right to Left Reading, Big Endian/Little Endian, UTF-8/UTF-7, Search file slack and unallocated space etc.	
20.	Should Support Internet and Emails Investigation for : Browsing History Analysis, WEB History & chche analysis, Kazaa toolkit, HTML carver, HTML page reconstruction, Internet artifacts, Instant Messenger toolkit - Microsoft Internet Explore, Mozilla Firefox, Opera and Apple Safari	
21.	Should Include Emails Support for: Outlook PSTs/OSTs ('97-'03), Outlook Express DBXs, Microsoft Exchange EDB Parser, Yahoo, Hotmail, MBOX archives, Netscape Mail, AOL 6.0, 7.0, 8.0, and 9.0 PFCs, Lotus Notes v6.0.3, v6.5.4 and v7	
22.	Should include system support for:	
a)	Hardware and Software RAIDs	
b)	Dynamic disk support for Windows 2000/XP/2003 Server	
c)	Interpret and analyze VMware, Microsoft Virtual PC, DD and SafeBack v2 image formats.	
d)	File System: Windows FAT12/16/32, NTFS; Macintosh HFS, HFS+; Sun Soloris UFS, ZFS; Linux EXT2/3; Reiser; BSD FFS, FreeBSD's Fast File System 2 (FFS2) and FreeBSD's UFS2; Novell's NSS & NWFS; IBM's AIX jfs, JFS and JFS with LVm8; TiVo Series One and Two; CDFS; Joliet; DVD; UDF; ISO 9660; and Plam	
23	Should support reporting facillity with	
a)	Listing of all files and folders in a case	
b)	Detailed listing of all URLs and corresponding dates and times of web site visited	
c)	Document incident response report	
d)	Log Records	
e)	Registry	

f)	Detailed hard drive information about physical and logical partitions	
g)	View data about the acquisition, drive geometry, folder structures and bookmarked files and images	
h)	Export reports in Text, RFT (opens in Microsoft Office), HTML. XML or PDF formats.	
24	Smart phone and Tablet support: Acquire data from devices running the following operating systems: Apple's iOS, Google's Android OS, Rim's Blackberry OS, Nokia Symbian, Microsoft's Windows Mobile OS etc.	
25	Should have reporting feature for quickly share a report with field investigators, district attorney, supervision and with a few simple clicks select the exact information for your report and generate an easy to review HTML report that can be viewed in any web browser.	
26	Should be portable also.	
27	Power backup for any hardware involved with tool.	
28	Should provide regular updates within 15 days for new release during warranty period.	

3. Mobile Forensic Tool		
Make :- Model :-		
Technical Specification		Compliance (Yes/No)
1.	Should have Pre-installed Mobile Phone Forensic Software with following features: -	
2.	Mobile forensic solution for on-the-spot investigation	
3.	Screening and analysis features based on time period and frequency of use	
4.	Minimize work time with each step using high-speed processes	
5.	Recording and capturing features using the shooting function	
6.	Over 800 most popular App data support	
7.	Samsung Knox bypassing extraction supports	
8.	Simple and convenient usage with intuitive user interface	
9.	Selected data extraction and analysis:- Only data related to the incident can be selected and analyzed. Minimization of unnecessary data extraction to protect the privacy of the subject who is under investigation and reduce the time spent on the site	
10.	Screen Mirroring :- Display mirroring function supports to take screen capture shot and recording as well as screen controlling	
11.	Analysis UI provision similar to actual smartphone:- Data identification improvement and screening capabilities by providing themes similar to smartphone environments during data analysis	
12.	Analysis report creation function:- Ongoing video filming. Summary of smartphone internal data, screen capture, multimedia and application analysis result. Report generation on selected evidence. PDF file report and extracted data export (CD, DVD, USB)	
13.	Assurance of evidence data integrity :- Hash calculation for ensuring the integrity of data and multimedia files used for analysis	

14.	Multimedia preview function:- Images, videos, documents preview in the smartphone. Support Smartphone screen capturing with comments and save	
15.	Easy and concise process :- Intuitive user interface and smartphone model auto-detection function which enables smooth, on-the-spot forensics with minimal training	
16.	Should Support both logical and physical extraction methods	
17.	Should take Max. 1 minute of download time for 1GBytes phone data	
18.	Should support Data preview	
19.	Should be able to Decryption of extracted image with keys provided.	
20.	Should be able to Partition auto recognition and extraction of selected partition	
21.	Should Support Field investigation with file/data preselection.	
22.	Should Support physical extraction with Samsung Knox bypassing.	
23.	Should Support Samsung Galaxy series up to S7 OS 6.0 model.	
24.	Should be able to android Live Data extraction method (able to extract deleted data and applicable as Samsung Know Bypassing method)	
25.	Should Support iOS Data Extraction	
26.	Should have feature of Keychain extraction by decryption of iOS backed up passcode	
27.	Should support Could Data Extraction (calculate each file's hash value)	
28.	Should Support to continuous extraction for process paused image	
29.	Should Support over 10 hash values and overwriting prevention.	
30.	Should support Auto mobile recognition for logical extraction	
31.	Should be a total extraction SW, supports Chip-off, JTAG, USIM, and SD card	
32.	Should support Support major global mobiles for Japan, South/North America and India	

