IITM Pravartak Technologies Foundation
IITM Research Park, Tharamani, Chennai – 600113
Contact Number: +9144 69000004
Email id: purchase@iitmpravartak.net

The Chief Executive Officer Date: 14.01.2024

Tender ref: PTF/005/23-24/CIC **Due Date:** 29.01.2024 @ 3 PM

Tenatative Technical Bid Opening: 30.1.2024 @ 3 PM

Dear Sir/Madam,

On behalf of the IITM Pravartak Technologies Foundation, offers are invited for the project of **"Cyber Innovation Centre"** conforming to the specifications given in **Technical Specification document – Annexure – III**

Instructions to the Bidder

I. **Prices:** - The offer/bid should be exclusive of taxes and duties. The percentage of tax & duties should be clearly indicated separately. IITM Pravartak is eligible for concessional custom duty. Relevant certificates will be issued wherever necessary.

II. **Submission of the Tender: -** The tender shall be sent to the address mentioned below, either by post or by courier (duly sealed and super scribed on the envelope with the Vendor Email ID, Contact Number, tender reference No and due date & time) so as to reach our office before the due date and time specified in our schedule. The offer/bid can also be dropped in the tender box on or before the due date and time specified in the schedule.

The tender box is kept in the office of the:

IITM Pravartak Technologies Foundation,
B5, B Block, 5th Floor,
IITM Research Park, Tharamani,
Kanagam Road, Chennai – 600113.

III. **Late offer: -** The offers received after the due date and time will not be considered. IITM Pravartak, shall not be responsible for the late receipt of Tender on account of Postal, Courier or any other delay.

IV. Opening of the tender: - The offer/bids will be opened by a committee duly constituted for this purpose. The technical bids will be opened first, and examined by a technical committee which will decide the bids' suitability per our specifications and requirements. Bidders will be intimated for the opening procedure of the technical bids. And Only the Technically qualified bidder will be called for Financial Bid Opening.

V. Prices: - The price should be quoted only in INR net per unit (after the breakup) and must include all packing, transit insurance and delivery charges to IITM Pravartak.

a. The offer/bid should be exclusive of taxes and duties. The percentage of tax & duties should be indicated separately.

VI. Terms of Delivery: -

Supplier will be fully responsible for the safe carriage of goods up to Palasamudram, Sri Sathya Sai District, Andhra Pradesh, Palasamudram–515241. Insurance coverage will be in the scope of the supplier.

The Installation/Commissioning should be completed as specified in our important conditions.

VII. IITM Pravartak reserves the full right to accept / reject any tender at any stage without assigning any reason.

Yours sincerely,

The Chief Executive Officer

IITM Pravartak Technologies Foundation,

IIT Madras Research park

Chennai – 600 113.

SCHEDULE

Important Conditions of the tender

1. The offers / bids should be submitted under two bid system (i.e.) Technical bid and financial bid. The Technical bid should consist of all technical details / specifications only. The Financial bid should indicate an item-wise price for each item and it should contain all Commercial Terms and Conditions including Taxes, transportation, packing & forwarding, installation, guarantee, payment terms, pricing terms etc. The Technical bid and financial bid should be put in separate covers and sealed. Both the sealed covers should be put in a bigger cover. The Tender for "**Cyber Innovation Centre**" should be written on the left side of the Outer bigger cover and sealed.

   ****Note: Supplier contact details (Email, contact person, Phone number) to be specified clearly in the outer bigger cover for the purpose of sending communication regarding the Technical Bid opening.**

2. For the same tender, either the OEM or the authorized dealer/service provider can only quote. But both of them cannot quote separately for the same tender.

3. The offers/bids should be sent only for a solutions/product that are available in the market and supplied to a number of customers.

4. The original catalogue/Datasheet (not any photocopy) of the quoted solutions/product duly signed by the OEM/Bidder must accompany the quotation in the technical bid.

5. Compliance or Confirmation report with reference to the specifications and other terms & conditions should also be obtained from the OEM/Bidder.

6. **Validity:** The validity of the Quotation should not be less than 120 days from the due date of tender.

7. **EMD:** Rs. 20,00,000/- (Rupees Twenty Lakhs Only) has to be paid by means of bank transfer. Bank Account Details are given below. Proof of remittance has to be enclosed along with technical bids; else the bid will be rejected due to non-enclosure of EMD. This Earnest Money will be returned to the unsuccessful tenderers after the finalization of the tenders. EMD will not carry any interest. EMD will not be waived under any circumstances. However, EMD is exempted for Micro and Small Enterprises (MSE) as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSME) and Startups as recognized by Department of Industrial Policy & Promotion (DIPP). **(MSE/MSME/DIPP PROOF should be enclosed in the cover containing technical bid).**

****Note: Any offer not accompanied with the EMD shall be rejected summarily as non-responsive.**

Account Name	IITM PRAVARTAK TECHNOLOGIES FOUNDATION
Account No	168001000711
IFSC CODE	ICIC0001680
Bank Name	ICICI
Branch Name	Adyar, Chennai
MICR No.	600229054
Account Type	Savings Account

8. **Performance Security: -** The successful bidder should remit Performance Security for an amount of 3% of the value of the contract/supply. The Performance Security may be furnished in the form of an Account Payee DD, FD Receipt in the name of "IITM PRAVARTAK TECHNOLOGIES FOUNDATION" from any scheduled commercial bank or Bank Guarantee from any scheduled commercial bank in India. The performance security should be furnished within 14 days from the date of the purchase order.

9. **Delivery Schedule**: - Within 4 Months from the date of Purchase order Issued. In case there is any deviation in the delivery schedule, a liquidated damages clause will be enforced or penalty for the delayed supply period will be levied.

   In the event of **delay or non-supply of materials/execution of Contract** beyond the date of delivery/completion of job. The penalty will be levied @1% per week of delay subject to a max of 10% of the value of purchase order and if the delay is more than accepted time frame by IITM Pravartak, the PO would be cancelled and liquidated damages will be enforced.

10. **Risk Purchase Clause**: - In the event of failure of supply of the item/equipment within the stipulated delivery schedule, the purchaser has all the right to purchase the item/equipment from other sources on the total risk of the supplier under risk purchase clause.

11. **On-site Installation**: - The equipment or machinery has to be installed or commissioned by the successful bidder within the number of days (as prescribed by PI) from the date of receipt of the item at the site of IITM Pravartak or location specified in PO.

12. **Warranty**: - All machinery/equipment/software should have 3 Years warranty. Any extended warranty offered for the same has to be mentioned separately.

    **** Note: PO which involves installation, warranty/guarantee shall be applicable from date of installation.**

13. **Acceptance and Rejection**: - IITM Pravartak has the right to accept the whole or any part of the Tender or portion of the quantity offered or reject it in full without assigning any reason.

14. **Do not quote optional items or additional items unless otherwise mentioned in the Tender documents / Specifications.**

15. **Debarment from Bidding**: In case of breach of Terms & Conditions, Bidder may be suspended from being eligible for bidding in any contract with IITM Pravartak for up to 2 Years [as per Rule 151(iii) of GFR] from the date of Tender.

16. **Disputes and Jurisdiction**:

Settlement of Disputes: Any dispute, controversy or claim arising out of or in connection with this PO including any question regarding its existence, validity, breach or termination, shall in the first instance be attempted to be resolved amicably by both the Parties. If attempts for such an amicable resolution fails or no decision is reached within 30 days whichever is earlier, then such disputes shall be settled by arbitration in accordance with the Arbitration and Conciliation Act, 1996. Unless the Parties agree on a sole arbitrator, within 30 days from the receipt of a written request by one Party from the other Party to so agree, the arbitral panel shall comprise of three arbitrators. In that event, the supplier will nominate one arbitrator and the Project Coordinator of IITM Pravartak shall nominate on arbitrator. The Chief Executive officer will nominate the Presiding Arbitrator of the arbitral tribunal. The arbitration proceeding shall be carried out in English language. The cost of arbitration and fees of the arbitrator(s) shall be shared equally by the Parties. The seat of arbitration shall be at IITM Pravartak Technologies Foundation, Chennai.

a. **The Applicable Law:** The Purchase Order shall be construed, interpreted and governed by the Laws of India. The court at Chennai shall have exclusive jurisdiction subject to the arbitration clause.
b. Any legal disputes arising out of any breach of contact pertaining to this tender shall be settled in the court of competent jurisdiction located within the city of Chennai in Tamil Nadu.

17. All Amendments, time extension, clarifications etc., will be uploaded on the website only and will not be published in newspapers. Bidders should regularly visit the above website to keep themselves updated. No extension of the bid due date/ time shall be considered on account of delay in receipt of any document by mail.

18. **Payment Terms:** 90% at the time of delivery and 10% after successful implementation.

19. **Eligibility Criteria:**

As per the Government of India Norms Preference shall be given to , "Class - I Local Suppliers" and "Class - II Local Suppliers" participated in this tender.

However in case of no participation or technically qualified Class I, Class II Supplier, the tender will be processed with the "Non Local suppliers" participated in this tender.

Bidder should confirm their acceptance that they comply with the provisions with report to "Guidelines for eligibility of a bidder from a country which shares a land border with India as detailed at Annexure-IV. The bidder should submit Certificate for "Bidder from/ Not from Country sharing Land border with India & Registration of Bidder with Competent Authority" as per Order of DoE F.No.6/18/2019-PPD dated 23.07.2020 as mentioned.

