Office of the Director General of Police Arunachal Pradesh Itanagar
सत्यमेव जयते

GOVERNMENT OF ARUNACHAL PRADESH
OFFICE OF THE DIRECTOR GENERAL OF POLICE
POLICE HEADQUARTERS::ITANAGAR

NO PHQ (PROV) - 15/2024-25. Dated Itanagar, the 26th November, 2024.

TENDER NOTICE

On behalf of the Governor of Arunachal Pradesh, Director General of Police, Arunachal Pradesh invites Sealed Tender under two Bid systems (Technical Bid & Financial Bid) from the manufacturers, authorized agents / dealers / suppliers of reputed firms for entering contract for supply & installation of FSL (Forensic Science Laboratory) equipments under Nirbhaya Scheme during the year 2024-25 for Arunachal Pradesh Police. For details, please visit our web site-www. arunpol.nic.in.

Sd/-
Director General of Police
Police Headquarters, Itanagar
Arunachal Pradesh

(Not to be published)

Memo No. PHQ (Prov) - 15/2024-25. Dated Itanagar the 27th November, 2024.
Copy to:

1 The Director of Information and Public Relations Govt. of Arunachal Pradesh, Naharlagun for information and wide Circulation. He is also requested to pass necessary order for publication of the above Tender Notice in one leading Newspaper of Arunachal Pradesh published from Itanagar namely "Arunachal Times" or "Arunachal Front".

2 The In- Charge, Computer Cell, PHQ, Itanagar. The tender notice along with lists of equipments with specifications may be uploaded in the website of Arunachal Pradesh Police (arunpol.nic.in)

3. Office copy

27.11.24.
Asstt. Inspector General of Police (E),
Police Headquarters, Itanagar
Arunachal Pradesh

Asstt. Inspector General of Police(E)
Arunachal Pradesh
Itanagar

of the Director General of Police Arunachal Pradesh, Itanagar
सत्यमेव जयते

GOVERNMENT T OF ARUNACHAL PRADESH
OFFICE OF THE DIRECTOR GENERAL OF POLICE
POLICE HEADQUARTERS: ITANAGAR

NO.PHQ(PROV)-15/2024-25. Dated Itanagar, the 27th November, 2024.

TENDER NOTICE – CUM – TERMS AND CONDITIONS

On behalf of the Governor of Arunachal Pradesh, Director General of Police, Arunachal Pradesh invites Sealed Tender under two Bid systems (Technical Bid & Financial Bid) from the manufacturers, authorized agents / dealers / suppliers of reputed firms for entering contract for supply & installation of Forensic Science Laboratory equipments under Nirbhaya Scheme during the year 2024-25 for Arunachal Pradesh Police. For details please visit our web site-www. arunpol.nic.in.

1.

SL No	Description of items to be procured	Approx. Cost of tender	Earnest money required	Tender Fee (Non-refundable)
1.	Procurement & installation of FSL (Forensic Science Laboratory) equipments under Nirbhaya Scheme 2022-23 during the year 2024-25 for Arunachal Pradesh Police. (items details along with specifications attached at Annexure- "A")	**Rs. 86,50,000/-**	Rs. 1,73,000/-	Rs. 1,000/-

2. Critical date sheet:

Sl.	Particulars	Date	Time
1	Date of publication of Tender	**28/11/2024**	
2	Bid submission start date	From the date of publication onward	
3	Bid submission end date	**23/12/2024**	**1100 hrs**
4	Submission of Tender fees (cost of tender documents)	The tenderer who wants to obtain tender document from PHQ, Itanagar, tender fee (in form of Demand Draft / Bank Draft in favour of AIGP(E), PHQ, Itanagar payable at SBI, Itanagar) may be furnished at the time of obtaining the tender documents. The firms registered under MSME are exempted for earnest money. They must submit copy of registration certificate of MSME.	
5	Date of Technical bid opening	**23/12/2024**	**1130 hrs**

3. The Tender documents must be provided in two (02) covers:

1. **Cover-1:** It shall contain scanned copies of eligibility information as under.

a) Technical bid along with its specifications leaflet, brochure, catalogue / literature, if any, of each tendered item.

b) Tender documents duly completed and signed BUT without indication of the rates "Quoted".

c) Earnest Money must be attached in form of TDR / FDR / Demand Draft / NSC / KVP etc. of Nationalized Bank / Post offices duly pledged in favour of Asstt. Inspector General of Police (E), PHQ, Itanagar. The firms registered under MSME are exempted for earnest money. They must submit copy of registration certificate of MSME.

d) Attested copy of PAN.

e) Attested copy of firm registration.

f) Attested copy of firm GST Registration.

g) Valid Trading license issued by competent authority for the tendered items.

h) Letter of authority (original) in respect of authorized distributors/dealership or Manufacturer Certificate (OEM) etc.

i) Latest Financially soundness certificate / Bank Solvency Certificate.

j) Undertaking letter about non-blacklisting of the firm.

k) Any other relevant document which the firm wishes to submit.

l) All the tender papers must be serialized / numbered properly and index / check list be submitted at the beginning of the tender papers indicating the pages of the relevant documents. Tenders without index / checklist shall be summarily rejected.

m) Technical compliance statement should be enclosed along with technical bid clearly specifying deviation, if any for all specifications mentioned in the tender.

n) 10 (Ten) years service and spare parts support after warranty period should be provided on payment basis. In this regard, an undertaking must be submitted by the participating firms.

2. **Cover-2:** It shall contain documents on "Financial Bid". Financial bid shall be opened only of those bidders who have been declared technically qualified by the committee. The criteria for eligibility and qualifications are to be met by the bidders such as minimum level of experience / past performance (if any), facilities and financial position etc. The date of opening of "Financial Bid" will be intimated to the firms which will be found qualified in technical compliance statement in due course of time.

GENERAL INSTRUCTIONS:

1. The tenders received after scheduled date & time will not be entertained. The tenderers or their representative may remain present at the time of opening of tenders.

2. Rates must be clearly written in figures as well as in words, showing GST Separately.

3. There should not be any cutting / over writing.

4. The Tenderer / Firm who fails to fulfill the eligibility conditions will be summarily rejected.

5. The firms will have to submit all documents (as mentioned in cover-1) including EMD, cost of Tender documents in the office of Assistant Inspector General of Police (E), Police Head Quarters, Itanagar, Arunachal Pradesh on **23/12/2024 at 1100 hrs.** The experience certificate (if any) must contain name designation, address, Phone No., Mail ID of issuing officer. The certificate should be countersigned by concerned OFFICE HEAD/DEPT. HEAD.

6. In case tender opening day is declared as holiday or bandh call at Itanagar, the tenders shall be received up to next working day till 1100 hrs. and opened on the same day at 1130 hrs.

a) The bidders should keep checking the website for any addendum / corrigendum to the notice / bidding documents till the date of submission of bids and the bidder should incorporate the same in his bid documents.

b) Conditional bids and the bids not meeting the qualifying criteria on the date of receipt of bids shall be summarily rejected.

c) Bids will be opened as per time & schedule mentioned.

d) Before submission of bids, bidders must ensure that scanned copy of all the necessary documents have been attached with bid.

e) The department will not be responsible for delay in submission due to any reason(s).

f) All the required information for the bid must be filled and submitted.

g) The details of EMD and other documents specified in the tender documents should be same as submitted (scanned copies), otherwise tender will be summarily rejected.

h) **Conditions:** If the tenderer who fails to supply the material/ perform the task assigned to him in the purchase order, within the period prescribed for such delivery specified above, the AIGP (E), or other competent authority, shall be entitled at his discretion to the actions as under:

i) Graded liquidated damages for delay in delivery of all or any good or performance of services will be liable for as under: -
   a) For first 30 days @ 1% of the value of the goods.
   b) For next 60 days @2% of the value of the goods.
   c) For delay above 2 month/ over & up to 4 months @ 4% of the value of the goods.
   d) Beyond 4 months and up to 6 months @ 5% of the value of the goods & on expiry of 6 months the contract would automatically get nullified and Security Money Deposit would be forfeited.

7. The tender papers containing full details with specifications and terms and conditions can be obtained from Dy. Superintendent of Police (Provisioning), PHQ Itanagar, on payment of tender fee of Rs. 1,000/- (Non-refundable through a bank draft in favour of the Asstt. Inspector General of Police (E), PHQ, Itanagar, Arunachal Pradesh payable at S.B.I. Itanagar) on any working day from 0930 hrs. to 1600 hrs w.e.f. **28/11/2024 to 23/12/2024**. The tender documents may also be downloaded from our website. The tenderers downloading the documents from website are also required to submit a Bank Draft of Rs. 1,000/- as tender fees. No other mode of payment will be accepted.

8. Successful tenderers will be required to deposit 5% of the total value of the articles to be supplied as performance security money within 10 days from the date of issue of letter of acceptance of tender. The successful tenders will have to enter into a "DEED OF AGREEMENT" stipulating the Terms and Conditions of the contract.

9. Non fulfillment of any or all the Terms & Conditions of Contract, performance security deposit and EMD of the successful tenderer will be forfeiture and supply order issued to the firm shall be cancelled.

10. Rate should be quoted F.O.R Central Store, PHQ, Itanagar and rates quoted other than F.O.R Central Store, PHQ, Itanagar shall not be accepted. No packing or forwarding charges will be allowed. The rate of GST (as applicable) may be charged/quoted by the tenderers and the amount be clearly mentioned for all items. The rate should be quoted in Indian currency both in figure and words clearly. Tenders must be legible and clear in all respect else the tenders shall be liable to be rejected.

11. Tenders should be addressed to the undersigned by designation and not by name. The separate sealed envelope containing the tender should be subscribed as "Tender for supply & installation of Forensic Science Laboratory equipments under Nirbhaya Scheme during the year 2024-25 for Arunachal Pradesh Police and sent by Registered Post / Speed Post / Courier Service or put in the Tender Box kept in the office of the undersigned (Provisioning Branch) on any working day from 0930 hrs. to 1600 hours. ***The tenders received after scheduled date & time will not be entertained.***

12. Any breakage or loss of any item will be at the supplier's risk.

13. Delivery of the stores will have to be completed within 90 days from the date of issue of supply order. In case of failure to supply the items in time, violation of any provision of Deed of Agreement, the firm is liable to be blacklisted.