33.	Should Support over 350 Chinese manufactured mobiles. Eg. Huawei, Xiaomi, Oppo, Vivo and more	
34.	Should be able to Auto generation of extraction report	
35.	Should have Witness document supports(evidence number, time, location, hash verification)	
36.	Should have Voice alert for extraction success or fail	
37.	Should Consistent adding for supporting lists	
38.	Should have Multi language Support (English, Chinese, Korean)	
39.	Should have High-speed analysis performance by multi-core based parallel processing	
40.	Should have Python script editor support	
41.	Should Scrip programming and debugging tools	
42.	Should have a feature of Code generation, Code completion, Syntax highlight, Breakpoint stop/resume, Variable, Call stack, Line by line execution	
43.	Should have a feature of File system / Signature based data categorization.	
44.	Should support DB, Hex, Plist, Text, Multimedia viewer	
45.	Should have Data Visualization in Timeline, Map, Chatroom view, etc	
46.	Should have Analyzed result filtering, Key operator for data comparison supports	
47.	Should be able to Analyzed result filtering, Key operator for data comparison supports	
48.	Should support Over 850 most popular App analysis	
49.	Should be able to Call log, Address book, SMS/MMS, e- Mail, Memo, Internet history, Encrypted app data, Deleted data recovery	
50.	Should support Asian apps specialized (eg. Cacao Talk, Wechat, Line, QQ, etc)	
51.	Should have iPhone keychain data analysis support	
52.	Should have WeChat multi account data analysis support	
53.	Should be able to Decryption of Telegram, Walker messenger	

54.	Should support Micro tracking for analyzed data (footage of initialization, and anti-forensic app)	
55.	Should Analysis smartphone pattern lock, and pass word	
56.	Should have Brute force searching for over 4digits pass word (combination with number and letter) by GPU acceleration feature	
57.	Should have QCP file, Silk codec supports	
58.	Should be able to Multimedia file recovery within document file	
59.	Should Recover deleted file and data carving	
60.	Should Frame based recovery for deleted video file	
61.	Should Support PDF, Excel, ODS format report	
62.	Should be able to run Multi program operation supports to analyze multiple evidences	
63.	Should be portable	
64.	Backup & restore facility	
65.	Should provide regular updates within 15 days for new release during warranty period	
66.	Should be able to open/analyse reports generated by other leading tools of same genre/category	
67.	Power backup for any hardware tool associated	

4. SATA/IDE Write Blocker.		
Make:- Model: -		
Sr .No	Technical Specification	Compliance (Y/N)
1.	Should be portable write-blocker that provides support for 6 different interfaces in one device	
2.	Should have Fast Super speed USB3.0 host connection.	
3.	Should Support SAS, SATA, Fire Wire, USB3.0, IDE source drives	
4.	Should have Browser-based user interface for drive preview, software updates, HPA/DCO management	
5.	Should Connect and image multiple source drives simultaneously with your forensic imaging software	
6.	Easily monitor functions with 8 LEDs for power, host, device, activity and HPA/DCO detection	
7.	Power backup	
8.	Display screen	
9.	Report generation	

5. Pen Drives		
Make:- Model :-		
S.No	Technical Specification	Compliance (Yes/No)
1.	Standard Make 16 GB Pen drives- 8 Qty (Steel Body)	
2.	Standard Make 32 GB Pen-drives- 7 Qty (Steel Body)	

6.Card Readers (15 nos.)		
Make:- Model :-		
S.No	Technical Specification	Compliance (Yes/No)
1.	Should be a portable device	
2.	Card Reader connects practically any flash memory media, including the latest SDHC and SDXC standards, to any computer or equipment via either high speed eSATA or the ubiquitous USB interface.	
3.	Write blocker enabled	
4.	Forensically sound	

7.Smart Phone and feature phones (16 nos.)		
Make Model :-		
S.No	Technical Specification	Compliance (Y/N)
1	Five Different types of Mobile phones available in India market manufactured by different OEMs with the following guidelines: 5 Devices with following OS's (1 each) • Android OS • BlackBerry OS • iPhone OS / iOS • Windows Mobile OS • Symbian OS • 2G,3G,4G supported • 2 to 4GB ram • 16 to 64GB space • Dual Sim preferable • Sim cards	

8.Hard Disk		
Make:- Model :-		
S.No	Technical Specification	Compliance (Yes/No)
1.	Standard Make 2 TB HDD – 8 (IDE/SATA/SAS) internal	
2.	Standard Make 1TB HDD - Qty- 7 (IDE/SATA/SAS) external	
3.	HDD Bay / Connecters for connecting to machine - 5	