20. Selection of Successful bidder and Award of Order - Evaluation and Award of contract will be done as per GOI MOCI Order No. 45021/2/2017-PP (BE II) Dt.16th September 2020 & P- 45021/102/2019-BE-II-Part(1) (E-50310) Dt.4th March 2021 and any subsequent modifications/Amendments, and latest orders if any with preference to Make in India. In case of No Local content present, the tender will be processed with the "Non Local suppliers" participated in this tender.

21. Preference to "class 1 Local Suppliers": preference will be given to "class 1 local suppliers" (subject to class -I local supplier's quoted price falling within the margin of purchase preference) as per public procurement (preference to make in India) order 2017 .O.M No P- 45021/2/2017 – pp(BE - 11) dt 04/06/2020 subject to the conditions that the "class 1 Local Supplier" should agree to supply goods / provide service at L1 rate and furnish a certificate with the technical bid document that the goods/service provided by them consists local content equal to or more than 50%.(certificate from Chartered Accountant in case value of contract exceeds Rs 10 crore).

- 'Class - I local supplier' means a supplier or service provider whose goods, services or works offered for procurement consists of local content equal to or more than 50% as defined under the above said order.

- 'Class - II local supplier' means a supplier or service provider whose goods, services or works offered for procurement consists of local content equal to 20% but less than 50% as defined under the above said order

- 'Non – local supplier' means a supplier or service provider whose goods, services or works offered for procurement consists of local content less than 20% as defined under the above said order.

- 'Margin of purchase preference': - The margin of purchase preference shall be 20%. The Definition of the margin of purchase preference is defined in the govt. of India Order No: P-45021/12/2017-PP (BE-II) Dt.4th June, 2020) Order 2017. As per the Government of India Order – "Margin of Purchase

Preference" means the maximum extent to which the price quoted by a "Class-I local supplier" may be above the L1 for the purpose of purchase preference.

****Note: Local content percentage to be calculated in accordance with the definition provided at clause 2 of revised public procurement preference to Make in India Policy vide GoI Order no. P-45021/2/2017-PP (B.E.-II) dated 15.06.2017 (subsequently revised vide orders dated 28.05.2018, 29.05.2019and 04.06.2020) MOCI order No. 45021/2/2017-PP (BE II) Dt.16th September 2020 & P- 45021/102/2019-BE-II-Part (1) (E-50310) Dt.4th March 2021**

Acknowledgement: - It is hereby acknowledged that the tenderer has gone through all the conditions mentioned above and agrees to abide by them.

SIGNATURE OF BIDDERS
ALONG WITH SEAL OF THE
COMPANY WITH DATE

Annexure I

FORMAT FOR AFFIDAVIT OF SELF-CERTIFICATION UNDER PREFERENCE TO MAKE IN INDIA.

Tender bidding Number:

Name of the item / Service: Date:

I/We_____S/o, D/o, W/o, _____ Resident of

Hereby solemnly affirm and declare as under:

That I will agree to abide by the terms and conditions of the Public Procurement (Preference to Make in India) Policy vide GoI Order no. P-45021/2/2017-PP (B.E.-II) dated 15.06.2017 (subsequently revised vide orders dated 28.05.2018, 29.05.2019and 04.06.2020)MOCI order No. 45021/2/2017-PP (BE II) Dt.16th September 2020 & P-45021/102/2019-BE-II-Part(1) (E-50310) Dt.4th March 2021 and any subsequent modifications/Amendments, if any and

That the local content for all inputs which constitute the said item/service/work has been verified by me and I am responsible for the correctness of the claims made therein.

Tick (✓) and Fill the Appropriate Category	
☐	I/We_____[name of the supplier] hereby confirm in respect of quoted items that Local Content is equal to or more than 50% and come under **"Class-I Local Supplier"** category.
☐	I/We_____[name of the supplier] hereby confirm in respect of quoted items that Local Content is equal to or more than 20% but less than 50% and come under **"Class-II Local Supplier"** category.
☐	I/We _____ [name of the manufacturer] hereby confirm in respect of quoted items that Local Content is less than 20% come under **'Non – Local Supplier'** category

- The details of the location (s) at which the local value addition is made and the proportionate value of local content in percentage

Address _____ _____ __ Percentage of Local content: _____%
_____

For and on behalf of .....(Name of firm/entity)

Authorized signatory (To be duly authorized by the Board of Directors)
<Insert Name, Designation and Contact No.>

[Note: In case of procurement for a value in excess of Rs. 10 Crores, the bidders shall provide this certificate from statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content.]

This letter should be on the letterhead of the quoting firm and should be signed by a competent authority. Non-submission of this will lead to Disqualification of bids

ANNEXURE – II

(To be given on the letter head of the bidder)

No._____ Dated: _____

CERTIFICATE

(Bidders from India)

I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and hereby certify that I am not from such a country.

OR *(whichever is applicable)*

(Bidders from Country which shares a land border with India)

I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and hereby certify that I from _____ (Name of Country) and has been registered with the Competent Authority. I also certify that I fulfil all the requirements in this regard and is eligible to be considered. *(Copy/ evidence of valid registration by the Competent Authority is to be attached)*

Place:
Date:

Signature of the Tenderer
Name & Address of the
Tenderer with Office Stamp

ANNEXURE-III

Pre-Qualification Criteria: I				
S.NO	**PRE-QUALIFICATION CRITERIA - I**	**Compliance (Yes/No)**	**Reference Page No.**	**Remarks, If any**
1	The bidder shall not be from a country sharing land border with India and if the bidder is from a country sharing land border with India the bidder should have been registered with the competent authority as per government of India orders. Declaration of Land border to be submitted as per Annexure II			
2	The bidder nor any of its partners has been blacklisted / debarred by any central or state government agencies in last 3 years. A self-declaration format given in Annexure V to be submitted along with Technical Bid.			
3	The Bidder, in case not OEM should submit the OEM authorization certification with reference to this tender as per Annexure IV for each product except general hardware and accessories.			
4	The bidder/OEM should have supplied similar solution to any government/PSU organization/ limited company for each solution in last 3 Years. OEM/Bidder to provide the same on letter head. IITM Pravartak Reserve rights to verify the claim.			
5	The Bidder should have valid GST Certificate.			
6	Bidder to submit GST Certificate along with PAN Card.			

Technical Specifications

General Terms & Conditions

S.No.	Specifications	Compliance (Yes/No)	Ref. Pg. No
1	All License should be with 3 Years support and upgrade		
2	All items Warranty should be of 3 Years.		
3	Software/Firmware updates should be included in warranty period		
4	Bidders must have tender specific manufacture authorization certificate (MAF) from OEM for all forensic solutions.		
5	OEM Standard Support should be included		
6	One time Implementation to be done onsite "Palasamudram, Sri Sathya Sai District Andhra Pradesh, Palasamudram– 515241"		
7	Technical Committee can ask for live demonstration of any solution if required during technical evaluation.		
8	MAF for Normal Workstation and regular accessories (Tech Specs No. 1.4, 4.2, 6.2, 10.2, 11.2) is not required. However, MAF for Forensic Workstation are required.		
9	Active Directory Setup if required to be provided by the vendor.		
10	Training to be provide for each solution.		

1. Computer Forensics

1.1 All in One Evidence Center

S.No.	Specifications	Compliance (Yes/No)	Ref. Pg. No
1	Solution should be easy for an investigator to acquire, search, analyze, store and share digital evidence found inside computer and mobile devices, RAM and cloud		
2	Solution should quickly extract digital evidence from multiple sources by analyzing hard drives, drive images, cloud, memory dumps, iOS, Blackberry and Android backups, UFED, JTAG and chip-off dumps.		
3	Solution should automatically analyze the data source and lay out the most forensically important artifacts for investigator to review, examine more closely or add to report.		
4	Solution should be able to discover more than 800 types of artifacts, including over 100 mobile applications, all major document formats, browsers, email clients, dozens of picture and video formats, instant messengers, social networks, system and registry files, P2P and file transfer tools, etc. Extracts data from all major operating systems, both computer and mobile: Windows, Linux, MacOS X, iOS, Android, Windows Phone, Blackberry.		
5	Solution should look for hidden and encrypted information, searches in unusual places, carves deleted and damaged data and examines files in little-known formats to discover more evidence than ever. The search includes unallocated and slack space, $MFT, $Log, Volume Shadow Copy and other special and little known areas of operating systems.		
6	Solution should allow you to perform evidence search faster than most tools as it does not index every single file found on the data source, instead searching for the most forensically significant types of artifacts. Efficient usage of CPU adds to speediness of processing, as does the code written by our team of highly qualified specialists in data analysis.		
7	Solution should recover corrupted and incomplete SQLite databases, restores deleted records and cleared history files. Processes freelists, write-ahead logs and journal files, and SQLite unallocated space.		
8	Solution should extract potentially crucial information from volatile memory, such as: in-private browsing and cleared browser histories, online chats and social networks, cloud service usage history, and much		