14. If any item is found damaged or otherwise unacceptable at the time of delivery / inspection, the supplier will be required to remove the same from Central Store, PHQ, Itanagar, Arunachal Pradesh at their own cost within 15 days. The demonstration of the items shall be conducted at the time of acceptance by the Board of Officers. The items not found as per specifications shall be rejected.

15. Payment will be made to the supplier directly on completion of supplies / installation and on receipt of stores. Documents / vouchers / bill etc.

16. The Director General of Police, Arunachal Pradesh, Itanagar reserves the right to reject the lowest or all or any of the tenders without assigning any reason thereof.

17. The Director General of Police of Arunachal Pradesh, Itanagar shall have the right to ask the firms to demonstrate their items before the items are accepted.

18. List of equipments/items with description & specification is enclosed at Annexure- A. The quantities mentioned in the enclosure are all approximation and subject to variation as per actual availability of funds.

19. Tenders will remain valid up to **31-03-2025**.

20. All items to be supplied shall be under warranty as mentioned in Annexure-A against each items/ equipments from the date of acceptance.

21. In case of any dispute, legal jurisdiction will be at Itanagar, Arunachal Pradesh.

22. In case of any query, the tenderers may contact at following phone no. / mail ID.

Officers	Telephone	E-mail ID
Dy. Superintendent of Police (Prov), PHQ, Itanagar	97749-07007 (Mobile)	arpolice@rediffmail.com.
Sub-Inspector (Prov), PHQ, Itanagar	81190-91663 (Mobile)	arpolice@rediffmail.com.

Note: In view of the Govt. policy of "Vocal for Local" and "Atma Nirbhar Bharat" to encourage local entrepreneurs vide No. FIN/E-30/2017/675 dated 19/008/2020, the firm registered within Arunachal Pradesh can only participate in the tender process.

27.11.24

Asstt. Inspector General of Police (E)
Police Head Quarters, Itanagar
Arunachal Pradesh

Asstt. Inspector General of Police(E)
Arunachal Pradesh
Itanagar

Annexure – "A"

LIST OF EQUIPMENTS WITH SPECIFICATIONS AND QUANTITY TO BE PROCURED & INSTALLED FOR IMPLEMENTATION OF NIRBHAYA SCHEME 2022-23 IN THE STATE OF ARUNACHAL PRADESH DURING THE YEAR 2024-25

A. CYBER FORENSIC DIVISION			
SL No.	Name of Item	Technical Specification	Quantity
1.	Forensic Workstation	1) **Cabinet**: Dual Chamber Super Tower Chassis 2) **Processor**: Single Processor, 32-Core, 64 Thread Processors 3) **Cooling Type**: Active Cooling for the Central Processing 4) **RAM**: 256GB DDR4 2933 MHz ECC RAM. Upgradable to 1024 GB 5) **OS Storage**: 4TB SSD for the Operating System 6) **Temp Storage**: 2TB M.2 NVMe SSD for Temporary Files 7) **RAID Storage**: 4x10TB Hard Drives configured in RAID 5/6/10 8) **Motherboard**: Supported Chipset 9) **Graphic Card**: 16 GB NVIDIA Graphics card or better 10) **Integrated Write Blocker**: Supports forensic acquisitions of SATA, USB 3.0, PCIe, SAS, FireWire 800 and IDE 11) **Hot Swap 2.5" Disk**: 4X 2.5" hot Swap Bay 12) **Hot Swap 3.5" Disk**: 3X 3.5" hot Swap Bay 13) **4 Port USB Hub 3.0**: 4 Port USB 3.0 Hub 14) **Connectivity**: Wireless WIFI+ Bluetooth 4.2 15) **Operating System**: Microsoft Windows 11 Pro 64 Bit 16) **Keyboard and Mouse**: One (1) Mechanical Keyboard and Mouse 17) **Monitor**: 32" 1920×1080 Full HD 18) **HDD Tray**: Cooling tray 19) **Pre-installed SW**: MS OFFICE 2021 20) **Pre-installed SW**: Hash match SW: Should allow users to select a file to generate its Hash Value; supports Hash such as MD5, SHA1, SHA256, SHA512, SHA384, RIPEMD-16, etc; Allow users to export generated Result in PDF Format; Allow users to Validate files against Hash value; Allow users to Compare two files for any selected Hash. 21) **Pre-installed SW**: Should have inbuilt tool for analyzing cryptocurrency-related information on recovered hard disk drives from various crimes. It should scan various document formats, such as text files, PDFs, images, emails, spreadsheets, and more, to extract data like seeds, public keys, private keys, transaction hashes, currency names, symbols, and exchange names. It should operate offline and present the gathered information on an in-app display. Supported cryptocurrencies include Bitcoin, Ethereum, Tether, USD Coin, Binance Coin, Ripple, Binance USD, Cardano, Solana, Dogecoin, PolkaDOT, DAI, Polygon, Shiba Inu, Tron, Avalanche, Uniswap, Wrapped Bitcoin, and Litecoin. 22) **General**: Preinstalled with Forensic certified software's such as FTK Imager, Encase Imager, Sluethkit Autopsy or more similar software's. 23) The product must have **Manufacturer's Authorization Letter.** 24) **Warranty/SMS/ATS: 3 (Three) Yrs Warranty/ Service Maintenance and Support (SMS) / Annual Technical Support (ATS).** Any Hardware/Software/Firmware updates or upgrades to be provided during the Warranty Period. 25) **Training**: On-site Product Training with certificate.	1 No.

2.	**High End Workstation**	**1)** Computer Type: All-in-One High-End Workstation **2)** Chipset Series: Intel Q Series. **3)** Chipset No.: Intel Q670. **4)** Processor Make: Intel. **5)** Processor Generation: i9. **6)** No. of Cores per Processor: 24. **7)** Processor: Intel Core i9 13900. **8)** Operating System: Windows 11 professional 64-bit (pre-installed) **9)** External bootable HDD with pre-installed Backup Software **10)** RAM: 64 GB DDR5 (expandable up to 128 GB) **11)** Types of Drives used to populate the Internal Bays: SSD, PCLe-SSD **12)** OS Drive: 500 GB SSD **13)** Cache Drive: 500 GB SSD **14)** Data Drive: 2 TB SATA HDD **15)** 1 RJ45 LAN port (Gigabit LAN controller) **16)** 802.11a/b/g/n/ac WiFi+ Bluetooth 4.0 **17)** 1x USB 3.1 Typ-C; 4x USB 3.0 Typ A **18)** 2xHDMI **19)** Digital Optical S/PDIF audio output & 3.5 mm Audio ports with In-built 2.1 Stereo Speaker **20)** Display size: - 23.8 Inch **21)** Display type: - non-touch. **22)** Panel Technology: - LED/IPS. **23)** Display resolution: - 1920x1080. **24)** Keyboard and Mouse Combo **25)** Availability of Webcam integrated with Display: - Yes. **26)** The product must have **Manufacturer's Authorization Letter.** **27)** On-site OEM Warranty: - 3 Yrs. **28)** **Training**: On-site Product Training with certificate.	1 No.
3.	**Magnet Axiom Complete**	1) **Software Type:** DIGITAL FORENSICS PLATFORM SOFTWARE FOR FORENSIC DATA EXTRACTION. 2) **Period of Subscription (in Years)**: 03 (Three) Years On-site Warranty/SMS/Software Subscription. Any Software/ Firmware updates to be provided during the Warranty Period. 3) The product must have **Manufacturer's Authorization Letter.** 4) **Training:** On-Site product training with certificate. 5) **Operating Systems supported**: Windows 11 Pro 64-bit 6) A versatile platform for comprehensive data extraction and analysis, supporting a wide array of sources, including real-time acquisition and memory analysis, computers, mobile devices, and vehicle data. 7) Tailored and dedicated workflows for Windows, MacOS, and Linux environments, ensuring seamless compatibility and smooth performance across diverse operating systems. 8) Capable of acquiring data from Android devices and conducting logical acquisition from iOS devices, Windows phones, MTP devices, SIM cards, and Kindles. 9) Compatibility should extend to renowned Linux distributions like Ubuntu, Debian, Red Hat, Kali, and more, accommodating a broad spectrum of systems.	1 No.

		10) Facilitates data export in the .ivo file format, empowering users to amalgamate vehicle forensic data with other sources within a single case, simplifying the analysis of waypoints, routes, velocity logs, contacts, call logs, attached devices, and more. **11)** Should also offer support for various file systems, including YAFFS2, NTFS, HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, and EXFAT. **12)** Targeted image for Windows includes Event Logs, Windows Registry Hives, Pagefile, Hibernation File, Master File Table, , USN Journal, , Setup API Logs, , LNK Files, User Profiles, Prefetch Files. **13)** It should have the capability to support the capture of Physical Memory (RAM Dump), allowing for the analysis of critical artifacts often exclusively found in memory. **14)** The utility should offer the option to capture memory from individual running processes. In cases where time is limited or specific processes are of interest, this feature allows for targeted retrieval, reducing data fragmentation and enhancing the recovery of larger data types. **15)** The system should provide both GUI and Command Line options for memory acquisition, minimizing its impact on the suspect system. **16)** A command-line tool should be available for quick and non-intrusive examination of suspect computer systems to identify encrypted volumes during incident response. **17)** Ability to analyze data from forensic image file formats i.e. E01, Ex01, L01, Lx01,.AFF .AD1, .DD, .RAW, .BIN, .IMG, .DMG, .FLP, .VFD, .BIF, .VMDK, .VHD, .VDI, .XVA, .ZIP, .TAR. **18)** Ability to analyse memory dumps in the format of .RAW, .CR*ASH*, .VMSS, .HPAK, .ELF, .MEM, .DMP, .DD, .IMG, .IMA, .VFD, .FLP etc. **19)** Support Full Drive Decryption, with the integrated capability, can detect and decrypt TrueCrypt, BitLocker, McAfee, VeraCrypt and FileValut2 with known password or using brutal force attack. **20)** Should have a utility for determining and retrieving user passwords based on keywords from a case file significantly reducing the time involved in trying to brute-force this password manually **21)** Multiple Device Queuing – Automatically process multiple devices in a row without the need for examiner-run separate process. **22)** Filter stacking allows you to layer on several dimensions of filter criteria to pinpoint specific items in a large dataset. **23)** Ability to view SQLite database files using built-in SQLite viewer **24)** Should support OCR support for extraction of text from PDF documents (including text in scanned documents and text from pictures in PDF documents) and from picture artefacts for Keyword Searching. **25)** Should support search for keywords on both recovered artefact and sector level content both prior to processing the case as well as after processing the complete case with an option to select all added evidence sources or any particular evidence source. **26)** Should allow users to tag or exclude artefact evidence from case data during processing based on a keyword list. Case examiner should be able to load the list of keywords and choose to either tag or exclude artefacts containing those keywords. This can be helpful where a manual review process is utilized to remove the content, or in scenarios where it must automatically be excluded. **27)** Recovers more artefacts from both allocated and unallocated space by extracting data from full files or carving for deleted data and traces of data elements/fragments left behind by apps and websites, presenting it in an organized and easy to read format.	