9. Social Media Analysis Tool		
Make:- Model :-		
S.No	Technical Specification	Compliance (Yes/No)
1.	It should have ability to collect and index data from social media streams, linked content and websites through APIs, webmail connectors and direct web navigation.	
2.	Tool should aggregate data from these multiple sources in real time, in a highly scalable and case- centric manner.	
	(i) Facebook	
	(ii) Twitter	
	(iii) Instagram	
	(iv) You Tube	
	(v) Tumblr	
	(vi) Web pages & Websites	
	(vii) Gmail	
	(viii) Yahoo Mail	
	(ix) Outlook.com	
	(x) AOL Mail	

	(xi) Internet Message Access Protocol (IMAP)	
3.	Should perform broad, unified searches across multiple accounts, social media streams and websites from a single interface. Linked content is automatically indexed and searched through the tool fast-as user types search from one user interface. Results are aggregated for sorting, tagging and export consistent with standard e-Discovery, or investigative, workflow.	
4.	MD5 hash values of individual items are calculated upon capture and maintained through export. Automated logging and reports generated. Key metadata unique to social media & web streams are captured through deep integration with APIs provided by the publisher. The metadata is important to establishing chain of custody and also provides key evidence relevant to the substantive case as well as authentication.	
5.	Should maintain data in a searchable native format from collection throughout production, uniquely providing a complete platform to address social media in the same manner as devices, e-mail and e-documents	
6.	Should deliver collected email in PST format while maintaining hierarchical structural integrity.	
7.	Should provide regular updates within 15 days for new release during warranty period.	
8.	Accessible from field through secure line	
9.	Reporting facility	
10.	Visual reporting	
11.	Current trend analysis	
12.	Image searching	

10. Hardware Disk Imaging and Drive Wiper Tool		
Make:- Model: -		
S.No	Technical Specification	Compliance (Yes/No)
1.	Should support forensic disk duplication of SAS/SATA/SCSI*/1394*/ PCIE*/Mini-PCIE*/M.2 NGFF* Multi Media USB Storage Devices like SSD, Cards etc.	
2.	Should support 1 to 1, 1 to 2 and 1 to 3 sources to destination combinations	
3.	Should support various forensic image format like RAW (dd), E01, .dmg, EX01	
4.	Should have imaging speed of up to 15GB per Min while concurrently calculating MD5 and SHA-1 hashes.	
5.	Should support Following Duplication Mode Disk to Disk (Clone) Disk to File (Image)	
6.	Should Calculate MD5 and SHA1 Hash simultaneously	
7.	Should allow Blank disk check	
8.	Should Allow encryption of forensic images using XTS-AES encryption algorithm	
9.	Should allow Destination Drive Wiping and formatting	
10.	Should have LCD Screen 3.5” for displaying various information related to drives connected and operations.	
11.	Should have USB port for connecting Keyboard and USB Printer	
12.	Should Have various types of adapters for 2.5” Drives, I.8” Drives, ZIF, LIF, Micro SATA, SSD etc.	
13.	Should support various file system formats (NTFS, FAT, FAT32, EXT, APFS etc)	
14.	Report facility	
15.	Power backup for any hardware device involved	

11. Steganography detection Tool		
Make:- Model: -		
Sr. No.	Technical Specification	Compliance (Yes/No)
1.	Tool should Quickly identify if Steganography is present in the investigations by scanning for over 1,000 data hiding applications using Fibonacci search methods.	
2.	Tool should Identify suspect carrier files that otherwise go undetected, including program artifacts, program signatures, and statistical anomalies.	
3.	Should utilize multiple operational discovery modes, including directory, drive, archives,drive image, and network path.	
4.	Should generate case specific reports for management or court presentations.	
5.	Should provide deep analysis for detected images and audio files	
6.	Should utilize the file viewing panel to display individual file attributes, including image details, DCT coefficients, and color pairs. This allows for a complete analysis of identified carriers	
7.	Select from various filter options for further analysis, such as Least Significant Bit (LSB's) of specific colors.	

12. GPS Forensic Tool		
Make :- Model :-		
S.No	Technical Specification	Compliance (Yes/No)
1.	Should Supports over 3500 different profiles of devices	
2.	Should have acquisition via logical, physical, file import, and flash memory decodes	
3.	Should Create custom reports in html, xml, Word, Excel, or PDF formats	
4.	Should do Online/Offline mapping with annotation tools	
5.	Should have Native Hex, Strings, xml, and SQLite data viewers	
6.	Should Export data in common formats. csv, txt, xlsx, xml, kml, kmz, or gdb	
7.	Should have Built-in analytical reports for geo locations, common activity location and time	
8.	Should have a Robust search function based on key words, hash value, file type and geo location	
9.	Should have User-based and global watch list capabilities	
10.	Should support Garmin, Magellan, TomTom, Furuno, Raymarine, SIMRad and Lowrance devices etc. For physical acquisitions, DD and E01 images should be supported. .	
11.	Should import files such as gdb, adm, gpx, cmap, usr, kml, csv, xls, xlxs, and txt. Users should also be able to import DD and E01 image sets from other acquisition tools.	
12.	Should have native data viewers such as hex, strings, XML, and SQLite. Data can be easily tagged and sent to the report builder	