	more.		
9	Solution should be equipped with File System Explorer, Hex Viewer, and Type Converter		
10	Solution should have free scripting module allows user to write their own custom scripts in order to automate some of the routine and further extend the product's functionality.		
11	Solution should support picture formats:3FR, ARW, BAY, BMP, BMQ, CAP, CINE, CR2, CRW, CS1, CUT, DC2, DCR, DDS, DIB, DNG, DRF, DSC, EMF, ERF, EXIF, EXR, FAX, FFF, G3, GIF, HDR, HEIC, IA, ICO, IFF, IIQ, J2C, J2K, JFIF, JNG, JP2, JPE, JPEG, JPG, K25, KC2, KDC, KOA, LBM, MDC, MEF, MNG, MOS, MRV, NEF, NRW, ORF, PBM, PCD, PCT, PCX, PEF, PFM, PGM, PIC, PICT, PNG, PNM, PPM, PSD, PTX, PXN, QTK, RAF, RAS, RAW, RDC, RLE, RPBM, RPGM, RPPM, RW2, RWZ, SGI, SR2, SRF, STI, TGA, TIF, TIFF, WBM, WBMP, WMF, XBM, XPM.		
12	Solution should have Picture analysis which allows detection of texts, faces, and skin tone. Detection of photo manipulation (forgery) is available with Forgery Detection plugin (extra module)		
13	Solution should have following formats that can be carved: GIF, JPEG/JPG, PNG, BMP, WMF		
14	Solution should support following video formats: 3GP, 3G2, ASF, AVI, DIVX, DRC, F4A, F4B, F4P, F4V, FLV, IFO, M2V, M4P, M4V, MK3D, MKA, MKS, MP2, MP4, MKV, MOV, MPE, MPEG, MPG, MPV, NSV, OGG, OGV, QT, RM, RMV8, SVI, TS, VOB, WEBM, WMV		
15	Solution should have Key frame analysis available for 3GP, 3G2, AVI, MP4, MPEG, MPG, WMV, MOV videos		
16	Solution should support Social Networks: Bebo, Facebook, Facebook Messenger, Google+, Myspace, Odnoklassniki, Orkut, Twitter, VKontakte		
17	Solution should support Cloud Services: Dropbox, Flickr, Google Drive, SkyDive, OneDrive, Yandex Disk		
18	Solution should have Multi-user Online Games: Karos, Lineage, World of Warcraft		

1.2 Disk Forensics

S.No.	Specifications	Compliance (Yes/No)
1	The solution should have a timeline view option to provide an easily to search adjustable, graphical calendar like display for file activity of particular interest.	
2	The solution should contain Full Unicode support to allow users to search text and fonts from any foreign county and in any language.	
3	Should support acquisition Restart facility: continue a window acquisition from its point of interruption.	

4	Should have inbuilt LinEn utility to acquire evidence via boot Disk.	
5	Should have inbuilt WinEn utility to acquire RAM evidence.	
6	Should do image verification by CR and MD5.	
7	Should have Inbuilt support for writing scripts & should have pre-built scripts.	
8	Should support more than 150 Filters and Conditions.	
9	Should support combining filters to create complex queries using simple "OR" or "AND" Logic.	
10	Should have Inbuilt Active Directory Information Extractor.	
11	Should be able to automatically rebuild the structure of formatted NTFS AND FAT volumes.	
12	Should support Recovery of deleted file/folders.	
13	Should have Inbuilt windows event log parser, Link file parser to search in unallocated space.	
14	Should have Inbuilt support for Compound (e.g., zipped)	
15	Should have native viewing support for 400 file formats.	
16	Should have built-in Registry Viewer.	
17	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 Sensitive, GREP ;Right to Left Reading, Big	
	Endian/Little Endian, UTF-8/UTF-7, Search file slack & unallocated space.	
18	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 Explorer, Mozilla Firefox, Opera and Apple Safari.	
19	Supports file signature analysis	
20	Should include system support for:	
	Hardware and Software RAIDs	
	Dynamic disk support for Windows Server	
	Interpret and analyze VMware, Microsoft Virtual PC, DD and	
	SafeBack v2 image formats.	
	File System: Windows FAT12/16/32, NTFS; Macintosh HFS, HFS+; Sun Solaris 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.	
21	Should support reporting facility with: • Listing of all files and folders in a case • Detailed listing of all URLs and corresponding dates and times of web site visited • Document incident response report • Log Records • Registry • Detailed hard drive information about physical and logical partitions • View data about the acquisition, drive geometry, folder structures and bookmarked files and images • Export reports in Text, RTF (opens in Microsoft Office), HTML. XML or PDF formats.	
22	Should have reporting feature to quickly share a report with organization officials and with a few simple clicks select the exact information for the report and generate an easy to review HTML report that can be viewed in any web browser	

1.3 Digital Investigation Platform

S.No.	Workstation Specifications	Compliance (Yes/No)
1	Tool to support data comprehensive extraction and analysis from Computer, Memory and Vehicle data analysis all in one single platform.	
2	Should have dedicated workflow for Windows, MacOS and Linux platform.	
3	Support for popular distributions in Linux including Ubuntu, Red Hat, Debian, Kali and more.	
4	Support for ivo file extension exports, which enables users to include vehicle forensic data with all the other evidence sources in one case to analyse waypoints, routes, velocity logs, contacts, call logs, Attached devices etc	
5	The tool should have an option letting investigators define and allocate number of logical cores on the examiner machine. Should support 32 cores for improved system performance and optimization of machine usage.	
6	Should support MD5, SHA1 and SHA 256 Hash formats for collected evidence.	
7	Should have an option to integrate Photo DNA to identify visually similar images.privi	
8	Should Support different file systems including HFS+, HFSX, EXT2, EXT3, EXT4, FAT32, EXFAT, NTFS, YAFFS2	
9	Targeted image for Windows includes USN Journal, Hibernation File, Master File Table, Pagefile, , Event Logs, Setup API Logs, Windows Registry Hives, LNK Files, User Profiles, Prefetch Files .	
10	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.	
11	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.	
12	Should Support capture of Physical Memory (RAM Dump) to analyse valuable artifacts that are often only found in memory.	
13	Should also capture memory from individual running processes. When investigators are short on time or are only interested in specific processes, the utility can retrieve specific processes and also provide less fragmented data and better recovery of larger data types.	
14	Should have option to acquire memory and individual process both using the GUI as well as Command Line to reduce the footprint on the suspect system.	
15	Command-line utility that can quickly and non-intrusively check for encrypted volumes on a suspect computer system during incident response.	
16	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.	

17	Ability to analyse memory dumps in the format of .RAW, .CRASH, .VMSS, .HPAK, .ELF, .MEM, .DMP, .DD, .IMG, .IMA, .VFD, .FLP etc.	
18	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.	
19	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	
20	Should have utility to quickly collect and preserve data from local endpoints before it is potentially modified or lost with support for pre-set collection profile giving investigators the ability to target a comprehensive set of files and data relevant to incident response investigations, including RAM. It should be useful in situations where non-technical users may need to collect and preserve data on behalf of law enforcement investigators as part of a cyber incident investigation.	
21	Multiple Device Queueing – 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 artifacts for Keyword Searching.	
25	Should support search for keywords on both recovered artifact 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	Recovers more artifacts 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.	
27	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	
28	identify and categorize handwritten documents automatically with AI,	
29	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	
30	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.	
31	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.	

32	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.	
33	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.	
34	Should allow investigator to filter video files with attributes such as video files within carving limit, media duration etc	
35	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.	
36	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.	
37	Should support pre-processing date filters which gives investigators the option of setting a date and time range for the artifacts that will be added to a case. This feature allows to limit the artifact data being collected in order to comply with warrant restrictions around the applicable dates for the investigation.	
38	Should support parse and carve and parse selected artifact option to save time on a case if carving is not necessary for investigation.	
39	Should support option to include or exclude specific content from the case pre processing the evidence.	
40	Should have Timeline explorer to consolidate all the timestamps from files and artifacts in a single view, with colours and tags to differentiate timestamp categorizes.	
41	Ability to automatically find potential chat databases along with other valuable evidence from non-chat apps that aren't yet supported in an artifact. users can then easily create an XML or Python artifact to be searched for in future cases.	
42	Capability for parsing unsupported database using custom artifacts or Python Scripts for popular local applications like Tally, Airbnb, ccleaner, FakeGPS, Linkedin, onion browser bookmarks etc.	
43	Should have a GUI/Wizard-driven utility, so no coding experience required to build custom artifacts 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.	
44	Should have a platform that allows forensics professionals access to repository of Custom artifacts and option to upload custom scripts that they have built, and help their peers with their cases, or download artifacts others have built to help with their own cases.	
45	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.	
46	Enhanced searching, sorting and filtering – search, sort and filter artifact 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.	
47	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).	
48	Support multiple data views, including Column/Table view, Summary Row view, World Map view, Timeline view, Chat Threading view and Histogram view.	
49	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.	
50	Should have a feature to reduce overexposure to illicit/ disturbing content extracted to protect improve investigator wellness. This features 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	
51	Should support Dark mode to help investigators work long hours staring at the screen.	