		28) Ability to identify luring and sexual conversations. 15+ AI Categories to automatically identify and bifurcate images related to drugs, weapons, nudity, weapons, militants, vehicles, screen captures, documents, ID Cards, Human Faces, License Plates, Building, Child Abuse, Tattoos, Invoices, etc **29)** Identify and categorize handwritten documents automatically with AI. **30)** Support CSAM investigations with AI technology, and help you uncover key evidence even more quickly including new AI technology from Thorn to identify illicit content leveraging their CSAM Image Classifier to improve the detection of CSAM across picture and video artefacts. **31)** Inbuilt Support for finding similar pictures by building picture comparison for identifying any similar pictures from the extracted images or external images using CBIR (Content Based Image Retrieval) feature **32)** Should have advance option to analyse media file using dedicated Media explorer to view, sort, and filter media evidence using criteria that are specific to pictures and videos. The Media explorer should stacks copies of the same picture or video that were found in different source locations. **33)** Ability to hover over image/video, which should provide a larger, higher resolution preview of the image or video. Users can also zoom and pan around an image within the preview. For videos, investigator should be able to use the mouse to quickly scroll through the contents of the video. **34)** Should allow investigator to filter media files by Investigation leads, including attributes such as camera serial numbers, Exif created dates, camera make & model, Items with Geolocation data, Deleted source, items matching social media platforms, Lens model & Serial Number, file extension, VICS attributes, media attributes, video attributes, and file attributes. The date / time filter is also available in the Filters bar. **35)** Should allow investigator to Sort by option to organize the evidence in ascending or descending order based on attributes such as skin tone, media size. **36)** Should allow investigator to filter video files with attributes such as video files within carving limit, media duration etc **37)** Should have utility which can be installed on any number of Windows Tablet or Laptop to empower frontline officers to collect and report on fleeting digital evidence. The tool should be capable to maintain privacy and build trust with the public while capturing crucial but fleeting digital evidence from consenting victims and witnesses. **38)** Quickly get Photo, video evidence with an external or internal camera or by connecting to the victim or witness's mobile phone, or memory card. **39)** Support case dashboard that displays high level details about the case, evidence sources and summaries of processed results of multiple digital evidence in one screen. **40)** Visualize connections between files, users, and devices. Discover the full history of a file or artifact to build case and prove intent. Visualizes evidence from disk and memory to show where files came from, who they are connected to, and where they're stored. **41)** Should support pre-processing date filters which give investigators the option of setting a date and time range for the artefacts that will be added to a case. This feature allows to limit the artefact data being collected in order to comply with warrant restrictions around the applicable dates for the investigation.	

		42) Should support parse and carve and parse selected artefact option to save time on a case if carving is not necessary for investigation. **43)** Should have Timeline explorer to consolidate all the timestamps from files and artefacts in a single view, with colours and tags to differentiate timestamp categorizes. **44)** Ability to automatically find potential chat databases along with other valuable evidence from non-chat apps that aren't yet supported in an artefact. Users can then easily create an XML or Python artefact to be searched for in future cases. **45)** Capability for parsing unsupported database using custom artefacts or Python Scripts for popular local applications like Tally, Airbnb, ccleaner, FakeGPS, Linkedin, onion browser bookmarks etc. **46)** Should have a GUI/Wizard-driven utility, so no coding experience required to build custom artefacts CSV/Delimited files (tab-separated, space-separated, or custom delimiters) and SQLite databases to bring data into the offered tool from other sources without needing to know XML/Python or API. **47)** Should have a platform that allows forensics professionals access to repository of Custom artefacts and option to upload custom scripts that they have built, and help their peers with their cases, or download artefacts others have built to help with their own cases. **48)** Add hash sets to either filter out non-relevant files to enhance search performance and reduce false positives or add hash sets that will specifically call out and identify known bad pictures and videos. **49)** Enhanced searching, sorting and filtering – search, sort and filter artefact data for relevant keywords, time/date stamps, tags or comments, or layer filter criteria to pinpoint items in a powerful and intuitive, but natural interface. Support filter stacking for multiple filters. **50)** Should capture web pages as they are at a specific point in time for situations where the web pages need to be displayed in an environment where Internet access is not available (such as a court room). **51)** Support multiple data views, including Column/Table view, Summary Row view, World Map view, Timeline view, Chat Threading view and Histogram view. **52)** Support to export & merge portable case and share with other stakeholders without the need for the software license or the need to install the software, the user can select different types of items to be included according to tags, comments and categories. **53)** Should have a feature to reduce overexposure to illicit/ disturbing content extracted to protect improve investigator wellness. This feature should be configurable and optional, allowing examiners to work the way that they want. Blur or block media thumbnails, Mute audio on videos, Set timer reminders to take breaks or alerts to stop grading, View grading progress and set goals for amount of media graded **54)** Should support Dark mode to help investigators work long hours staring at the screen.	
4.	**UFED 4PC along with cloud analyzer**	**1)** Software Type: ALL IN ONE MOBILE FORENSICS TOOL **2)** Period of Subscription (in Years): 03 (Three) Years On-site Warranty/SMS/Software Subscription. Any Software/ Firmware updates to be provided during the Warranty Period. **3)** The product must have Manufacturer's Authorization Letter. **4)** Training: On-Site product training with certificate.	1 No.

5) Operating Systems supported: Windows 11 Pro 64-bit

6) **Generic Features:**

- The solution should be able to capture critical forensic evidence from mobile devices including mobile phones, handheld tablets, portable GPS devices, drones and devices manufactured with Chinese chipsets.
- It should provide users with all physical file system and advanced logical extraction capabilities for different devices and different Operating Systems as well as allow extraction of Cloud Data source tokens accessed by the Mobile Phone.
- It should support more than 32,000 device profiles and 12,200 different mobile application versions. All the supported mobile device models and device profiles must be tested and verified by the OEM's R&D Team.
- The solution should be able to integrate with a central management platform that can oversee usage, permissions, SOPs, configurations, licensing, and SW updates.
- The extraction software should be touch screen enabled, allowing easy use on tablets.
- The solution should have an autodetect function to locate and identify the mobile device.
- It shall have the ability to offer dynamic profiles of phones, based on IMEI, OS type, version and chipset.
- It should come with a compact and lightweight case with all necessary cables for the supported phones/OS).
- Support Android, iOS, Blackberry, Bada, Symbian & Windows mobile device and generic capabilities for certain chipsets like MTK and Qualcomm, to obtain decrypted Physical Extractions.
- The solution should be technically capable to clone the SIM ID, which allows to extract phone data while preventing the mobile device from connecting to the network.
- The solution should be technically capable to copy a SIM ID from one SIM card to another SIM card or to a vendor's SIM ID access card.
- The solution should be technically capable to perform SIM data extraction, i.e., the extraction of information from a SIM or USIM card.
- It should be able to support file system extraction of blocked application data by downgrading the APK version temporarily for Android devices running on Android 6 and above.
- The solution should be technically capable to extract flight data and multimedia files from supported drones, i.e., to perform physical extractions, as well capture images of drones.
- The solution must support the use of custom-made proprietary boot loaders instead of the 3rd party bootloaders.
- The software should provide lock bypassing physical extraction support for devices with Coolsand based chipsets.
- The software should allow examiners to perform a quick selective extraction of specific applicationsor files, while doing Full File System extraction for supported Android as well as iOS devices.
- The software should also allow selective extraction of only cloud tokens from the phone while doing Full File System extraction.

		• It should provide a simple extraction flow with generic extraction for unsupported devices. • The software should be supplied with USB 3.0 adapter which connects to PC's USB port for faster extraction. This adapter should also have a RJ45 port for device connectivity. • The software should also be supplied with a multi-SIM adapter with support for Micro, Nano and standard SIM cards. • The software should also be able to quickly capture the chat data, by automatically taking screenshots from any Android device. It should also allow the user to perform a text search on the captured screens as well. This should support applications like WhatsApp, Signal, Instagram and Snapchat • The software should be able to categorize the applications found in mobile devices and user should be able to filter by category. This capability should be available for supported Android as well as iOS devices. • The software should have a workflow guidance widget to help managers and administrators to guide, control and enforce working procedures. • The software should include a copy functionality which allows selection of specific files such as images, videos, audio and documents from any unlocked device such as Android & iOS phones or removable drives. **7) Extraction Support** • It should support advanced unlocking capability to perform Full File-System extraction from locked Samsung Exynos FBE and FDE devices with Secure start-up. This capability should support devices S8, S9, S10, and A10-A50 series, runningup to the latest Android 11. It should allow users to upload their own custom dictionary to enhance the unlocking process to make the process easier and faster. • There should be a capability which allows lock bypass and get full file system & physical data collection from Samsung S8, S8+, S9, Note8 and Note 9 models with Qualcomm chipset. As part of full file system extraction, there should also be ability to extract Samsung Secure Folder. • It should allow full backup of the Signal database from unlocked Android devices. • The software should support Full File System extraction for the latest unlocked Samsung Exynos high-end devices like S20, S21 running on Android 11.S21 should be with Android 12 as well. • The software should support extraction of Full File System data from unlocked Qualcomm chipset-based Samsung devices like S9, S10, S20, S21, S21 Ultra 5G, S21 Plus devices running on latest security patch level and up to the most recent Android 11. • The software should allow full file system extraction for unlocked Huawei Kirin devices running Android 9 and higher. • The software should allow collection of data from applications like Signal Private Messenger, Samsung Health and Proton Mai that	

leverage keystore for additional security using methods like full file system extraction for wide range of Android devices.