13.	Geolocation data can be easily plotted and included in the report from online/offline maps such as Google, Bing, Yahoo, Open Street Maps, ArcGIS Topographical, Aviation Charts, NOAA Maritime Charts or Microsoft's MapPoint. Users can make annotation on the maps that will be included in the report. Reports can be saved in html, xml, Microsoft Word, Microsoft Excel, or PDF formats. Any of the data acquired with tool can be exported from the application in csv, txt, xlsx, xml, kml, kmz, or gdb formats.	
14.	Should have Built-in analytical reports to identify activity by geolocation as well as correlations across cases or devices by identifying common locations and times. The search function should include key words, hash value, file type and geo location.	
15.	Should have a watch list feature, which provides users with immediate notifications when data being acquired matches a pre-defined trigger. Watch list items can be created based on locations, key words or GREP expressions. Users can maintain multiple watch lists for either specific cases or at a global level.	

13. Password Recovery Tool		
Make:- Model :-		
Sr. No.	Technical Specification	Compliance (Yes/No)
1.	Should be a all-in-one password recovery for 200+ file types.	
2.	Should have Integrated Encryption Analyzer Pro to scan computers for password-protected items.	
3.	Should Include Search Index Examiner to retrieve electronic evidence from a Windows Desktop Search Database.	
4.	Should Includes FireWire Memory Imager to acquire physical memory images of the seized computers with Firewire support.	
5.	Should allow investigator to resets passwords for Local and Domain Windows Administrators, including Windows 7.	
6.	Should be able to recover encryption keys for hard drives protected with BitLocker from memory.	
7.	Should recover passwords for Windows users, email, websites and network connections from standalone registry files.	
8.	Should Recovers passwords for Mac key chain files.	
9.	Should Extract passwords from Windows/ Unix/ Mac hashes.	
10.	Should have Instant offline decryption of Word/Excel files via Rainbow Attack.	
11.	Should Recover passwords for PGP archives, virtual disks, key ring files.	
12.	Should have different password recovery attacks: Dictionary, Xieve, Brute-force, Known Password/ Part, Previous Passwords.	
13.	Should have Password modifiers supported (case changes, reversed words, etc.)	
14.	Should generate MD5 hash values for forensic reports.	
15.	Should support Encase Password Recovery Hardware	

14. Video Forensic and CCTV analysis Tool			
Make:- Model :-			
Sr. No.	Features	Technical Specification	Compliance (Yes/No)
1.	Image Format	Should take input from any standard image format (i.e. jpeg, tiff, png, bmp, targa, etc.…).	
2.	Video Format	Should take input from any standard video format (avi, flv, 3gpp, wmv, mov), also without the need of the codec installed on the system. Expandable by system codecs.	
3.	Capture Playback	Should have screen capture utility to capture playback from DVR console display or proprietary player to avoid conversion and downscale issues	
4.	Proprietary File Conversion	Should Convert proprietary surveillance video files to a standard AVI format like H264	
5.	Print Image	Should allow Print generated images.	
6.	Report Generation	Should allow automatic generation of a report containing all the scientific methodology and details of the processing steps, settings, and the bibliographic references to the algorithms in HTML format. This reporting feature is a critical advantage for users working in Frye or Daubert rules and should be provided.	
7.	Track Targets or Areas of Interest	Should allow tracking areas, people, objects through static, dynamic, and custom tracking.	
8.	File Verification	Should Verify alteration of image and video files in saved projects using hash function.	
9.	File information	Should display information about the file formats.	

10.	Exif data	Should display Exif data contained in digital images.	
11.	Hash Code	Should display Hash Code specific to saved files	
12.	Image information	Should display current image morphological and statistical features.	
13.	Video playback	Should have advanced video playback with frame by frame navigation, adjustable frame rate and jog controls.	
14.	Visualization	Should have custom zoom on an area of the image and color space selection.	
15.	Processing Workflow	Should allow display of Instant results like: add, configure, move, and modify an unlimited number of filters, in real time even while playing video. User can apply real-time, non-destructive image adjustments that don't require re-rendering as changes are applied.	
16.	Samples and tutorial	Should have a rich collection of examples and video lessons to start from basics and solve the most common cases.	
17.	Supported Platform	Should support Microsoft Windows	
	LOAD	**Loads image and video files**	
1.	Image Loader	Loads an image from file	
2.	Sequence Loader	Loads a list of images as video	
3.	Video Loader	Loads a video from file	
4.	Image Paster	Pastes the image in the clipboard for further processing.	
5.	Video Input	Live feed from DirectShow video sources.	
	LINK	**Connects and mixes different source filters.**	
1.	Video Mixer	Overlays or put side by side two different chains	