1.4 Hardware

S.No.	Workstation Specifications	Compliance (Yes/No)
1	Processor: Intel Core i7 or Higher	
2	Memory: RAM 32 GB	
3	Hard Disk: 1 TB or higher	
4	Operating System: Windows 10 or higher	
5	Screen 21 inch or higher	
6	Any software hardware required to run solution quoted by bidder	

2 Mobile Forensics

2.1 Mobile Multi Channel Analyzer

S.No.	Specifications	Compliance (Yes/No)
1	Should be a new generation of mobile forensics, with high speed simultaneous extraction and analysis of cell phones, tablets and GPS devices	
2	Should have ability to extract deleted data, call history, contacts, text messages, multimedia messages, photos, videos, recordings, calendar items, reminders, notes, data files, passwords, and data from apps such as Skype, Dropbox, Evernote, Facebook, WhatsApp, Viber, Signal, WeChat and many others with only a few clicks.	
3	Should be able to find passwords to encrypted device backups and images	
4	Should be able to bypass screen lock on popular Android OS devices	
5	Should be able to acquire data from cloud services and storages	
6	Should be able to extract flight history and media files from drones	
7	Should be able to acquire data from IoT devices and smartwatches	
8	Should be able to provide social links analysis and Timeline view	
9	Should be able to Collect user data on Windows, MacOS and Linux PCs	
10	should have Wireless charging station in the device	
11	Should support 8-channel analysis of cell phones using Parallel Forensics Technology.	
12	Should have IN WIN A1 Mini-ITX Case with 600 Watt Power supply	
13	Should have 8-Core Intel® Core™ i9-11900 Processor with 16M	

	Cache, 2.50 GHz - 5.20 GHz	
14	Should have Corsair Cooling Hydro Series H45 Watercooling + CORSAIR Commander PRO, Digital Fan & RGB Controller	
15	Should have 32 GB RAM	
16	Should have 1 - 500 GB SSD and 1 - 2 TB SSD Drives	
17	Should have 2x USB 3.1 (Gen2) Metal HUB mit 4 Ports 2 x USB-C und 2 x USB-A Anschluss	
18	Must have a Collection of carefully selected cables covering majority of phones that have ever been on a market	
19	Should have 3 years Warranty and Support	

2.2 Mobile Forensics

S.No.	Specifications	Compliance (Yes/No)
1	The perfect data extraction tool for diverse mobile and digital devices · Data acquisition for various global smartphone manufacturers (Samsung/Apple/LG/HTC/ZTE) models · Other manufactured devices (Huawei/Xiaomi/Oppo/Vivo, etc.) · IoT device, AI Speaker, Drone, and Smart TV	
2	· Supports Bootloader, Fastboot, MTK, QEDL, Custom Image Android Rooted, iOS Physical, DL, JTAG, Chip-off, SD Card, Removable Media · ADB Pro extraction which supports data acquisition using vulnerability attacks from Android-based devices ·JTAG pin map viewer and connection scanning with AP	
3	IoT device data extraction ·Smart Watch - Apple Watch(iOS), Galaxy Gear(TizenOS), Fitbit ·SmartTV - Samsung(TizenOS), LG(WebOS), Android TV · AI Speaker - Amazon Echo, Google Home, Kakao Mini, Naver Clova, KT Giga Genie, SK NUGU ·Drone - DJI (Phantom, Mavic), Parrot, PixHawk	
4	Advanced logical extraction · Android Live, MTP, iOS full filesystem Backup, Vendor backup protocol, Local backup, USIM	
5	Supports extraction and unlocking of the latest Asian phone · Physical extraction through all lock bypass (KNOX, FRP/OEM, Screen Lock): Samsung Galaxy S/J/A/Note series · Unlock screen: Samsung Galaxy S/J/A/Note series · ADB Pro physical KNOX bypass – Samsung Galaxy S/J/A/Note series · Vendor Backup protocol extraction – Samsung, LG, Huawei · Local backup extraction - Huawei, Xiaomi, Oppo, Gionee · Physical extraction for Japanese manufacturer model - Sharp, Sony	
6	Supports the latest iPhone logical extraction ·iOS keychain ·iOS full filesystem ·Logical extraction for iPhone up to XS/XR model ·The decryption of backed up data for the latest version of the iOS device	

7	Useful extraction options ·User-defined extraction for unlisted models using pre-defined methods · Selective extraction by the partition, file, category, app for privacy protection ·Auto-recognition and decryption of partition table and encrypted partition ·Automatic firmware restoration and retrial after restoration failure ·Pause/Resume feature ·Merges multiple image files – MDF and binary file ·Creates MDF file from PC backup	
8	Assures evidence data integrity ·Write-protection for every piece of evidence · Supports ten different hash algorithms, including MD5, SHA1/224/256/384/512, RIPEMD128/160/256/320	
9	Support multiple device extraction ·Supports both simultaneous and sequential extraction	
10	Supports diverse physical data reading hardware ·JTAG Reader (MD-BOX) ·Memory Chip Reader (MD-READER) ·SD Memory Reader/USIM Reader	
11	Data preview and saving features ·Extraction data preview- Hex viewer ·Sound alarm and TTS alarm for extraction status change	
12	User-friendly and intuitive user interface ·Intuitive graphical user guide for each extraction method ·Features 'Recently Selected Models' List	
13	Report generation ·Extraction information - Hash value, Time, Method and Filename ·'Extracted File List' generation with a hash value of each file ·Generates 'Witness Document'	
14	Supports wide variety of mobile operating systems and devices ·Feature phones, Smartphones and various other digital devices ·iOS, Android, Windows, TizenOS and other mobile operating systems	
15	Parsing and recovery of various filesystems · FAT12/16/32, exFAT, NTFS, ext3/4, HFS+, EFS, YAFFS, FSR, XSR, F2FS, VDFS, XFS filesystems ·Data carving of unused areas	
16	Supports analysis of mobile data over 2,000 popular mobile apps ·Multimedia files taken by device camera · Call logs, Address book information, SMS/MMS messages, emails, Memos, and Internet history ·Social networking, maps, navigation, banking, health, and lifestyle apps ·Detection of Anti-forensic apps, and hidden apps	
17	Supports decoding screen lock and password information ·Decoding unlock patterns, PINs, and passwords ·Brute force through GPU acceleration · iPhone keychain data analysis – Credential (collected from iOS keychain, iOS, App information) can be exported and analyzed	
18	Data decryption ·Identifying encrypted documents	

	·Supports decryption of chat messages, emails, files, and other app data	
19	Deep analysis on popular messenger apps ·Deserialization, decryption, and recovery of data · Skype, Facebook messenger, Telegram, Wickr, QQ, KakaoTalk, Line, Zalo, Viber, Snapchat, and many more ·WhatsApp – Multiple backup file analysis ·WeChat – Multiple account analysis, rainbow table analysis	
20	Multimedia data recovery and analysis ·Supports frame recovery for deleted/damaged video files · Supports the use of Reference Data Set (RDS) for excluding over 9.8M known unusable images from analysis result data · Supports audio file conversion (From AMR/AUD/QCP/SILK to MP3/AMR/WAV) ·Supports playing QCP files and SILK-encoded audio	
21	Log analysis · Supports analysis of various logs: media, search word, system, and network logs (Bluetooth, WiFi, Cell towers)	
22	Social relationship analysis ·Provides Basic/Advanced modes for analyzing single/multiple phones ·Call history, messenger, and email communication data analysis ·Filtering by app, time period, contact(s), and type(s) of communication ·Community analysis ·Relationship visualization and automatic re-organizing	
23	Embedded data viewers ·View extracted data and source information directly in-application · SQLite databases, HEX, PLists, Documents (Text, XML, PDF, MS Office), Photos, Videos, and Audio	
24	Visualization of analyzed data ·Map viewer for GPS and cell tower location data ·Offline / Online map (Region / Country / City view levels) ·Timeline view ·Link viewer (social relationship visualizer) ·Chat viewer ·Web browser view (for internet browsing history)	
25	Advanced data filtering options ·Filtering by a variety of properties such as filesystem, signature, and time ·Dynamic filtering operators, sorting, and grouping ·Search by regular expression ·Character search – Supports to search similar words ·Keyword registration ·Bookmarking selected data	
26	New digital device analysis · Drone data analysis - Flight history, Multimedia data, Supports manufacturer DJI/Parrot/PixHawk ·IoT device data analysis - AI Speakers, Smart TV, Car Navigation	
27	Python scripting IDE for user-defined analysis ·Includes a Python script editor · Supports generating, executing, and debugging code and includes sample scripts	

28	Case management and hash value verification ·Various case management features ·Grouping extraction images ·Hash value verification on a per-image basis	
29	Maximized performance · High speed analysis achieved through multi-core CPU/GPU parallel processing · Supports running multiple instances of the program (i.e.: one instance for each open case) · Analysis status alarm – Pop-up message will let user know when forensically important data and history are found (i.e. Initialization history, Data hidden apps, Parallel space)	
30	Report generation ·Hashing individual files ·Export analyzed multimedia ·Automatic report generation (PDF, Excel, HTML, XML, SQLite DB formats) ·Supports 3rd party reporting formats like Nuix and Relativity · Bundling feature – Bundle generated reports/outputs (exported folder, etc.) into MDF file	

2.3 Mobile Forensic with AI Capabilities

S.No.	Specifications	Compliance (Yes/No)
1	The mobile forensic solution should offer a choice of software license or USB hardware dongle(CodeMeter) license. The offered license should be perpetual.	
2	The mobile forensic solution should provide a case binder for all the cables.	
3	The mobile forensic solution should provide a SIM Card Reader with support of Standard, Micro and Nano SIM cards.	
4	The mobile forensic solution should provide SIM-ID Cloner Cards.	
5	The mobile forensic solution should provide a Write Protected Universal Memory Card Reader.	
6	The mobile forensic solution should have at least 45,600+ mobile device profiles. It should support more than 460+ Applications and 4400+ different versions of these applications.	
7	The mobile forensic solution should have a image content recognition capability and utilising NVidia GPUs to accelerate image classification times.	
8	The mobile forensic solution should allow for the extraction of at least up to 3 mobile devices simultaneously with just a single license key if required.	
9	The mobile forensic solution should have fast file opening and users should not need to wait longer than a maximum of 60 seconds to visualize the extracted data.	
10	The mobile forensic solution shall provide options for support of mobile devices via Generic Profiles to allow for support of new and	