- The software should have support for a generic Full File System or Physical Extraction for unlocked high-end Android devices with Qualcomm chipsets. This capability should be available for the latest devices from major Android vendors such as Samsung, Huawei, Xiaomi, OPPO, OnePlus, VIVO, as well as devices from Nokia, LG and Motorola, running on Android Versions from 7 up to 10.
- There should be support for Full File system extractions from latest high-end Android Qualcomm devices such as Samsung Galaxy S21, S21 Ultra 5G and S21 Plus, Xiaomi Mi 11, One Plus 9, Redmi K40 pro, and others.
- The software should at least provide the following extraction methods to the user: Selective Filesystem Extraction, Selective App data extraction, Selective cloud token extraction, EDL extraction with decryption, MTK Live, Qualcomm Live, Smart ADB, Samsung Qualcomm, Samsung Decrypting Exynos, Samsung MTK, Samsung Spreadtrum, Samsung Exynos Physical Bypass, Generic Android Unlock using Lockpick, APK Downgrade (Android 6 & above), Huawei Kirin extraction, LG LAF, Advanced ADB, TWRP, Coolsand chipset extraction.
- It should provide capability for Nokia feature phones with proprietary Nokia OS and MTK & Spreadtrum chipsets to get physical extraction from Nokia 105, 110, and 130 families.
- The software should have support to bypass pattern, password and pin locks and overcome encryption challenges for a wide range of Qualcomm EDL, Qualcomm and Exynos based supported Samsung, Motorola, LG and Sony devices.
- The software should retract a range of data e.g., Call Logs, Contacts, Calendar SMS, MMS, Video, Image, Apps Data, GPS Trail, Chat, E-mails etc.
- It should support custom boot loaders to ensure forensically sound bit-by -bit physical extractions, without tampering the data.
- It should have support for data extraction, decoding and analysis for unlocked devices running up to iOS 15.2.
- The software should be able to support full file system extraction using Checkm8 capability for Apple iPhone 7,7+,8.8+ and X for iOS 15.2 depending on the iPhone device supported based on Apple official release.

Additional Points:

- Support for different handsets brands like Apple, SANYO, KYOCERA, Motorola, ASUS, Sharp, Lenovo, HUAWEI, CASIO, NOKIA, NEC, Samsung, iPhone, Xiaomi, OPPO, VIVO, OnePlus, HYUNDAI, BlackBerry, ZTE, LG, Acer, Qtek, Vodafone, Telit, Toshiba, Plam, i-mate, Ubiquam, Haier, Zonda, Sony Ericsson, Samsung, HP, Jaga, Sagem, Alcatel, Mediatek, HTC, etc.
- It should be able to integrate with Active Directory for user authentication.

		8) **Support for Various Phones:** **Android Phones:** • It should support unlocking with physical extraction for at least 100 Qualcomm and Exynos based Samsung devices, including S7, S7 Edge, S6, S6 Edge+, Note 5, A5, A7, J4+, J5, J6, J7 and J8 families. • The software should be able to support full file system extraction on more than 12 Samsung Exynos devices which includes S10, S10+, S10e and A10-A50 phone model. • The software should able to support Samsung devices with full disk encryption such as Samsung S9 or Samsung Note 9 running on Android 10. • It should support lock bypass using file system extraction for latest Samsung devices like Galaxy J7, Galaxy S8, Galaxy Note8 and Galaxy S8+. • It should have lock bypassing decrypted physical extraction capability for Qualcomm Android devices including LG, ZTE, Xiaomi, Huawei, Alcatel and Motorola. • It should be able to perform selective file system extraction on popular Samsung models with the Qualcomm processor (SOC). • The software should have a capability to extract Qualcomm chipset phone in a generic option that support popular brand like Samsung and Huawei. • The software should have a capability to extract MTK chipset phone in a generic option. • It should have decrypting bootloader capability for Huawei devices with HI Silicon Kirin chipsets and Samsung devices with Exynos processor. • It should be able to allows users to perform a full file system and selective extraction on smartphones with the Huawei HI Silicon KIRIN 970 processor and other popular devices with the KIRIN 659, 960 and 980 chipsets For Huawei and Huawei Honor must be running android 8 and 9. • It should support Physical Extraction via ADB for android devices directly to any USB storage or an SD card connected to the device. This method should be generic and should be supported across most Android phones available in the market. This method should support android devices including OS version 7. • It should support Physical Extraction over ADB for Samsung devices running up to Android OS v8. • It should support bootloader-based physical extraction for zte, Alcatel and Xiaomi devices running Qualcomm chipset. • It should support Partial File System extraction while bypassing User Lock for more than 100 Android devices. • It should have physical extraction method from more than 400 locked Android based devices bypassing any type of lock (Pattern/PIN/Password) using proprietary boot loaders, enabling a forensically sound extraction process. • It should support automatic detection of supported devices. It should also support manual search for devices by manufacturer, model and IMEI number.	

		• It should be able to perform physical, full file system and selective file system extraction on Smartphone with Samsung Qualcomm Processor • It should acquire apps data from Android devices via all extraction types including: Facebook, Facebook Messenger, Google+, PingChat! (aka Touch), Skype, Twitter, Viber, Yahoo Messenger, WhatsApp, TigerText, Dropbox, QIP, Kik Messenger, Evernote, Kakao Talk, ICQ, Vkontakte, HideSMS, Kakao Story, MeetMe, Coco, Google Duo, FitBit, Zalo, Yubo, Zello. • Physical Extraction of Major Device Support should at least include the following phones: • HTC – HTC Evo, HTC One M8, Incredible, Desire 310, Desire C, 2PS6500 10, U11, U-1w Ultra. • Motorola – Milestone, Milestone 2, Droid, Droid 2, Droid 3, Droid X, Droid Razr, Razr Maxx, Defy, Moto X Play, Moto G, XT1710-02 Z2 Play, G4, G5, Nexus 6. • Samsung – Galaxy S7, Galaxy Note 7, Galaxy Note 5, Galaxy Note 8, Galaxy S6, Galaxy S8, Galaxy S8+, Galaxy S6 Edge, Galaxy S5, Galaxy S4, Galaxy SIII Family, Galaxy SII, Galaxy Note 4, Galaxy Note II, Galaxy Mega, Galaxy s5 duos, Galaxy alpha, J3 Neo, J5, J7, A5 and A7 • LG – G5, G4, G3, Optimus, Optimus one, Optimus 3D, Optimus black, Nexus 5X, L51AL, Fiesta LTE, K10, G6, V30, Nexus 5x, H820 G5, LM-X210MA & MP260. • Indian Phones – Intex Aqua Amoled, Intex Aqua Core; Intex Cloud Y5; Intex Aqua i7; Karbonn A12+; Karbonn A25, Karboon S99 Titanium, Xolo A50zip0S ; A114R Canvas Beat, Micromax A190 Canvas HD Plus, Intex Aqua ring. • Huawei – Ascend, Honor 3x, 5 vision, Honor 5x, Honor 4c, H1611, Mi5, C8815, Nova 2i, U8600 Move, Mate 8, Honor 8, Nexus 6P, P10, Mate 10, P9. • Sony: Xperia X, Xperia z5, Xperia e5, Xperia X Dual, XZ, L1, XA1 Plus, Xperia XA1. • Others: Asus Zenfone 4 Max, Xiaomi Redmi 3S/4, Oppo F3, Alcatel 5090i A7. Blackberry Phones: • It should enable physical extraction and decoding from BlackBerry devices running OS 4-7. Physical extraction should be performed using proprietary boot loaders, enabling a forensically sound process. Real-time decryption should be enabled for selected devices. • It should support advanced decoding of existing and deleted data for Blackberry running OS 4-7: • BBM history (if enabled by the user) • BlackBerry Messenger (BBM) messages including Deleted messages and chats, message attachments, contact photos, BBM from groups: Chats, contacts and shared photos. • Installed applications data: WhatsApp, Facebook, Twitter, Google Talk (Gtalk), UberSocial (WhatsApp data retrieval includes decryption of the database and recovery of contacts, chats, chat attachments and user account).	