	WRITE	**Writes image and video files**	
1.	Image Writer	Writes the current image to a file	
2.	Sequence Writer	Writes all frames as image files	
3.	Video Writer	Writes the current video to a file.	
	SELECT FRAMES	**Selects video frames**	
1.	Single Selector	Selects a single frame of the video	
2.	Range Selector	Selects frames of the video within an interval with an optional step	
3.	Sparse Selector	Selects a list of frames in random positions	
4.	Remove Duplicates	Removes duplicated frames	
5.	Auto Selector	Automatically selects similar frames (for discarding bad frames)	
6.	IFrames Selector	Select only I frames	
7.	Demultiplexer	Separates different scenes multiplexed in the same video	
8.	Motion Detection	Fast seek of events in a video	
9.	Reverse	Plays back the video in the reverse direction.	
	EDIT	**Edit image geometric features.**	
1.	Crop	Crops a region of interest of the image	
2.	Flip	Mirror the image	
3.	Rotate	Rotate the image	
4.	Resize	Resize the image (zoom)	
5.	Smart Resize	Resize the image with a smart zoom algorithm	
6.	Correct Perspective	Remove the perspective effect on a plane of interest in the image	
7.	Deinterlace	Convert interlaced videos into progressive ones	
8.	Field Shift	Align the two fields of an interlaced frame	

9.	Undistort	Correct the geometric distortion, caused by capturing devices' optics.	

10.	Correct Aspect Ratio	Correct the aspect ratio of field based video.	
11.	Interleave	Convert a video with juxtaposed fields into an ordinary interlaced video.	
12.	Correct Fisheye	Compensate the distortion of common fisheye lenses.	
13.	Unroll	Convert an omnidirectional image to a panoramic one.	
	CHANNELS	**Color conversion and extraction functions**	
1.	Grayscale Conversion	Convert the image into grayscale	
2.	Color Conversion	Convert the image from grayscale to RGB	
3.	Color Switch	Exchange R and B color channels in the image	
4.	Extract Channel	Extract a single channel from the image	
5.	Enable Channels	Display only selected color channels	
	ADJUST	**Adjust image values**	
1.	Contrast/Brightness	Adjust the contrast and brightness values	
2.	Exposure	Adjust the image exposure to correct improper camera settings	
3.	Hue/Saturation/Value	Adjust the hue, the saturation and the color value of the image	
4.	Curves	Adjust the tone values according to the desired curve	
5.	Levels	Adjust intensity and color levels	
6.	Histogram Equalization	Improve the image contrast by equalizing the histogram of its values	
7.	CLAHE	Apply a contrast limited histogram equalization.	
8.	Contrast Stretch	Improve the image contrast by expanding the range of intensity values	

	EXTRACT	**Extract and analyze image features.**	
1.	Negative	Negative of the image	
2.	Threshold	Cut image values to the desired threshold(s)	
3.	Adaptive Threshold	Extract edges with adaptive threshold algorithm.	
4.	Laplace	Extract the edges with a Laplacian filter	
5.	Sobel	Extract the edges with a Sobel filter	
6.	Scharr	Extract the edges with a Scharr filter	
7.	Canny	Extract the edges with a Canny filter	
8.	Linear Filter	Filter the image with a user-defined kernel.	
9.	Bilinear Filter	Filter the image with two user-defined kernels and combines the results.	
10.	Channel Mixer	Mix the ratio of color in every channel	
11.	Color Deconvolution	Maximize the differences between specific colors in the image.	
12.	Component Separation	Separate different informative components in an image	
13.	Fourier	Remove periodic noise, backgrounds and interference in the Fourier domain	
	VERIFY FILE	**Verify digital image and video files**	
1.	File Info (EXIF Data)	Save file information and EXIF metadata from the original media in the report	
2.	Hash Code	Calculate input file hash code and check integrity loading the project	
	MEASURE	**Extract real-world measurements from the image**	
1.	Measure 1d	Take a measure on the planar image in 1 dimension	
2.	Measure 2d	Take a measure on planar image after perspective correction in 2 dimensions	
3.	Measure 3d	Take a measure on the image with a 3d reconstruction model of the perspective	

	SHARPEN	**Enhance image details.**	
1.	Laplacian Sharpening	Sharpen the image using a Laplacian filter.	
2.	Unsharp Masking	Sharpen the image using unsharp masking filter.	
	DENOISE	**Reduce the image noise.**	
1.	Averaging Filter	Smooth the image with an averaging filter.	
2.	Gaussian Filter	Smooth the image with a Gaussian filter.	
3.	Bilateral Filter	Smooth the image with a bilateral Gaussian filter.	
4.	Median Filter	Reduce the impulsive noise with a median filter.	
5.	Wiener Filter	Smooth the image with a Wiener filter	
6.	Deblocking	Reduce block artifacts from lossy compression.	
	DEBLURRING	**Reduce image blurring**	
1.	Motion Deblurring	Correct the blur of moving objects	
2.	Optical Deblurring	Correct the blur of objects which are out of focus (big blur)	
3.	Nonlinear Deblurring	Correct the blur caused by nonlinear motion	
4.	Blind Deconvolution	Correct the blur of objects out of focus with blind deconvolution (little blur)	
5.	Turbulence Deblurring	Correct the blur caused by air turbulence at long distances	
	STABILIZATION	**Stabilize video frames**	
1.	Local Stabilization	Stabilize a shaking video keeping steady the current selection	
2.	Global Stabilization	Stabilize the overall scene of a shaking video	
3.	Perspective Registration	Align the perspective of different images of the same object, taken from different points of view.	