	untested devices. Required generic profiles : a) Android generic, Apple iOS generic, RIM Blackberry generic, Windows generic. b) Android MediaTek generic, Android Spreadtrum generic, Qualcomm generic, Samsung exynos generic. c) Mediatek generic, Spreadtrum generic, Coolsand generic. d) LG Android generic Qualcomm, Samsung generic, Sony generic.	
11	The mobile forensic solution should support searching of content on text-based documents.It must have capability to search for specific words in different file formats such as pdf, txt, xml, html, and SQL databases.	
12	The mobile forensic solution should have a viewer to save and recall a quick view to avoid recreating the same set of filter repeatedly.	
13	The mobile forensic solution should have a viewer to show extraction from single or multiple devices.	
14	The mobile forensic solution should have a viewer to show extraction in multiple tab and multi-monitor mode.	
15	The mobile forensic solution should have a viewer to easily tag an item as Important with one mouse click.	
16	The mobile forensic solution should have a viewer to create new tag with desire tag name and colour. User created tag can be transferred to another computer easily.	
17	The mobile forensic solution should have a viewer to create, customize or delete any filter.	
18	The mobile forensic solution should have a viewer to provide four investigator views(List, Column, Gallery and File Tree).	
19	The mobile forensic solution should have a viewer to show data in Source Mode, SQL Viewer and Map View without using the native or 3rd party application.	
20	The mobile forensic solution should have scalable Overview page with Recently Opened Extraction, Case Content, Exhibits, Quick View, Artifacts information, Exhibit Data, Summary & Statistic, General Information, Device Overview and Extraction Log.	
21	The mobile forensic solution should have options for export of data into the standard file formats of XLS, PDF, WORD, GPX, KMZ, VIC, FILE, EXTENDED XML, HTML, OpenDocument Text, OpenDocument SpreadSheet	
22	The mobile forensic solution must be able to import Python Script to assists on the decoding and analysis. It should use python v3.4.3 or above.	
23	The mobile forensic solution must be able to bookmark Hex data.	
24	The mobile forensic solution must have App database mapper tool for unsupported apps to manually map data in SQLite database tables to artifacts. Once mapped it should have option to save the template for future use.	
25	The mobile forensic solution must be able to manually reconstruct of Hex data.	
26	The mobile forensic solution should generate hex-dumps from the phone memory, typically by bypassing the device operating system.	
27	The mobile forensic solution must be able to provide PLIST, XML & SQL Database Viewers.	

28	The mobile forensic solution must be able to group duplicate artifacts.	
29	The mobile forensic solution must be able to provide Known Data Filtering.	
30	The soultion must be able to provide file anomalies filter.	
31	If Drone data and information is available, The mobile forensic solution must be able to display the data and information on a Drone Tab.	
32	The mobile forensic solution must be able to allow Column export in WYSIWYG format from column view.	
33	The mobile forensic solution should be a software based solution, complete with all necessary hardware for recovering data from device in a secured manner.	
34	The mobile forensic solution should be able to extract device data logically and physically.	
35	The mobile forensic solution should be able to extract SIM Card data.	
36	The mobile forensic solution should support bypass and recovery of lock codes for mobile devices.	
37	The mobile forensic solution must have option to bruteforce encrypted iTunes backup.	
38	The mobile forensic solution should have selective app extraction option for targetting extraction to only recover data from selectes apps.	
39	The mobile forensic solution should support Bluetooth and Hosted Wifi Extraction for mobile devices.	
40	The mobile forensic solution should utlise the latest 64Bit software technology to ensure future capability and support of large multi-gigabyte mobile devices.	
41	The mobile forensic solution should be able to extract vital application data on device running but not limited to below OS: a) iOS b) Android c) Blackberry OS d) Windows Phone/Mobile/CE/RT e) Asha Platform f) KaiOS g) Tizen OS	
42	The mobile forensic solution shall provide options for support of mobile devices via Generic Profiles to allow for support of new and untested devices.	
43	The mobile forensic solution should be regularly updated with new releases containing updates to device and app support as part of the license.	
44	The mobile forensic solution should perform extraction, decoding and indexing on a single operation.	
45	The mobile forensic solution must use Windows Certified and signed USB drivers to avoid inteference with any other software running on the computer and for IT Security reasons: https://docs.microsoft.com/en-gb/windows-hardware/drivers/develop/signing-a-driver.	
46	The mobile forensic solution should normalize timestamps from all mobile devices extracted to ensure that exported data formats are all	

	consistently reported to 3rd party tools.	
47	The mobile forensic solution support extraction and decoding of data from applications, minimally including WhatsApp, Skype, Telegram, WeChat, Snapchat, Line, Facebook Messenger, Facebook, Twitter, Instagram, Tinder, Skout, Gmail, Yahoo Mail, Outlook, SMS, etc.	
48	The mobile forensic solution should be able to extract the internet and download history from common web browsers.	
49	The mobile forensic solution should support Rapid hash match functionality that enables you to acquire information about the device data before the extraction has even finished. Hash matching functionality should support MD5, SHA1 and SHA 256 hash algorithms.	
50	The mobile forensic solution should adhere to the fundementals of digital forensic principles: a) A secured data file container to avoid allegations of interference with electronic evidence after extraction; b) An audit log to show exactly what functions the forensic tool performed on the digital device; c) Hash Algorithm options for enhanced file security and cross referencing; d) To provide password protection on extraction data; e) Examinations should not assume file extentions can be relied upon and instead it should only read the raw digital data.	
51	The mobile forensic solution should have a fully documented manual that: a) Manually lists all devices and apps supported via the extraction software to aid investigators; b) List what data types can be extracted on specific device profile; c) List what data types cannot be extracted on specific device profile; d) Available via mobile phone app to manually lists all devices and apps supported to aid investigators.	
52	The mobile forensic solution should have a fully documented manual that lists out the device or application based on: a) Device Type; b) Manufacturer; c) Form Factor; d) Device Operating System; e) Application Category; f) Application Operating System.	
53	The mobile forensic solution should have built in decoders for the recovery of the following artifacts: a) Deleted Video and Image Carving b) Audio Files c) Picture Files d) Document Files e) Smartphone App data	
54	The mobile forensic solution should natively enable connection to a mobile device via any USB port on the installed PC. No hardware converter devices should be required to be installed.	
55	The mobile forensic solution should be able to perform device cleanup by specifying individually or the whole list.	

56	The mobile forensic solution must support physical extraction using Raspberry Pi Zero.	
57	The mobile forensic solution should provide Application Downgrade Method to support at least 55+ latest Android OS non-system applications. For example (Whatsapp, Skype, WeChat, Instagram, KakaoTalk, Line, Facebook Messenger, Facebook, QQ and etc).	
58	The mobile forensic solution should have Triage mode with android extraction option of rooted and non rooted device.	
59	The mobile forensic solution should be able to extract evidence from mobile device where a screenshot is the only way to capture relevant evidence and help validate device extraction results. Capturing screenshot should be available for both Android as well as iOS devices.	
60	The mobile forensic solution should automatically generate an audit trail of the forensic process for peer review.	
61	The mobile forensic solution should have support for Telegram Android clones like Graph Messenger, Plus Messenger and Mobogram.	
62	The mobile forensic solution should support decoding of geolocation information from KMZ files.	
63	The mobile forensic solution should have an automated version of manual app examination on Whatsapp, signal, Telegram, Whatsapp for Business and dual instances of these apps with the benefit of storing image, text data and Emoji in a searchable way. Stored text data and Emoji must be presented with 100% accuracy. Method should also support of Manual app examination to capture app data from any application by manually opening app from which user wants to capture data.	
64	The mobile forensic Solution must include camera which allows capturing of still and video images of the examined devices. The results must be stored using the same secure file format supported by the Solution. USB Camera hardware with at least 4K resolution must be included with the Solution.	
65	The mobile forensic solution should have option to recover data from cloud based storages.	
66	The mobile forensic solution should be able to extract cloud based data based on application tokens recovered during a standard mobile device extraction.	
67	The mobile forensic solution should be able to extract cloud based data based on provided user id and password login details without physical possesion of the mobile devices.	
68	The mobile forensic solution should be able to combine extracted data into the case file, to ensure all exhibits held together in one place.	
69	The mobile forensic solution must be able to provide a Conversation view Visualization , Connection (Link Analysis) View Visualization, Time Line View Visualization & Geographical View Visualization.	
70	The mobile forensic solution must be able to import Call Data Records.	
71	The mobile forensic solution must have Persons' AI Capability, Unique intelligent core decoder able to present and link multiple identifiers to a single person identity. The solution must have participant filter for tracing a conversation that includes many	

	persons using different message apps.	
72	The mobile forensic solution must have solution to import warrant returns from Apple, Coinbase, Facebook, Google, Instagram & Snapchat.	
73	The mobile forensic Solution should have feature to integrate offline Maps.	
74	The mobile forensic solution should have option for dealing with non-standard mobile devices, which are cheaper clone phones where the challenge forensically is the connector pin-outs, which vary in configuration and sometimes is not known. The mobile forensic solution should provide interface cable, binder, adapter kit consists of at various tips, power cable alligator, power cable clips, power cable PCB, voltage reduction adapter etc. The mobile forensic solution should powered by a software solution which is regularly updated and thus avoiding the perils of separate black box solutions with frozen firmware that gets outdated as soon as they are purchased.	
75	The mobile forensic solution should be able to extract call logs, contacts, SMS/MMS, ,media files, calendar, tasks, notes, deleted data, chip ID and file system.	
76	The mobile forensic solution should be able to support non-standard mobile devices with chipsets from: a) MediaTek b) SpredTrum c) Coolsand d) Infineon	
77	The mobile forensic solution should be on the latest version as per the latest software update from the OEM.	