		• Address book, SMS, MMS, Emails, PIN messages, Calendar entries, Memo pad notes, Web browser history, Web bookmarks, Bluetooth devices and Cookies. • Recent email contacts (BB OS 6 and above, where available). • Device Info (Model, IMEI\MEID, ICCID, PIN, OS version, Platform, Supported Networks). • REM files – decryption of encrypted files on external memory. Windows Phone: • It should support physical extraction and decoding of devices running Windows Phone devices running OS versions 8.0, 8.1 and 10. It should also support obsolete OS including 6.0 and 6.5. • JTAG decoding of contacts, call logs and SMS from Windows Phone 8.x devices is enabled via physical extraction. • The Devices supporting Physical Extraction should at least include HTC Pro, HTC HD2 T9193, Xperia X1, Nokia Lumia 520, LG GM750 and other popular models. • It should support applications for Windows Phone devices running OS 8.1 including apps such as Facebook, Facebook Messenger, Waze, WhatsApp, ooVoo, Skype, Voxer, Kik and Odnoklassniki. • Support for .SDF files being used by Windows Phone apps. Nokia BB5 Phones: • It should support bit-for-bit physical extraction from locked and unlocked Nokia BB5 devices using proprietary boot loaders. • It should enable Password extraction on selected devices. • It should support decoding of Symbian databases including Decoding of intact and deleted contacts, SMS, MMS and call logs; Decoding support for multilingual content. • It should support physical decoding of data obtained through Chip Off method for BB5 devices. Portable GPS Device: • It should enable physical extraction and decoding of data from a range of portable GPS devices. The Decoded data should include: Entered locations, GPS fixes, Favorite locations, GPS info. • It should provide a solution to the encrypted TomTom trip-log files that reside in the TomTom device STATDATA folder. It should support Extraction and decoding of existing and deleted data from TomTom devices. TomTom extraction and decoding of information includes: Home, Favorites, Recent, User entered, Locations, Last journey, Location, Date & Time, Routes, GPS fixes (also deleted), Deleted locations (of all categories). • It should support Data Extraction from Garmin & Mio devices. Extracted data includes: Favorites, Past journey (containing all the fixes during the journey), deleted GPS fixes. Feature Phones: • It should enable physical, file system and logical extraction, and decoding from selected devices. Decoding of intact and deleted data: Phonebook, SMS, MMS, calendar entries, SIM ID and more.	

		• The Supported Phones (for either Physical/ File System/ Logical) should at least include: • Nokia: 1280, 1616, 1650, 1661, 1661-2b, 1680 Classic, 1800, 2720 fold, 2720a-2b, 2730 Classic, 2760, 3109 Classic, 3110 Classic. • Samsung: SGH-C120, SGH-A127, SGH-M130L, SGH-A137, SGH-T139, SGH-J150, SGH-X150, SGH-X160, SGH-X166, SGH-X168, SGH-C170, GT-E1195, GT-E1230, SGH-E1310B, SGH-B2100. • LG: KP175, KP202 i-mode, GB220, KG220, CG225, KG225, GB230 Julia, KG290, NTLG300GB, KG320, KG320S, KG328, L343i, KF350, KF600, KE800, KG800, KE850 Prada, KE970, Shine, C1100, L1100. • Motorola: E1 ROKR, C113, C117, C118, C119, C115, C139, C140, V300, V303, V330, W375, E398, V400, V500, V505, V525, V551, V620, V635L, C975, E1000, V1050. Chinese Chipsets Based Phones: • Using proprietary boot loaders, it should perform a bit-by-bit physical extraction, from devices manufactured with Chinese chipsets, accessing the device's memory, whilst maintaining forensic integrity. The boot loaders prevent the tampering of data, during physical extraction. • In addition, it should bypass user lock code from these devices and decode the user lock from the extraction within Tool. • The tool should provide generic extraction with Decrypting bootloader for MTK based chipsets including 6580, 6735, 6737, 6753, 6755, 6757 & 6797. • The software should be able to supports acquisition and decryption of 80+ MTK distinct chipsets and have the ability to conduct Physical or Full file system (FDE &FBE) extraction of unlocked MTK devices with ADB enabled. The Android OS supported should be up to version 9. IOS Phones: • The full list of supported iOS devices should minimally include the following: iPhone 2G, iPhone 3G, iPhone 3GS, iPhone 4, iPhone 4S, iPhone 5, iPhone 5S, iPhone 5C, iPhone 6, iPhone 6Plus, iPhone 6s, iPhone 6s Plus, iPhone 7, iPhone 7 Plus, iPhone 8, iPhone 8 Plus, iPhone X, iphone XS, iphone 11, iphone 11 Pro, iphone 11 Pro Max, iphone 12 mini, iphone 12, iphone 12 Pro, iphone 12 Pro Max, iPod Touch 1G, iPod Touch 2G, iPod Touch 3G, iPod Touch 4G, iPod Touch 5G, iPad Mini, iPad 1, iPad 2, iPad3, iPad 4, iPad Pro, iPad Air, iPad Air 2. • Decoding of additional iOS databases from KnowledgeC, Health App, Siri native messages and Telegram should be supported. 9) Should include toolkit box containing cables, adaptors, accessories, etc.	
5.	**DVR Examiner**	**1)** Software Type: DVR DATA EXTRACTION TOOL **2)** Period of Subscription (in Years): 03 (Three) Years On-site Warranty/SMS/Software Subscription. Any Software/ Firmware updates to be provided during the Warranty Period. **3)** The product must have Manufacturer's Authorization Letter.	1 No.

		4) Training: On-Site product training with certificate. **5)** Operating Systems supported: Windows 11 Pro 64-bit **6)** The tool must exhibit the capability to perform video extraction and recovery from DVR video surveillance systems in a forensically sound manner during investigative procedures. **7)** User-friendly graphical user interface (GUI) featuring a Case Wizard, allowing investigators to effortlessly construct a simple case centered around one piece of evidence or expand to more complex cases with multiple pieces of evidence. **8)** The software ought to be compatible with over 50 of the most widely used native or proprietary video formats sourced from various recording devices, including DVRs, as well as open video formats such as H264, MOVs, MP4s, and AVIs. **9)** It should be capable of recovering and analyzing video evidence obtained from popular cloud video sources like Ring and Arlo, using user credentials. **10)** The tool must support the recovery of video content and metadata from diverse sources such as supported body cams, dash cams, mobile devices, drones, and more, with compatibility for Open AVI and MP4 in supported codecs. **11)** The software is designed to perform MD5, Sha-1, and Sha-256 hashing of extracted files, ensuring the creation of forensically sound reports. **12)** Immediately accessible comprehensive detection results, including filesystem-specific information such as Filesystem Name, version, format, and Output, upon connecting the DVR Drive/Image. **13)** The software incorporates keyboard shortcuts for various functionalities, such as adding incident details, location, device, bookmarking, tagging, managing date and time offset, generating reports, adjusting settings, starting a new case, restarting, and exiting. This ensures ease of use and expedites results. **14)** The dashboard includes a view of keyboard shortcuts for quick access, aiding examiners in accessing all available keyboard shortcuts and their associated functions at any time during investigations. **15)** The option to conduct an Accessible scan and inaccessible options as distinct processes is provided to ensure examiners have an option to save time during investigation when the Video of interest is available on the DVR or there is a need for inaccessible scan for bit-by-bit scan. **16)** Ability to ignore indexes during extraction/scan **17)** Investigators should be capable of conducting a focused scan exclusively for Accessible files, streamlining the investigative process and saving valuable time, especially when dealing with identified videos of interest. **18)** Maintain workflow continuity by opening the most recently accessed cases directly from the start-up window. **19)** Should have Automation capability to Choose Post-Scan export jobs to automatically execute upon the completion of the initial scan, offering the flexibility to export all or a selected set of clips in Excel or PDF formats to a designated folder in a specified media format with a chosen hash algorithm.	

20) Pre-select post-scan jobs, including options such as clips recorded within specific date and time ranges, specific channel numbers, and thumbnails from particular clips/DVR sources.

21) Prior to extraction/scanning, configure scan filters and date/time offsets to minimize scan time and yield immediately relevant results.

22) Synchronized matrix view preview of multiple videos (minimum 4) at one time

23) Create notes, tags, and bookmarks for others to review important pieces of evidence and use them to generate reports.

24) Sub-clipping to extract pertinent information from larger video files. Clips from DVRs can often contain hours of content irrelevant to the case. should allow examiners to create a smaller clip file that contains a segment from a larger parent clip allowing examiners to easily focus on the footage of interest.

25) Filters to also include capability to filter based on specific date and time, applying specific time range for all days, and option to select specific week days.

26) Clip list filtering to apply clip attribute filter including clip size clip duration, sources, channels, include unknown channels, sources, status, tags, bookmark etc

27) Should have specific filters on all columns with and/ Or filtering with is equal to, is not equal to, is less than, is less than or equal to, is greater etc than option

28) Bypass passwords and skip unfamiliar or complicated third-party menus or interfaces.

29) Easily organize evidence by location and/or device to handle complex cases spanning many sources and locations creating a easy to understand case hierarchy.

30) Ability to recover deleted or partially overwritten video from supported surveillance DVRs.

31) Should support to cull down hours of video into the few seconds that matter with sub-clipping.

32) Ability to run videos at .5x, 1x,2x,4x,8x,16x speed to help examiners play slowly or quickly through the clips.

33) Should be capable to Highlight video clips, segments, or specific frames with items of interest and add detailed notes and reporting using notes, tags, and bookmarks that other stakeholders can review.

34) Should support Setting default values and properties to save time later when running through workflows. Changes made in the Settings section are applied across all future cases and actions.

35) A notification icon should be prominently displayed, with its colour indicating the severity level of notifications (red, yellow, green, or white).

36) Option to Pause and play any Job during the process.