	INTEGRATE	**Enhance image by multiple frames**	
1.	Temporal Smoothing	Reduce the noise integrating current and previous frames	
2.	Motion Smoothing	Reduce the noise integrating current and previous frames and avoiding halos on moving objects	
3.	Frame Averaging	Reduce the noise by creating an image which is the average of all the frames	
4.	Super Resolution	Merge all frames to improve the resolution of the image	
	PRESENTATION	**Prepare a video or image for presentation**	
1.	Add Timestamp	Indicate date and time for the current frame	
2.	Add Text	Insert text on the image.	
3.	Add Shape	Select and draw shape on current frame	
4.	Hide Selection	Pixelize, darkens or blur an area of interest in a video (witness protection)	
5.	Change Frame Rate	Change the frame rate of the video	
6.	Spotlight	Add a spotlight effect to a selection	
7.	Compare Original	Juxtapose or overlay original and enhanced image for comparison	
8.	Load Time stamp	Display subtitles on the video frame	
9.	Load Subtitles	Display content from embedded subtitle files on the video frame	

15. Data Recovery from Damaged Hard disk		
Make: - Model: -		
Sr. No.	Technical Specification	Compliance (Yes/No)
1.	Should have PCI-Express 1.0 Interface with two native SATA 2.0 ports and one IDE port	
2.	Should Support of all IDE (CE, CF, ZIF), SATA (MICRO SATA) interface HDDs	
3.	Should Support 1.8 inch, 2.5 inch, and 3.5 HDDs with a capacity of up to 5TB	
4.	One-click automatic HDD diagnostic repair module	
5.	Efficient USB terminal that can work with Seagate F3 serial HDDs	
6.	Should Support Flash ROM programming unit	
7.	Should Support the recovery of corrupted firmware in HDDs	
8.	Should Support the ability to unlock and reset hard drive password (i.e. decrypt the hard drive)	
9.	Should Support data recovery and HDDs repair due to failed read/write heads	
10.	Should support virtual head map technology	
11.	Should Support the repair of HDDs with physically-damaged sectors	
12.	Should Support disk imaging, imaging by selective head, file recovery	
13.	Should support Head map editing in RAM for data recovery	
14.	Review defect tables (P-list, G-list, T-list, etc.)	
15.	Load service information access program – LDR	
16.	Hide found defects of magnetic surface	
17.	Should Provide direct read and write to Seagate SA track	
18.	Forward and reverse scan and directly recover data from bad sectors	
19.	Provide MFT Scan to recover accidentally deleted files	
20.	File Carving	
21.	File recovery for unallocated space	
22.	Partition recovery	

23.	Should support almost all known file system (FAT32, FAT, NTFS, EXT, APFS etc)	
24.	Power backup for hardware device.	
25.	Report facility	

16. Malware Analyzer		
Make: - Model: -		
Sr. No	Technical Specification	Compliance (Yes/No)
1.	Should have the ability to conduct scans on a stand-alone system or network resource	
2.	Should Include 20 data-sets containing over 20,000 malicious threats	
3.	Should have 32-bit and 64-bit drive mounting and management integration	
4.	Should have detailed customizable XML-based evidence reports, XML based, with secure timestamping	
5.	Should have ability to scan within archive files (.zip, .rar, .jar, .bh, .arj, iha, lzh, .tar, .war, .enc,.bz2)	
6.	Should have Timelining feature	
7.	Should have fibonacci driven discovery engine that delivers >200MB/sec performance on most platforms	

17. Trainer Laptops (1 Windows +1 mac OS)			
Make:- Model :-			
Sr.No	Technical Specification	Compliance (Yes/No)	Remarks
1.	Intel i7 Processor or higher with 9th Generation or higher.		
2.	16GB or above DDR4 Ram		
3.	1TB@7200 rpm or higher SSD		
4.	4GB or above Graphic Card		
5.	Screen Size 15inch or above		
6.	Windows 10 pro		

7.	DVD R/W		
8.	Major connectivity ports (USD, HDMI, Serial etc)		
9.	Standard USB, HDMI and serial ports		
10.	Internet security Antivirus software		

18. Training Laptops with extra wireless keyboard and mouse (Windows)15			
Make:- Model :-			
Sr.No	Technical Specification	Compliance (Yes/No)	Remarks
1.	Intel i7 Processor		
2.	16GB DDR4 Ram		
3.	500GB SSD		
4.	4GB Graphic Card		
5.	Screen Size 15inch or above.		
6.	Windows 10 pro		
7.	DVD R/W		
8.	Major connectivity ports (USD, HDMI, Serial etc)		
9.	Standard USB, HDMI and serial ports		
10.	Internet security Antivirus software		