2.4 Mobile Forensic

S.No.	Specifications	Compliance (Yes/No)
1	**Extraction Capabilities**	
2	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.	
3	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.	
4	It should support more than 32,000 device profiles and 12,400 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.	
5	The solution should be able to integrate with a central management platform that can oversee usage, permissions, SOPs, configurations, licensing, and SW updates.	
6	The extraction software should be touch screen enabled, allowing easy use on tablets.	
7	The solution should have an autodetect function to locate and identify the mobile device.	
8	It shall have the ability to offer dynamic profiles of phones, based on IMEI, OS type, version and chipset.	
9	It should come with a compact and lightweight case with all necessary cables for the supported phones/OS).	
10	Support Android, iOS, Blackberry, Bada, Symbian & Windows mobile device and generic capabilities for certain chipsets like MTK and Qualcomm, to obtain decrypted Physical Extractions.	
11	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.	
12	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.	
13	The solution should be technically capable to perform SIM data extraction, i.e., the extraction of information from a SIM or USIM card.	
14	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.	
15	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.	
16	The solution must support the use of custom-made proprietary boot loaders instead of the 3rd party bootloaders.	
17	The software should provide lock bypassing physical extraction support for devices with Coolsand based chipsets.	
18	There should be a consent-based collection capability without the need to select the device profile and extraction method, solution should automatically use the relevant device access method and	

	present available extraction options to the user	
19	The software should allow the users to select specific files and folders in the file system for extraction	
20	The software should allow examiners to perform a quick selective extraction of specific applications or files, while doing Full File System extraction for supported Android as well as iOS devices.	
21	The software should also allow selective extraction of only cloud tokens from the phone while doing Full File System extraction.	
22	It should provide a simple extraction flow with generic extraction for unsupported devices.	
23	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.	
24	The software should also be supplied with a multi-SIM adapter with support for Micro, Nano and standard SIM cards.	
25	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	
26	The software should be able to categorize the applications and group these categories for 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.	
27	The software should have a workflow guidance widget to help managers and administrators to guide, control and enforce working procedures.	
28	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.	
29	The software should have the capability to allow the user to stop the Android File System extractions (except for Android Backup and APK downgrade) before they complete to save the partial extraction up to that point.	
30	**Extraction Support**	
31	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, running up to the Android 11. It should allow users to upload their own custom dictionary to enhance the unlocking process to make the process easier and faster.	
32	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.	
33	It should allow full backup of the Signal database from unlocked Android devices.	
34	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 supported with Android 12 as well.	

35	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.	
36	The software should allow full file system extraction for unlocked Huawei Kirin devices running Android 9 and higher	
37	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.	
38	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 popular 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 11.	
39	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.	
40	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, Exynos Live, 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.	
41	The software should provide capability to perform Full File System or Physical extraction from unlocked MTK 64-bit devices running Android 9 and above for devices like Oppo A55, Realme 7, Vivo Y19, Xiaomi 11T and others with chipsets like mt6732, mt6735, mt6738, mt6763, mt6768, mt6769, mt6771, mt6781, mt6785, mt6797,mt6983, mt8161, mt8163, mt8165,mt8732 and mt8752	
42	The software should provide capability to perform Full File System or Physical extraction from unlocked Exynos 64-bit devices running Android 9 and above for devices. It should support all Exynos chipsets up to Exynos 2200.	
43	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.	
44	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.	
45	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.	
46	It should support custom boot loaders to ensure forensically sound bit-by -bit physical extractions, without tampering the data.	
47	It should have support for data extraction, decoding and analysis for unlocked devices running up to iOS 16.0.	

48	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 15.7 depending on the iPhone device supported based on Apple official release	
49	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.	
50	It should be able to integrate with Active Directory for user authentication.	
51	**Support for Various Phones:**	
52	**Android Phones**	
53	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	
54	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.	
55	The software should able to support Samsung devices with full disk encryption such as Samsung S9 or Samsung Note 9 running on Android 10.	
56	It should support lock bypass using file system extraction for popular Samsung devices like Galaxy J7, Galaxy S8, Galaxy Note8 and Galaxy S8+.	
57	It should have lock bypassing decrypted physical extraction capability for Qualcomm Android devices including LG, ZTE, Xiaomi, Huawei, Alcatel and Motorola	
58	It should be able to perform selective file system extraction on popular Samsung models with the Qualcomm processor (SOC).	
59	The software should have a capability to extract Qualcomm chipset phone in a generic option that support popular brand like Samsung and Huawei.	
60	The software should have a capability to extract MTK chipset phone in a generic option.	
61	It should have decrypting bootloader capability for Huawei devices with HiSilicon Kirin chipsets and Samsung devices with Exynos processor	
62	It should be able to allows users to perform a full file system and selective extraction on smartphones with the Huawei HiSilicon 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.	
63	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	
64	It should support Physical Extraction over ADB for Samsung devices running up to Android OS v8	
65	It should support bootloader-based physical extraction for zte, alcatel and xiaomi devices running Qualcomm chipset	

66	It should support Partial File System extraction while bypassing User Lock for more than 100 Android devices	
67	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.	
68	It should support automatic detection of supported devices. It should also support manual search for devices by manufacturer, model and IMEI number.	
69	It should be able to perform physical, full file system and selective file system extraction on Smartphone with Samsung Qualcomm Processor	
70	It should acquire apps data from Android devices via all extraction types including:	
71	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	
72	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 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	
73	**Blackberry Phones:**	
74	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.	
75	BlackBerry Messenger (BBM) messages including Deleted messages and chats, message attachments, contact photos, BBM from groups: Chats, contacts and shared photos	
76	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).	
77	Address book, SMS, MMS, Emails, PIN messages, Calendar entries, Memo pad notes, Web browser history, Web bookmarks, Bluetooth devices and Cookies.	
78	Recent email contacts (BB OS 6 and above, where available)	
79	Device Info (Model, IMEI\MEID, ICCID, PIN, OS version, Platform, Supported Networks)	

80	Windows Phone:	
81	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.	
82	JTAG decoding of contacts, call logs and SMS from Windows Phone 8.x devices is enabled via physical extraction	
83	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.	
84	**Nokia BB5 Phones:**	
85	It should support bit-for-bit physical extraction from locked and unlocked Nokia BB5 devices using proprietary boot loaders.	
86	It should support decoding of Symbian databases including Decoding of intact and deleted contacts, SMS, MMS and call logs; Decoding support for multilingual content.	
87	**Portable GPS Device:**	
88	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.	
89	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)	
90	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	
91	**Feature Phones:**	
92	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.	
93	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.	
94	**Chinese Chipsets Based Phones:**	
95	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.	
96	The tool should provide generic extraction with Decrypting bootloader for MTK based chipsets including 6580, 6735, 6737, 6753, 6755, 6757 & 6797.	
97	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.	
98	**IOS Phones:**	
99	The supported unlocked 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, iphone 13, iphone 13 mini, iphone 13 Pro, iphone 13 Pro Max, iphone 14, iphone 14 Plus, iphone 14 Pro, iphone 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.	
100	Decoding of additional iOS databases from KnowledgeC, Health App, Siri native messages and Telegram should be supported.	
101	**Decoding and Analysis Capability**	
102	Capability to provide powerful decoding and analysis solution for the extracted device data and simplify the task of navigating through the device's data structures and to assist in the complex tasks of intelligence gathering, investigative research, and providing legal evidence in the form of reports.	
103	It should have a function to allow view of cloud data in the platform with a valid cloud extraction license. Users can review the device data and cloud data through a single software interface with a unified experience, for a seamless and simplified review process.	
104	It should be able to run Python scripts via plugins and edit and create new customized decoding chains.	
105	The software should enable the user to identify the usage of cryptocurrency and detect addresses or transactions within the device data to provide coin data including value, currency type, artifact type and model type.	
106	The software should have the media classification capability to detect and categorize images and video frames into key categories. This capability should be selectable and user should be able to decide if he wants to run the media classification on a particular case.	
107	The software should also be able to segregate the different media classifications into relevant groups like people, textual etc. to make the data review simpler and more efficient.	
108	It should be able to decode network usage information to record the sending and receiving of information via various network connections.	
109	It should be able to support parsing of the Samsung wiped data to get the device factory reset data and also able to detect the time of last iOS data-wipe	
110	It should support parsing of Apple pay data to get Apple wallet transactions and location data. Data should be available for transactions from both Safari and iMessages.	
111	It shall verify file integrity with use of MD5 and SHA 256.	
112	It should support tagging of events using one or more labels via hotkeys. It should have capability to import and export tags from one system to another as XML files.	

113	It should be able to support the applications such as WhatsApp, Skype, Facebook Messenger, Azar, Telegram, Discord, Tiktok, Wechat, Wickr, Reddit, Signal, Viber, Zalo, Cash App, imo, DuckDuck Go browser, Plus Messenger and WhatsApp dual mode.	
114	It should support the parsing of messages, calls and user accounts for the secure messaging app Threema for Android devices	
115	It should have a built-in SQLite Viewer.	
116	It should have a wizard to visually map data from databases which are not automatically decoded by building queries.	
117	It should be able to save the queries created by the wizard and then run them again when the same application is encountered in other extractions.	
118	It should have a built-in tool for researching databases recovered as part of the investigation using Fuzzy Model.	
119	It should be able to match files extracted against Hash Databases and it should have built-in support for Project VIC and CAID hash databases.	
120	It should allow user to have the control to input IMEI number to decrypt WeChat database if needed.	
121	It should include the provision of a case id as well as other relevant case-related information as part of the extraction report and allow filtering based on specified date range.	
122	It should enable visualizing of events over time, view distances between events and see the number of events within a defined timespan in a table.	
123	It should support viewing of all locations on a single map. It should enable viewing of extracted locations using offline maps even without an Internet connection. There should be an option to connect to offline maps from a shared central location.	
124	It should support the ability to highlight information based on predefined list of values.	
125	It should support viewing of text files including file information, content, and Hex.	
126	It should support quick search within decoded data.	
127	It should enable quick reference pointer to set to analyzed data item and data file item.	
128	It should support Hexadecimal view of the extracted data enabling advanced search based on multiple parameters, regular expressions and more.	
129	It should enable the translation of foreign-language content from extractions to English. In-built offline translation should be possible from at least 5 languages. If required, then at least 70+ languages should be available at additional cost.	
130	It should be able to Generate and customize reports in different formats e. g. PDF, HTML, XML, Excel and Word. It should provide global setting to select/unselect items in a report. The software should also allow to password protect the reports.	
131	There should be a time range filter for the reports to display data from a specific date and time range	
132	It should be able to provide a separate report with device information and user account information for quick reference of users.	