37) Pre-scan troubleshooting options:

- Force 512 Sector Size for Forensic Images
- Force sector count
- Force a Detection for a particular filesystem with option to Default detect only filesystem, Filesystem 20D, Filesystem 20D secondary,

		Filesystem 60D **38)** Should support creating a thumbnail automatically by opening a clip in the preview page, or manually by selecting a frame from the clip timeline for videos supporting preview. **39)** Should allow Drag and drop column headings into different locations in the table to re-organize information and headings into the sort header to group clips by the attribute value. **40)** Should support exploring data from both the clip list and from a playlist allowing investigators to Compile a list of clips to export as they analyze the clips and then run the export, Export all clips immediately, Export selected clips immediately, Custom export selected clips immediately **41)** The software should be capable of generating forensically sound reports at any point during the extraction process or upon case completion. **42)** It features an interactive report generator, enabling investigators to create reports such as Case Summaries, Clip Lists, Gallery Previews, Audit Logs, or Export reports. **43)** The software should have the capability to create reports simultaneously to multiple destination folders without any limit. **44)** Should support evidence source in form of physical DVR Drive, Forensic Image (DD & E01), Video file from different sources, Cloud Camera (Ring & Arlo with MFA) **45)** It has the capacity to rectify incorrect date and time settings on recorded videos, enabling users to establish offsets for individual or groups of clips. **46)** Users can include an adjusted date and time timestamp overlay on exported clips using the software. **47)** The software should include an in-application automated prompt for new versions/updates. **48)** Should have built-in functionality in the software to directly send unsupported files or filesystems to OEM Tech support when the file or file system is not recognized, ensuring future support for such unrecognized data. **49)** The software should maintain an audit log detailing all actions carried out during a case, including selected options and filters during the investigation, enabling examiners to export a comprehensive report for tracking purposes. **50)** Ability to queue clips for export from either the clip list or from the Preview view of a clip. **51)** Case Summary tab that displays important case information such as Case Details, Incident Details, Locations, Devices and Sources, Case Statistics, and an Audit log of all actions performed within the software for the open case. **52)** Should let examiners toggle between light mode and dark mode to help investigators work long hours staring at the screen. **53)** Should have utility to empower frontline officers to collect and report on fleeting digital evidence. The tool should be capable to install and actively use simultaneously on any number of windows tablet/ Laptop and record videos directly from a DVR in a forensically sound manner with	

		Timestamp and MD5 & SHA Hash. **54)** The utility should help the investigator to record the date and time mismatch in the DVR System at the crime scene. **55)** Quickly get photo, video with an external or internal camera or by connecting to the victim or witness's mobile phone, or memory card as additional/ supporting case video and help create easy forensically sound reports with Hash value, Source device information and geolocation if available on picture or video metadata. **56)** Should include toolkit box containing cables, adaptors, accessories, etc.	
6.	**Encase Forensic**	**1)** Software Type: DIGITAL FORENSICS PLATFORM SOFTWARE **2)** Period of Subscription (in Years): 03 (Three) Years On-site Warranty/SMS/Software Subscription. Software/ Firmware updates to be provided during the Warranty Period. **3)** The product must have Manufacturer's Authorization Letter. **4)** Training: On-Site product training with certificate. **5)** Operating Systems supported: Windows 11 Pro 64-bit **6)** Imaging: Should support the widest variety of devices, from the latest smartphones, tablets, GPS devices, and including more than 36,000 mobile device profiles, all while empowering the examiner to conduct logical and physical acquisitions. **7)** Should have inbuilt LinEn utility to acquire evidence via boot disk and WinEn utility to acquire RAM evidence. **8)** Evidence Processing: Should have ability to process and to parse evidence, data structures, initiate searching, and data carving features. These consist of recovering evidence related to Internet, email, registry, compound files, event logs, Windows and OS X artefacts, along with many others. **9)** Signature Analysis: Should perform analysis of files based on their signatures and file extensions. **10)** Hash Analysis: Should calculate hash values for entries, ability to add hash values into a hash set, and to organize hash sets into a hash library. **11)** Bookmarks and Tags: Should bookmark or tag a single entry, multiple entries, or to bookmark highlighted data for evidence. **12)** Raw Searching: Should have raw keyword searching feature on the evidence entries. **13)** Conditions Filters and EnScript Programs: Should create custom conditions or utilize built-in filters and powerful EnScript programs for analysis of the evidence. **14)** Reviewing Email: Should support email review and email recovery. Support email analysis of various email clients as: Outlook PST/OST, Outlook Express DBX, Exchange EDB, Notes NSF, EML (Microsoft Internet Mail), Eudora, Thunderbird, Quickmail, Netscape, AOL etc. **15)** Encryption Support: Should support encryptions such as Microsoft BitLocker, Guardian Edge Encryption Plus/Encryption Anywhere/Hard Disk Encryption, UtimacoSafeGuard Easy, McAfee SafeBoot, McAfee Endpoint Encryption, WinMagicSecureDoc Full Disk Encryption, PGP Whole Disk Encryption, Checkpoint FDE (Full Disk Encryption), Dell FDE (Full Disk	1 No.

		Encryption), Apple File System (APFS) Encryption. **16)** Reviewing Internet: Should be capable to parse numerous Internet data storage structures. **17)** Compound File Analysis: Should be able to access data stored within compound files. **18)** Case Analyzer: Should report Review capabilities across collected data from registry, inside the Case Analyzer. **19)** Creating Triage and Basic: Create simple reports or unlock the ability to customize report templates for reporting. **20)** Apple File System (APFS) support: Should support APFS, the file system used in helping investigators conduct targeted data collections from APFS and send the output as an EnCase logical evidence file. **21)** AFF4 support: Provides physical and logical read capabilities to allow for ingestion of evidence from other investigative tools, enabling all relevant evidence to be collected within a single case file and helping investigators quickly gain a more comprehensive view of the evidence available to their case. **22)** Apple T2 Security Bypass: Should be able to acquire machines equipped with Apple T2 Security chips without additional hardware, drive partitions, or hassle. And if the user is logged in, no credentials are required. **23)** Volume Shadow Copy Capabilities: Should be able to examine Volume Shadow Snapshot (VSS) backups, also known as volume shadow copies, generated by Microsoft Windows, allowing investigators to recover deleted or modified files, as well as full volumes and learn what may have taken place on a system before the investigation. **24)** Connect to the Cloud: Should enable Investigators to collect evidence from cloud-based applications, including social media, storage, and communication tools. **25)** Enhanced indexing engine: Should empower investigators to conduct investigations with powerful processing speeds, advanced index searching, comprehensive language support and optimized performance. **26)** Extensibility: Should offer extensibility through EnScripts, which are automated code commands that streamline and automate tasks and extend the capabilities of the solution to help the examiners complete investigations more efficiently. **27)** Deep Forensic Analysis: The software should not only deliver an "artefacts first" approach but also let investigators dive deep into the operating system to locate artefacts that would otherwise be well-hidden by bad actors. **28)** Media Analysis: Should be able to process your evidence with the Media analysis module which assigns confidence level scores to all supported images for 19 categories. **29)** Workflow Automation: Should deliver automated investigation workflows so examiners can easily navigate through the solution to enhance how they uncover evidence. **30)** Reporting: Should provide customizable templates to help examiners create compelling, easy to read, professional reports that can be shared for every case.	

		31) Continuous updates and support for the warranty period notified in the tender from the vendor to ensure that the tool remains up to date with the latest forensic and investigative techniques. **32)** Should include toolkit box containing cables, adaptors, accessories, etc.	
7.	**Oxygen Forensic Detective with cable kit**	**1)** Software Type: ALL IN ONE DIGITAL FORENSICS PLATFORM SOFTWARE **2)** Period of Subscription (in Years): 03 (Three) Years On-site Warranty/SMS/Software Subscription. Software/ Firmware updates to be provided during the Warranty Period. **3)** The product must have Manufacturer's Authorization Letter. **4)** Training: On-Site product training with certificate. **5)** Operating Systems supported: Windows 11 Pro 64-bit **6)** Data Extraction: Should be capable of extracting data and artefacts from multiple devices, including mobile phones and computers. This includes comprehensive extraction methods for various operating systems and device types. It should support extraction from a wide range of devices, ensuring compatibility with the latest models and versions. **7)** Application Support: Should extract data from 40,000 App versions of 800+ Unique Apps. **8)** Computer Data Extraction: Should be capable of extracting data from computers running Windows, Linux, and macOS operating systems. This includes extracting user profiles, browsing history, email communications, documents, multimedia files, and other relevant data from desktops, laptops, and servers. The software should support both live and dead system analysis for thorough forensic examinations. **9)** Desktop App Data Extraction: Should include a utility like KeyScout for extracting and decrypting credentials, system files, and user data from web browsers and desktop apps. This includes extracting login credentials, chat histories, attachment files, and other data from popular desktop applications and web browsers used for communication and productivity purposes. The software should ensure compatibility with a wide range of applications for comprehensive data extraction. **10)** Mobile Device Extraction: Should be able to extract data from over 31,000 different mobile devices running Apple iOS and Android operating systems. This includes the extraction of various data types such as contacts, messages, call logs, photos, videos, and app data from smartphones and tablets. The software should support both logical and physical extraction methods for comprehensive data retrieval. **11)** Drone Data Extraction: Should be capable of extracting and analyzing data from drones, including physical dumps, flight logs, and mobile applications. This includes parsing GPS locations, flight telemetry data, media files captured by drones, and other relevant information to reconstruct flight paths and analyze drone activities. The software should support major drone manufacturers and models for broad compatibility. **12)** IoT Device Data Extraction: Should support the extraction and analysis of data from IoT devices such as Amazon Alexa and Google Home. This includes accessing data stored on these devices or associated cloud	1 No.