19. Workstation for Practical Work			
Make:- Model: -			
Sr. No.	Parameters	Technical Specification	Compliance (Yes/No)
1.	Processor	Dual (2) Intel Xeon E5-2620 v4 CPU, (8 Core) 2.1 GHz, 20MB Cache, 8.0 GT/s Intel QPI	
2.	Processor Speed	Processor speed 2.1 GHz or higher	
3.	Cache Memory	20 MB or higher	

4.	RAM	128 GB DDR4 or latest	
5.	Storage Type	1 x 256 GB Solid State SATA III Drive - OS Drive 1 x 256 GB Solid State SATA III Hard Drive - Temp/Cache/DB Drive 1 x 2.0 TB 7200 RPM SATA III Hard Drive - Data Drive installed in HotSwap Bay1	
6.	OS	Windows 10 Pro (64 bits) or latest	
7.	Peripherals	Mouse and keyboard and inbuilt speakers	
8.	Connectivity and Compatibility	USB and standard ports with IEEE 802.11a/b/g/n compatible	
9.	Screen of Size Monitor	21/22 Inch widescreen	
10.	Wireless Connectivity	Yes	
11.	Type of Ethernet connectivity	10/100/1000 on board Integrated Gigabit Port	
12.	Bluetooth connectivity	Yes	
13.	DVD Writer	Yes	
14.	Graphics	Nvidia GTX 1050Ti 4GB 128 bit DDR5 PCI- Express Video Card with 1 Display Port, 1 HDMI, and 1 DVI-D Ports	
15.	Others	Inbuild write blocker for all kind of media (SATA / PATA / Serial HDDs / USB devices / Firewire Devices etc)	
16.	Antivirus	Antivirus software	

20. Smart Podium		
Make:- Model :-		
S.No	Technical Specification	Compliance (Yes/No)
1.	Smart Podium with 19" Touch screen Panel.	
2.	Should come with 9U Rack with centralized locking system	
3.	Should have space to keep other devices like PC, Laptop, Visualizer etc.	

21. LED Touch Screen 85"		
Make:- Model :-		
S.No	Technical Specification	Compliance (Yes/No)
1.	85"/86" Touch Screen LED Display with 3840(H)*2160(V) resolution	
2.	Should have 1 billions + Colors	
3.	Source :- VGA Input (15 Pin D-sub) - 1 Port	
4.	Display Port Input - 1 Port HDMI Input (1.4) - 2 Ports HDMI Input (2.0) - 1 Port PC-Audio Input - 1 Port VGA Output - 1 Port HDMI Output - 1 port Coaxial Digital Audio Output - 1 Port Audio Output (Earphone Port) - 1 Port USB (A) 2.0/3.0 - 4/2 Ports USB (B) - 2 Ports RJ45 - 1 Port	
5.	Should have powerful Android system along with built in apps to make meetings, conferences and trainings more interactive	

22. Digital Evidence Seizure Kit		
Make :- Model :-		
1.	Should be a portable field kit which can be used at crime scene.	
2.	Should allow user to preview & image suspected storage media in read only mode.	
3.	Should support IDE/SATA/USB 3.0/Firewire/SAS storage device.	
4.	Should detect HPA/DCO	
5.	Should allow network connectivity if required.	
6.	Should allow user to open files on suspected storage media without changing time stamp.	
7.	Should allow user to make forensic image of suspected storage media with following features :-	
8.	Extremely Fast Imaging speeds of 23GB/min, speed with SAS/SATA-3 should be 37GB/min.	
9.	Support multiple Imager Formats , native or mirror copy , dd image , e01,ex01(e01 and ex01 withcompression) and file- based copy.	
10.	Multipal Imaging Ports: Write -Protected source ports include: 2SAS/SATA 1 USB 3.0 (should be converted to SATA using an optional USB to SATA adapter) 1 Firewire 1 SCSI (using the SCSI Module Option)"	
11.	Destination Ports should include 2SAS/SATA , 2 USB 3.0 (can be converted to SATA using An optional USB to SATA adapter, 1 Firewire and 1 SCSI (using the SCSI Module Option)	
12.	Gigabit Ethernet port for network connectivity. The unit should include a USB 3.0 device port for drive preview and two USB 2.0 host ports	
13.	Capability of Parallel Imaging, Simultaneously perform multiple imaging tasks from thesame source drive to multiple destinations using different imaging formats.	
14.	The source should contain at least 4 ports i.e. SATA, SAS, USB and Firewire, similarly destination should also have atleast 4 ports i.e. SATA, SAS, USB and	