133	It should enable chat messages to be exported in conversation format, in PDF reports.	
134	It should support exporting selected emails to EML format.	
135	It should support hash verification to ensure the extraction decoded is the same extraction received from the device.	
136	It should be able to merge multiple extractions in a single unified report for efficient reporting and investigation.	
137	It should have the option to adjust the timestamp according to the time zone and offset setting on the device.	
138	The software should provide a file format viewer which allows users to view, search and copy readable content from various file types like plist, bplist, etc.	
139	It shall have an in-built screen capture capability to visually document (via pictures and/ or by video recording) and capture the examination process for sharing with stakeholders and easily insert it in a report.	
140	The software also has the capability to extract Google advertisement ID (AD-ID) on advanced logical extraction and iOS advertisement ID on iphones.	
141	The software should allow playback of WhatsApp audio files in analysis software. It should also provide indication of reply for WhatsApp messages in application and reports generated.	
142	It should have support decoding and review of secret messages from Facebook Messenger in Android, with support for vanish mode (self-destructing messages).	
143	It should have support for parsing WhatsApp's disappearing messages and iOS "view once" media. Should also supporting parsing of Signal iOS messages which were set to self-destruct at a specified date-time.	
144	It should be possible to validate the image hash directly from the software GUI	
145	The software is able to extract memory from Samsung devices to decrypt Samsung Health DB	
146	The software should decrypt and decode location information from Samsung Rubin service	
147	The software should be able to decrypt the Facebook messenger offline account on an iOS mobile device and parse the messages, calls and contacts.	
148	The software should support Samsung browser passwords and allow user to review the decrypted password data of the device owner.	
149	The software should be able to read interactionC database from IOS.	
150	The solution should come with separate software with below capabilities	
151	The solution should be able to perform searches of cryptocurrency artifacts from the HDDs in an offline mode. It should at least support popular cryptocurrencies, including 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. It should be able to scan a variety of document formats, including text files, documents, PDFs, images, emails, spreadsheets, wallets, and PowerPoints, to retrieve valuable information such as seeds, public keys, private keys, transaction hashes, currency names, currency symbols, and exchange names. Once the process is finished, users should be able to download a PDF	

	document containing the same results.	
152	It should allow users to select a file to generate its Hash Value.	
153	It should support Hash such as MD5, SHA1, SHA256, SHA512.	
154	It should allow users to export generated Result in PDF Format.	
155	It should allow users to Validate files against Hash value.	
156	It should allow users to Compare two files for any selected Hash.	
157	The software should support the following decoding capabilities:	
158	Decode the powering events, decode Samsung password manager and Samsung locked notes	
159	Decode iOS CashApp to parse user account, transactions, contacts, and credit card data	
160	Decode Microsoft Teams to parse chats, calls, contacts, user account, calendar events, and web artifacts	
161	Decode encrypted media from iOS Private Photo vault including location and transaction data, should include transactions done with Safari and iMessages	
162	Decode SkyPhone application to parse account information, address book and call history	
163	Decode Google Archive Files	
164	Decoding of backups for MTK based Android phones.	
165	Decoding of warrant return packages from WhatsApp, Facebook, Google, Snapchat, Instagram, Apple iCloud, Discord, TextNow and SkyECC	
166	Decoding of physical activity data from health and wellness applications	
167	Decoding of different WhatsApp variants like WhatsApp2Plus, obwhatsapp, ob2whatsapp, ob3whatsapp and ob4whatsapp	
168	Seamless process for cloud data decoding	
169	Automatic decoding of data from .zip and TAR files	
170	Decoding of the iCloud backup production set obtained from Apple devices and Instagram production set from other devices	
171	Decoding of Huawei backup and Huawei HiSuite backup.	
172	Decoding of ADB backup, MTK backup, iTunes backup, Blackberry 10 backup, Google Takeout (Google Archive) and LG backup	
173	User should be able to save and abort decoding process	
174	Decoding of Berla ivx files	

2.5 High End Forensic Workstation

S.No.	High End Forensic Workstation Specifications	Compliance (Yes/No)
1	A high-end analysis workstation for digital data processing with cyber speed.	
2	A high-end analysis workstation is the Non-Plus Ultra when it comes to indexing and processing IT forensic cases at the workplace.	
3	A high-end analysis workstation series are globally recognized and popular for its speed, reliability and durability.	
4	A high-end analysis workstation are certified and tested for the use of the programs of the leading software manufacturers (like Access Data, OpenText, Magnet Forensics, etc.)	
5	Should have 11 x 5.25 Drive Bays	
6	Should have 10-Core Intel® Core™ i9-10900X X-series Processor (19.25M Cache, 3.70 GHz - 4.50 GHz) with active liquid cooling	
7	Chassis: Must be a Big Tower Case: 306(W) x 651(H) x 639(D)mm	
8	Should have RAM 64GB (expandable up to 256GB)	
9	Should have 1 x 1TB SSD M.2 NVMe PCIe for OS 1 x 1TB SSD M.2 NVMe PCIe for Temp 4 x 4TB SSD M.2 NVMe PCIe in RAID0 via vroc"	
10	Should have Integrated Silent edition Write Blocker with IDE, SATA, USB, SAS, FIREWIRE, PCIe interface	
11	Should have NVIDIA GTX1660. 6GB memory, PCIe, HDMI/ DisplayPort	
12	Must have Retractable Ice Tray internal cooler for suspected drive	
13	Should have 10/100/1000 Mbs Gigabit Ethernet Network Adapter	
14	Should have 1 PCI-Express 3.0(x16)Slot	
15	Digital Optical S/PDIF audio output	
16	Should have 1 RJ45 LAN port (Gigabit LAN controller)	
17	Should have 802.11a/b/g/n/ac Wi-Fi+ Bluetooth 4.0	
18	Should have 1x USB 3.1 Type-C; 4x USB 3.0 Type A front Mounted	
19	Should have 2x USB 3.1 ports (1 port at Type A, 1 port at Type C) Back Mounted	
20	Should have Keyboard and Mouse Combo	
21	Should have Adapters and Cables: Cables and adapters to image and process internal/external drives including SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air Blade Type SSDs, mini/micro SSD cards, 1.8-inch IDE (iPod), 2.5 inch IDE (laptop), PCIe Card SSD Adapter, PCIe M.2 SSDS Adapter, PCIe Apple SSD Adapter and PCIe Cable	
22	Should have Windows 10 Professional 64-bit, Forensik Software: TIM (Tableau Imager, FTK Imager, EnCase Imager) Software	
23	Should have advanced malware discovery with the rapid search of malicious applications and comprehensive reporting. This should conduct scans on a stand-alone system or drive images. This should be able to Identify and categorize malware and potentially unwanted	

	applications using hash datasets. This should be scanned using factory, supplemental, and custom datasets. It should support Integration with Forensic Toolkit, Encase Forensic, Forensic Explorer, etc. It should support on-demand forensic malware discovery scans on a live system. It should support the discovery of botnets, trojans, anti-forensics, mobile malware, or a host of other malicious applications. It should have at least 12 months of support and updates.	
24	Support for Yara Rules can be created by own.	
25	Should have conduct scans on a stand-alone system or drive images.	
26	Support multiplatfom like Windows, Windows Sever, and Linux Platforms.	
27	Should have Identify and categorize malware and potentially unwanted applications using supplied hash datasets.	
28	should have provide access to monthly dataset updates	
29	Should have an External bootable HDD with pre-installed Backup Software	
30	Should be passed through 12/24 hours Burn-in Test with the accurate results	
31	OEM should be ISO 9001:2015 certified and the workstation should have a TUV quality certificate.	
32	Product should carry 3 (Three) Years On-Site Warranty. Any Software/ Firmware updates to be provided during the Warranty Period.	