		services, extracting voice recordings, device settings, activity logs, and other relevant information for forensic analysis. The software should offer methods to extract data from IoT devices securely and comprehensively. **13)** Cloud Services: Should support extraction from over 100 cloud services, including popular platforms like WhatsApp, iCloud, Google, and Facebook. This includes the ability to extract data from cloud backups, messages, media, and other relevant information stored on these platforms. The software should ensure compatibility with a diverse range of cloud services, enabling thorough digital investigations. **14)** Wearable Device Data Extraction: Should support the extraction of data from popular wearable devices and health apps, including Apple Health, Samsung Health, and Fitbit. This includes extracting health and fitness data, activity logs, sleep patterns, and other relevant information from wearable devices and associated mobile applications. The software should ensure compatibility with major wearable device brands and models. **15)** Simultaneous Device Acquisition: Should enable simultaneous acquisition of several devices to save time during investigations. This includes the ability to connect and acquire data from multiple devices concurrently, optimizing the workflow for forensic analysts and investigators. The software should support parallel processing of extraction tasks while maintaining data integrity and forensic soundness. **16)** Backup and Image Import: Should support the import of various backups and images, including iTunes, Android backups, and GrayKey. This includes importing data from forensic images, backups created by mobile device management (MDM) solutions, and other image formats commonly used in digital investigations. The software should ensure seamless integration of imported data for comprehensive analysis. **17)** Screen Lock Bypass: Should include proprietary methods to bypass screen locks on mobile devices and find passwords to encrypted backups and images. **18)** Cloud Service Credential Extraction: Should provide the ability to extract credentials and tokens directly from devices or computers for accessing cloud services. This includes extracting login credentials, access tokens, authentication cookies, and other authentication artifacts required to access cloud storage and communication platforms for forensic analysis. The software should support secure extraction of credentials without altering the original data. **19)** Drone Data Parsing and Analysis: Should enable verbose data parsing and analysis from drone collections, flight logs, mobile apps, and cloud services. This includes parsing and analyzing GPS locations, flight telemetry data, media files, application logs, and other relevant data sources to reconstruct drone activities and identify key events or patterns for forensic examination. The software should offer comprehensive analysis tools for interpreting drone data effectively. **20)** GPS Location Parsing: Should support the parsing of GPS locations, device telemetry, and drone images and videos. This includes extracting geo coordinates, altitude, speed, direction, and other telemetry data from various sources such as photos, videos, apps, drone flight logs, and cloud	

		services for mapping and analysis purposes. The software should provide accurate and reliable parsing of location data for forensic investigations. **21)** Smartwatch and Fitness App Data Extraction: Should offer logical acquisition of smartwatches and fitness apps data from both mobile devices and cloud services. This includes extracting device model, contacts, calls, messages, multimedia files, health and fitness data, and other relevant information from wearable devices and associated mobile applications for forensic analysis. The software should ensure compatibility with major smartwatch brands and fitness app platforms. **22)** Optical Character Recognition (OCR): Should include OCR functionality for converting text within images to machine-encoded text. This includes automatically recognizing and extracting text content embedded in images, screenshots, or documents to enable text-based searching and analysis of visual information. The software should support accurate and efficient OCR processing for various languages and fonts commonly encountered in forensic investigations. **23)** Statistical Analysis Tools: Should provide statistical analysis tools for both device data and investigator interactions with the evidence. This includes generating statistical reports, visualizing data trends, identifying patterns, and conducting correlation analysis to facilitate data interpretation and decision-making during forensic examinations. The software should offer customizable statistical analysis features tailored to forensic workflows and requirements. **24)** Social Graph Exploration: Should feature a built-in Social Graph for exploring social connections between device owners and contacts. This includes visualizing communication networks, identifying key individuals or groups, and analyzing communication patterns across multiple devices or accounts to uncover relationships and interactions relevant to the investigation. The software should offer interactive and intuitive visualization tools for social network analysis. **25)** Timeline View of Device Events: Should offer a Timeline view of all device events, including chats, calls, web activity, and calendar events. This includes organizing chronological events in a timeline format, filtering and sorting events based on various criteria, and correlating events across multiple devices to reconstruct timelines of user activities and interactions for forensic analysis. The software should provide a comprehensive and user-friendly timeline interface for data visualization and exploration. **26)** Mapping Capabilities: Should include mapping capabilities for visualizing device movements and frequently visited places. This includes plotting geo coordinates on interactive maps, analyzing location data patterns, identifying common routes or hotspots, and visualizing spatial relationships between devices or individuals for forensic mapping and geospatial analysis. The software should support both online and offline mapping functionalities for flexible data visualization and exploration. **27)** Search Functionality: Should allow investigators to search across devices for various types of data, including text, phone numbers, and geo coordinates. This includes conducting keyword searches, regular expression searches, and custom searches across single devices, multiple devices, or	

		entire case databases. **28)** Should include toolkit box containing cables, adaptors, accessories, etc.	
8.	**Passware Kit Forensics**	**1)** Software Type: ALL IN ONE PASSWORD RECOVERY TOOL **2)** Period of Subscription (in Years): 03 (Three) Years On-site Warranty/SMS/Software Subscription. Software/ Firmware updates to be provided during the Warranty Period. **3)** The product must have Manufacturer's Authorization Letter. **4)** Training: On-Site product training with certificate. **5)** Operating Systems supported: Windows 11 Pro 64-bit **6)** Should recover passwords for 200+ file types and decrypt hard disks providing an all-in-one User interface. **7)** Should scan computers and network for password-protected files (including Encryption Analyzer Professional). **8)** Should acquire memory images of the seized computers (including FireWire Memory Imager) **9)** Should retrieve electronic evidence in a matter of minutes from a Windows Desktop Search Database (incluing Search Index Examiner). **10)** Should support Distributed Password Recovery. **11)** Should run from a USB thumb drive and recovers passwords without installation on a target PC (including Portable Version). **12)** Should instantly recover many password types. **13)** Should instantly decrypt MS Word and Excel files for all versions (including Decryptumattack). **14)** Should reset passwords for Local and Domain Windows Administrators instantly. **15)** Should recover encryption keys for hard disks protected with BitLocker, including BitLocker To Go. **16)** Should decrypt True Crypt. **17)** Should recover from 8 different password attacks (and any combination of them) with an easy-to-use setup wizard and drag & drop attacks editor. **18)** Should use multiple-core CPUs and NVIDIA GPUs efficiently to speed up the password recovery process. **19)** Should provide detailed reports with MD5 hash values. **20)** Should be capable of recovering Mac User Login passwords and FileVault2 keys from computer. **21)** Should support Distributed and Cloud Computing password recovery on both Windows and Linux platforms. **22)** Should recover Passwords for Windows users from a memory image or a standalone SAM file, including UPEK. **23)** Should recover passwords for email, websites and network connections from standalone registry files in a very short time. **24)** Should have Search Index Examiner to retrieve electronic evidence from a Windows Desktop Search Database.	1 No.
9.	**Forensic Toolkit (FTK)**	**1)** Software Type: DIGITAL FORENSICS PLATFORM SOFTWARE **2)** Period of Subscription (in Years): 03 (Three) Years On-site Warranty/SMS/Software Subscription.	1 No.

3) The product must have Manufacturer's Authorization Letter.

4) Training: On-Site product training with certificate.

5) Operating Systems supported: Windows 11 Pro 64-bit

6) Should provide a platform to do thorough computer forensic examinations and help law enforcement officials, corporate security, and IT professionals access and evaluate the evidentiary value of various data.

7) Should be proposed as a single or suite of software applications compatible with Windows operating system.

8) Should be compatible with VMware and Hyper-V virtual platforms, AWS and Azure Cloud environments, as well as physical servers.

9) Should be compatible with Microsoft SQL and PostgreSQL databases.

10) Should be able to create images of local hard drives, floppy diskettes, CDs and DVDs, thumb drives or other USB devices, entire folders, or individual files from various places within the media in a forensically sound manner by creating copies of data without making changes to the original evidence.

11) Should support processing of different file systems such as APFS, AFF4, CDFS, EFS, exFAT, EXT2FS, EXT3FS, EXT4FS, FAT12, FAT16, FAT32, HFS, HFS+, JFS, NTFS, ReiserFS 3, UFS1, UFS2, VxFS, Windows 8 and Server 2012 ReFS, and XFS.

12) Should be able to ingest various types of data images such as AD1, AFF, DMG, CTR (X-Ways), E01, EX01, L01, Expert Witness, Ghost forensic image, ICS, IMG, IMA, Linux DD, Lx0, Lx01, LVM, LVM2, VHD, VHDX, Raw (.001, .1, .BIN, .DD, .GHO, .RAW, .IMG), Safeback 2.0 and below, SMART (.S01), SnapBack, VDI, VMDK, YAFFS1, YAFFS2, and UFDR.

13) Should be able to ingest various types of optical media images such as MDS, BDAV, CCD, ISO, IsoBuster CUE, NRG, PDI, PXI, CIF, SACD, SVCD, VCD, and VC4.

14) Should be able to examine data that is contained in NTFS Volume Shadow Copies (Restore Points) which can be used to recover renamed and deleted files. The solution should be able to mount and processes each restore point as a separate evidence item. When restore points are processed, a unique file system image for each restore point should be created.

15) Should provide an option to exclude specific data based on different factors from being added to the case when importing evidence. These factors include file type, file date, file size, encryption status, etc.

16) Should be capable of extracting data from various compound files such as archives (7-ZIP, BZIP2, GZIP, RAR, TAR, ZIP), Browser files (Chrome Bookmarks, Chrome Cache, Chrome Json, Chrome LevelDB, Chrome SNSS, Chrome SQLite, Edge Bookmarks, Edge Cache, Edge SQLite, Firefox Cache, Firefox Firefox JSON, Firefox SQLite, IE Cookie Text, IE Recovery, IE WebCache, Safari Plist, Safari SQLite), Email containers (DBX, MBOX, MSG, Mac Outlook OLM, PST, OST, RFC822 Internet Email, Unistore Database), Windows Artefacts (Active Directory, ESE DB, MS Exchange, MS Office OLE and OPC documents, Windows Registry, Windows Thumbnails, Event logs, IIS logs, Windows Firewall logs), Mobile Data (Android applications, Android calendar, Android call history, Android contacts, Android Gmail, Android Hangouts, Android Instagram, Android Kik, Android SMS/MMS, Android Viber, Android WeChat, Android WhatsApp, Blackberry IPD backup, iOS backup, iOS WeChat, iOS WhatsApp), etc.

17) Should be able to generate a digital fingerprint (hash) for individual files within the evidence using algorithms MD5, SHA1, and SHA-256. The solution should be able to identify and mark duplicate files within evidence data based on the file hash.

18) Should be able to identify the files'type based on their signature and mark bad file extensions. The solution should support custom file identifiers to allow administrators specify which file category or extension should be assigned to files with a certain signature. It also should allow to define or change the category associated with any file with a certain file extension.

19) Should be able to detect encrypted files and automatically decrypt the files using the supplied password file.

20) Should be able to perform known-key decryption of encrypted file systems such as EFS, Dropbox DBX files, Lotus Notes stores files, S/MIME email items, Bitlocker partitions, Dell Encryption files, McAfee Drive Encryption images, Safeguard Utimaco files, etc.

21) Should be able to create a searchable index of the words and strings of characters within a case.