	Firewire or better	
15.	Web Browser/Remote Operation to allows to connect with device from a web browser	
16.	Broad Interface Support, Built-in support forAS/SATA/USB/Firewire storage devices. Supports 1.8”/2.5”/3.5” IDE and 1.8” IDE ZIF and microSATA. Adapters for eSATA, mSATA and flash drive	
17.	Support M.2 SSD hard drive that use the PCIe interface as well as the SATA interface, PCIe Express cards and mini-PCIe express cards.	
18.	PCIe Express Cards & Mini-PCIe Express Cards to support PCIe-based storage expansion cards for PCs and laptops	
19.	Image to External Storage Device such as a NAS, using the Gigabit Ethernet port, USB 3.0 or via the SAS/SATA connection.	
20.	Forensic, Filter-Based File Copy,users can filter and then image by the file extension (such as.PDF,.xls, .JPEG, .mov etc.).	
21.	Image from a MAC system booted in “target disk mode” using the write-blocked FireWire port on	
22.	Concurrent Image and Verify	
23.	Generate Audit Trail Reporting/Log Files in XML, HTML or PDF format	
24.	Secure sensitive evidence data with whole drive AES 256 bit encryption	
25.	Should allow user to acquire RAM from Running PC.	
26.	Should allow user to obtain system protected files like windows registry.	
27.	Should allow user to create case to log seizure information.	
28.	Should allow user to enter various information required for creating seizure memo like location of seizure , Details of Crime, Details of seized exhibit etc.	
29.	Should allow user to export seizure memo for printing purpose.	
30.	Application should allow automatic insertion of hash value of selected files as well as whole disk media on phones/ hard drive media in seizure memo WITHOUT manual typing	
31.	Seizure memo application should be installed on a portable laptop / Tablet.	

32.	Kit should have screwdriver kit to open hard drive from laptop and desktops in field.	
33.	Kit should have 16 Mega Pixel Camera to capture the details of storage media.	
34.	Kit should have Faraday Bag to Isolate mobile phones from active mobile network to prevent incoming calls / SMS / Instant Message like Whats-app & remote deletion.	
35.	Kit should have evidence labels to label seized exhibit.	
36.	Kit should have protective hard drive case to carry suspect hard drive from crime scene to lab.	
37.	Whole kit should come in a portable hard waterproof case.	

23. Multi Function Printer			
Make:- Model: -			
Sr.No.	Technical Specification	Compliance (Yes/No)	Remarks
1.	Printer, Scan, Copy		
2.	Color and Black & White		
3.	Speed 28PPM or higher		
4.	Automatic Duplex		
5.	Print Resolution 1200dpi		
6.	Monthly duty cycle 5000 pages or higher		
7.	Scanning Type Flatbed and ADF		
8.	Memory 128MB or more		
9.	Processor 600MHz or more		
10.	Should support all major paper sizes (		
11.	Connectivity USB, Network , Wifi		
12.	Support for following paper size		

	Letter- 215.9 x 279.4 mm Letter Rotated - 279.4 x 215.9 mm Legal - 215.9 x 355.6 mm Executive - 184.2 x 266.7 mm Statement - 139.7 x 215.9 mm Oficio 8.5 x 13 - 215.9 x 330.2 mm Tabloid - 279.4 x 431.8 4 x 6 - 101.6 x 152.4 mm 5 x 7 - 127 x 177.8 mm 5 x 8 - 127 x 203.2 mm A3 - 297 x 420 mm A4 - 210 x 297 mm A4 Rotated - 297 x 210 mm A5 - 148 x 210 mm A5 Rotated - 210 x 148 mm A6 - 105 x 148 mm RA4 - 215 x 305 mm SRA4 - 225 x 320 mm B4 (JIS) - 257 x 364 mm B5 (JIS) - 182 x 257 mm B6 (JIS) - 128 x 182 mm 10 x 15 cm - 101.6 x 152.4 mm Oficio 216 x 340 - 215.9 x 340 mm 8K 270 x 390 - 270 x 390 16K 195 x 270 - 195 x 270 8K 260 x 368 - 260 x 368 16K 184 x 260 mm - 184 x 260 mm 8K 273 x 394 mm - 273 x 393.7 mm 16K 197 x 273 mm - 196.8 x 273 mm Japanese Postcard - 100 by 148 mm Japanese Double Postcard - 148 x 200 mm Envelope #9 - 98.4 x 225.4 mm Envelope #10 - 104.8 x 241.3 mm Envelope Monarch - 98.4 x 190.5 mm Envelope B5 - 176 x 250 mm Envelope C5 - 162 x 229 mm Envelope C6 -114 x 162 mm Custom size		

24. Digital Pointer			
Make:- Model:-			
Sr.No.	Technical Specification	Compliance (Yes/No)	Remarks
1.	Reliable 2.4Ghz wireless operation for smooth and immediate response		
2.	Convenient portable USB receiver and laser pointer to control your		
	presentations		
3.	Plug & Play Device.		
4.	Remotely controls your PowerPointpresentations from up to 10 meters distance,		
5.	4 buttons to control your slide show.		

25. Furnishing and Renovation of existing Cyber Lab.

There is a present Cyber Lab in CID which need to be renovated and cabin for trainers should be made. Bidder has to make it of modern look with closing of windows, lighting and interiors which includes false ceiling, good quality table and chairs with plug point integrated, mat on floor, bookshelf, modern doors which can control access by bio metric identity or entry card etc.

The purpose is to make the Lab look like a professional and state of the art Cyber Lab.

26. Bio metric and card controlled door access system for the Lab and cabin.

27. **Electric work and Networking with all necessary equipments.**