22) The user should be able to modify indexing options such as specifying the letters and numbers to index, characters that should be treated as hyphens or space, actions to be taken against binary files, etc.

23) The user should be able to define the list of words to be considered as —noise|| and ignored during indexing.

24) Should be able to create thumbnails from graphic and video files.

25) Should be able to extract EXIF data from multimedia files.

26) Should be capable of locating and carving files and objects on media that have been deleted, lost from the file system, or embedded in other files. Apart from the predefined data carvers, the solution should support creating custom data carvers.

27) Should be capable of analysing graphics and video files and recognizing images such as knife, pistol, vehicle, nudity, banknotes, coins, people, passport, signature, etc.

28) Should be capable of analysing images and recognizing similar faces and objects.

29) Should be capable of analysing executable binaries and zip files located on a disk and identify malicious behaviour.

30) Should have Optical Character Recognition (OCR) feature in 40+ different languages and should be able to detect text from different file formats such as TIFF, BMP, PNG, JPEG, GIF, PCX, TGA, PSD, PCD, etc. The minimum and maximum file size thresholds should be customizable on which the OCR process will run.

31) Should be capable of detecting and summarising operating system artefacts such as installed and autorun applications, prefetch items, ShimCache, Startup items, system services, User Assist, Jump Lists, Links, MRU, Shell Bags, user and group accounts, time zone information, various

Windows event log categories, Windows registry information, device information, network interfaces, network connections and shares.

32) Should be capable of processing Internet browser history for visualisation and extracting data such as cookies, downloads, searched keywords, URLs, URL categorization, etc.

33) Should be able to perform document content analysis for grouping the documents according to their topic and extract data such as phone numbers, email addresses, credit card numbers, etc.

34) Should be able to compare the graphics within evidence to the known Project VIC hash values and flag matched items to identify child sexual exploitation and trafficking contents.

35) Should be able to scrape contact information for identities of interest from signatures in emails from disparate sets of evidence and connect information found in all items to one suspect.

36) Should be able to compare file hashes in the evidence against a database of hashes from files known to be ignorable (such as known system and program files) or with alert status (such as known contraband or illicit material) and allow quick elimination or pinpointing of these files during an investigation.

37) Should allow the investigators to run any Python script against evidence and generate results which can then be added back to the case.

38) Should support emulating what a file might look like in its native application and displaying contents of hundreds of different file formats without the native application being installed.

39) Should have a resizable thumbnail view for reviewing graphics files.

40) Should be able to extract and display various metadata of the files such as file attributes, DOS attributes, NTFS information, Microsoft Office metadata, etc.

41) Should be able to display the file contents in hexadecimal and interpret selected hexadecimal values into decimal integers, possible time and date values, as well as Unicode strings.

42) Should categorise the objects within the evidence based on the file type (graphics, office documents, executables, etc.), file status (encrypted files, deleted items, duplicate items, etc.), file extension, etc.

43) Should have a visualisation feature to provide a graphical interface to enhance understanding and analysis of files and emails in a case.

44) Should be able to provide a visual representation of file categories and file volume within the case as a heatmap view.

45) Should be able to display email data on a timeline view and visualize the email communication between different domains using an analyzer tool.

46) Should contain a map view and display real-world geographic location of evidence items that have geolocation information associated with them.

47) Should be capable of presenting a realistic view of chat conversations (bubble view) in an orderly manner for messaging applications such as WhatsApp, Hangouts, etc. making it easier to view.

48) Should support data filtering using predefined and custom filters.

49) The user should be able to save custom filters for later use and define as many rules as needed.

50) The filters should be able to leverage item attributes to locate specific files.

51) Should support nested and compound filters using —AND|| or —OR|| operators.

52) The user should be able to create case-specific custom filters that can be used in a single case or shared among other cases.

53) The user should be able to export the custom filters as an XML file and import them to a different case or application instance.

54) Should be able to instantaneously provide search results from indexed data.

55) Should provide options to find synonyms, misspelt words, and words with similar pronunciation for the index search keyword.

56) Should be able to perform the search in a subset of items within an evidence based on a definable filter.

57) Should also support a live search feature in text, Regex, and HEX formats to find things not contained in the index.

58) Should be able to export results of searches for terms, words, or predefined patterns into a comma delimited text file (CSV).

59) Should support tagging items using customizable labels. The investigators should be able to create case-specific labels, group labels, and share individual labels and groups among multiple cases.

60) Should be able to export a list of individual files within evidence, a list of hash values of all individual files, and a word list of contents of the case index.

61) Should provide the ability to perform cross-case investigation.

62) Should support exporting evidence files to a native format and to an image such as E01, AD1, S01 (Smart), and 001 (RAW/DD). The solution should be capable of encrypting data when exporting to an image.

63) Should be able to mount forensic images such as RAW/dd, E01, S01, AD1, and L01 images as a drive or physical device to the host computer, for read-only viewing. The user should be able to open the image as a drive and browse the contents in Windows Explorer and other applications.

64) Should be capable of restoring a physical image such as 001 (RAW/dd), E01, or S01, to a drive.

65) Should be able to export specific items from the case for review in a —portable|| instance with a lightweight viewer application with limited feature set such as quick search, labelling, etc. The portable case should be viewable without the original application.

66) Should provide an option to create backup copies of cases including case information and database files. The user should be able to restore a case from its backup.

67) Should provide an option to archive and detach the cases for which the immediate access is no longer necessary. A detached case should be attachable to the same or a different machine or database from where it was archived and detached originally.

68) Should enable the investigators to generate reports from the reviewed data that can represent the data in a meaningful way.

		69) Should be able to include data such as case details, thumbnail images of the case graphics and videos, paths and properties of files, screen captures from the review platform, etc. in the reports. **70)** Should be able to generate reports in different formats such as HTML, XML, RTF, WML, DOCX, ODT, and PDF. **71)** Should have in built password cracking. **72)** The HTML report should be customizable using a custom CSS file and logo. **73)** Should be able to generate reports in different languages such as English, Arabic, Chinese, German, Japanese, Korean, Lithuanian, Portuguese, Russian, Spanish, Swedish, and Turkish. **74)** Should include toolkit box containing cables, adaptors, accessories, etc.	
		B. NARCOTIC DIVISION	
1.	**Hot Air Oven Table top with 3 chambers and adjustable system**	• Adjustable Air ventilator • Motorized blower fan to maintain uniform temperature inside the chamber • Control panel is consisting of main & Load ON/OFF Switches • Indicating Lamp • Digital Temperature Controller-cum-Indicator Safety Thermostat • Controller: Microprocessor PID Digital Controller for temperature control • Timer: Digital Timer 99hr 59min or Continuous Selectable • Inner Material: Stainless Steel 304 • Outer Material: Mild Steel with Antibacterial Powder Coated Paint • Door: Metal Double Walled Door • Insulation: Double Wall Construction & Mineral Wool Insulation to avoid heat loss Inner Dimensions: 18 x 18 x 18 inches (W x D x H) • Capacity: 150 liters • Temperature Range: Ambient +5°C to 200°C • Temperature Accuracy: ±5°C • Temperature Uniformity: ±1°C • Heater Load: 1kW Heater resistance Nichrome wire • Display: LED Digit Display • Shelves (Removable): SS 304 made 02nos. Wire Mesh Shelves • Safety: Over Temp. Cut off, Over Current Breaker • Electric Supply: 220V, 50Hz; with 3-pin safety plug and Power cord • Warranty: 3 years	1 No.
2.	**Centrifuge**	• Microprocessor controlled table top refrigerated centrifuge with adjustable speed. • from 300 to 17,800 rpm or more and max. RCF Value 30,200 x g or higher. • It should have provision to add higher capacity (8x50 ml, 8x15 ml) Full Swing out rotor, Fixed angle rotor 6 x 50 ml, Micro Plate rotor 2 x 2, 8 x 8 PCR Strip rotor, 8 x 50 ml individual sealed rotor, 30 x 15 ml Cliniconic rotor etc. any time in future. • Digital display (LCD) for Speed, Time, RCF and Temperature. • Maintenance –free frequency –controlled direct brushless induction drive. • Max timer range: 10 second to 99 h, 59 min + Continuous.	1 No.

		• Temp. Range: -10°C to 40°C with direct Pre cooling function. • Imbalance Detection System: Continuous vibration measurement, with rotor mass correction. • It should have Automatic rotor lock system so that it can be installed and removed without any tools. With just a push of a button for quick and easy change of rotors less than 5 sec. • It should be certified for quality & safety by International Certification Agency, like UL, • CE marked IVD compliant & Certified Biocontainment etc. • It should have a 3 direct program buttons and 96 additional programs accessible via folder. • It should have Quick run facility. • System should not have any kind of drain condensation system inside the rotor chamber. The angle rotors must be manufactured from a highly corrosion and fatigue resistant material. • Noise level: Should not be more than 52dBA with small rotor. • Refrigeration System: CFC • Power Consumption: 750 or lower. • Power: Suitable for 230V, single phase, AC, 50 Hz operation. • Accessories: • Fixed Angel Rotor for 6 x 50 mL Conical tubes and Adapters for 6 x 15 mL • Conical tubes, Minimum Speed 9,500 rpm or more should be quoted. • Fixed Angel Microliter Rotor 24 x 1.5/2.0 mL Tube, Minimum Speed 17,850 rpm or more should be quoted. • Suitable Voltage Stabilizer should be quoted. • Prompt & Efficient after-sales service should be available from OEM Service Engineer at Kolkata/ Easter Region. • Bidder should provide printed brochure of the quoted model and details specification must be available in the Manufacture Website for the Quoted Model. • Warranty: 3 years. • Customized Model would not be accepted without any quality control certificate or 3rd Party approved certification. • At least 50 Nos or more installation should be in Govt. Institute/ University, Hospitals, etc.	

27.11.24.

Asstt. Inspector General of Police (E),
Police Headquarters, Itanagar
Arunachal Pradesh

Asstt. Inspector General of Police(E)
Arunachal Pradesh
Itanagar