3 Video Forensics

3.1 Video Analysis & Enhancement

S.No.	Specifications	Compliance (Yes/No)
1	**Import Capabilities**	
2	Import video, image and audio files quickly and easily	
3	Batch import video sequences from VMSes like Milestone and numerous directly supported proprietary files	
4	Supports and manages ingest of data from multiple storage sources and device type	
5	Import of digital video file format, Rapidly decode video using a unique combination of Windows codecs	
6	Import via screen capture from proprietary player using designed capture tool	
7	Support advanced importation of files from Ovation systems, Timespace and others.	
8	Gather screen capture technical information on frames rate etc when screen capturing	
9	Import from analog video sources	
10	Import for IP network camera and over the internet	
11	Automatic identification of video file format for standard file types	
12	Player Manager solution aims to identify correct Player to play a video file	
13	Player Manger provides a broad range of players and information on those players	
14	Store proprietary players in a library, enabling you to access the right player for a video	
15	Ensure you can play a video by using unique library of over 800 players	
16	Eliminate the installation of players by using virtualized players	
17	Automatically analysis codec and encoding of a file type	
18	Import multiple different sources of video simultaneously	
19	Organize and display multiple sources of video relating to your case	
20	Add evidential metadata to you video like source, exhibit reference etc	
21	Correct time anomalies by offsetting the time to the speaking clock.	
22	Ability to add Metadata information such as file/data format, capture information (e.g. location, time, camera settings)	
23	Ensure the integrity of your data by using frame by frame hashing	
24	Deinterlace video	
25	**Viewing/Exploration Capabilities**	

26	Display and view video on timeline	
27	Ability to split multiplexed video into different channels.	
28	Jump from one video to another video in your case quickly and easily	
29	Quickly review the timeline to see all motion events	
30	Search your video by time	
31	Review key events frame by frame	
32	Play/ Pause / Stop / Rewind video	
33	Speed up video playback for rapid reviewing	
34	Connect to jogg shuttler control device for fast review	
35	Pop out a video timeline to a second screen	
36	Rotate your video view	
37	Zoom in on key areas of the video to see objects clearer	
38	Lock timelines to view overlaps between to videos	
39	Ensure collaboration during a case with simultaneous multi-user access	
40	**Searching Video**	
41	Detect moving objects in video	
42	Process and search video with very low frame rates	
43	Process video with low light and poor quality	
44	Filter video for objects/movement (Allows user to select/omit data for viewing based on specified criteria) by:	
45	Search video automatically by direction i.e. movement right, left, straight etc	
46	Search video automatically by object colours	
47	Search video automatically by region i.e. partial view of recording	
48	Object tracking (following of a person/object/vehicle within a video without leaving the field of view)	
49	**Report**	
50	Create video and image reports	
51	Export multiple video frames to pdf document	
52	Add text notes to images	
53	Export video as a sequence of frames	
54	Select clips from a video manually	
55	Select clips from a video by slecting all events	
56	Ability to export all frames in a video clip	
57	Ability to storyboard clips from multiple video sources (Produces a shortened video that conveys all activity from a longer video stream)	
58	Ability to combine videos of different frame rates and aspect ratios to the same video report	

59	Correctly represent all original frame rates and frame sizes	
60	Edit a clip frame by frame	
61	Add text notes to images	
62	Add presentation slide with fade and cross fade options	
63	Export to .avi/ DVD	
64	Save a reporting project so you can return to it at a later date	
65	Quickly redact or highlight key persons or events of interest using blurring, pixilation, spotlight and arrows without having to do it frame by frame.	
66	Suspect tagging: Functionality for the manual annotation of content, e.g. persons wearing backpacks, license plate locations, pedestrian silhouettes	
67	Selection and filtering of tagging by object, key word and notes	
68	Image & video spotlight, blur and text options	
69	Create interactive viewing logs of key persons of interest across video sources in your case	
70	Export your viewing log to excel, MS Word or PDF	
71	Export your viewing log and video sources to the IBM Analyst Notebook for large scale data exploitation	
72	All video frames individually security tagged with both an opensource and a tamper evident digital signature.	
73	All reports are tagged with a tamper evident digital signature	
74	**Clarification of video and images**	
75	Clarify images and video using multiple and layer techniques	
76	Crop, lens distortion, perspective crop, rotate image, rotate or mirror, scale	
77	Brightness & Contrast, contrast crop, deinterlace, gamma correction, Invert, Noise removal, sharpening, split channel, Histogram Stretch, De blur, stabilize, super resolution, temporal median	
78	Check data integrity with tamper evident mechanism	
79	Side by side viewing of 2 video streams	
80	Automatic speed calculation algorithm	
81	Export video in side by side view	
82	**Video management**	
83	Change language	
84	Create named user logins and passwords	
85	Customised settings in Admin configuration e.g. user access, compression, reports templates	
86	Automatic speed calculation algorithm	
87	Export video in side by side view	

3.2 Face Recognition (Video Analytics)

S.No.	Specifications	Compliance (Yes/No)
1	**Face Detection** Solution should find the position and location of faces in photos or videos. This usually works despite of unfavourable lighting, rotations, partial occlusion or poor video quality. In video, faces are tracked from frame to frame to form continuous tracks. These tracks can be used for more precise identification than single frames alone.	
2	**Age and gender** In addition to classic identification, the age and gender of individuals can also be estimated by analysing the face. Thus, you can create statistics on the age and gender distribution of customer groups or start searches for these features ("soft biometrics").	
3	**Person and object recognition** Here people are recognized as a whole. This way, a person can be detected even if they are only partially in the picture or visible from behind only. With object recognition, you can quickly find different types of vehicles and luggage in the image and video material.	
4	**Face recognition** For facial recognition, so-called templates are extracted, which represent the individual characteristics of each face in a compact way. These templates can then be compared with reference templates of query identities. Creating identities from more than one reference template ("enrolment") leads to better recognition rates than with single template comparison.	
5	**Advanced facial features** You can also search for attributes such as glasses, masks, hats, beards, etc. It enables you to find people based on descriptions or, for example, to check whether or not they are wearing a mask.	
6	**Analyse videos and photos** automatically locates faces and creates templates. Each face or track becomes a discoverable event.	
7	**Live analysis** Cameras can be directly connected and analyzed in real time. In the live display, the resulting events can be observed as they are produced, hits are highlighted.	
8	**Integrated video player** In the built-in video player, every face is "clickable". There are also comfort functions such as magnification, variable speed, brightness adjustment, multi-monitor setup, etc.	
9	**Retrospective search** Using retrospective search, videos, pictures and camera recordings can be searched for identities that were not known at the time of the recording. Various sortings and filters are available. Freshly discovered sightings of a person can be added easily to the query identity in order to iteratively refine the search.	
10	**Manage identities** Identities can be created and dynamically extended with events from video or image sources. Image uploads can also be used to create identities.	

3.3 High End Forensic Workstation

S.No.	High End Forensic Workstation Specifications	Compliance (Yes/No)
1	A high-end analysis workstation for digital data processing with cyber speed.	
2	A high-end analysis workstation is the Non-Plus Ultra when it comes to indexing and processing IT forensic cases at the workplace.	
3	A high-end analysis workstation series are globally recognized and popular for its speed, reliability and durability.	
4	A high-end analysis workstation are certified and tested for the use of the programs of the leading software manufacturers (like Access Data, OpenText, Magnet Forensics, etc.)	
5	Should have 11 x 5.25 Drive Bays	
6	Should have 10-Core Intel® Core™ i9-10900X X-series Processor (19.25M Cache, 3.70 GHz - 4.50 GHz) with active liquid cooling	
7	Chassis: Must be a Big Tower Case: 306(W) x 651(H) x 639(D)mm	
8	Should have RAM 64GB (expandable up to 256GB)	
9	Should have 1 x 1TB SSD M.2 NVMe PCIe for OS 1 x 1TB SSD M.2 NVMe PCIe for Temp 4 x 4TB SSD M.2 NVMe PCIe in RAID0 via vroc"	
10	Should have Integrated Silent edition Write Blocker with IDE, SATA, USB, SAS, FIREWIRE, PCIe interface	
11	Should have NVIDIA GTX1660. 6GB memory, PCIe, HDMI/ DisplayPort	
12	Must have Retractable Ice Tray internal cooler for suspected drive	
13	Should have 10/100/1000 Mbs Gigabit Ethernet Network Adapter	
14	Should have 1 PCI-Express 3.0(x16)Slot	
15	Digital Optical S/PDIF audio output	
16	Should have 1 RJ45 LAN port (Gigabit LAN controller)	
17	Should have 802.11a/b/g/n/ac Wi-Fi+ Bluetooth 4.0	
18	Should have 1x USB 3.1 Type-C; 4x USB 3.0 Type A front Mounted	
19	Should have 2x USB 3.1 ports (1 port at Type A, 1 port at Type C) Back Mounted	
20	Should have Keyboard and Mouse Combo	
21	Should have Adapters and Cables: Cables and adapters to image and process internal/external drives including SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air Blade Type SSDs, mini/micro SSD cards, 1.8-inch IDE (iPod), 2.5 inch IDE (laptop), PCIe Card SSD Adapter, PCIe M.2 SSDS Adapter, PCIe Apple SSD Adapter and PCIe Cable	
22	Should have Windows 10 Professional 64-bit, Forensik Software: TIM (Tableau Imager, FTK Imager, EnCase Imager) Software	
23	Should have advanced malware discovery with the rapid search of malicious applications and comprehensive reporting. This should conduct scans on a stand-alone system or drive images. This should	

	be able to Identify and categorize malware and potentially unwanted applications using hash datasets. This should be scanned using factory, supplemental, and custom datasets. It should support Integration with Forensic Toolkit, Encase Forensic, Forensic Explorer, etc. It should support on-demand forensic malware discovery scans on a live system. It should support the discovery of botnets, trojans, anti-forensics, mobile malware, or a host of other malicious applications. It should have at least 12 months of support and updates.	
24	Support for Yara Rules can be created by own.	
25	Should have conduct scans on a stand-alone system or drive images.	
26	Support multiplatfom like Windows, Windows Sever, and Linux Platforms.	
27	Should have Identify and categorize malware and potentially unwanted applications using supplied hash datasets.	

4.1 Audio Forensics

S.No.	Specifications		Compliance (Yes/No)
1	Export/import database	It should allow the export and import of the population database	
2	Export/import speakers	It should enables individual or batch export/import of speakers, with the option to selectively include or exclude specific speakers	
3	Voiceprint compatibility	It should support voiceprint compatibility with SID L4 or SID XL5 versions of the Speech Engine	
4	Report editing	It should provide report edit functionality	
5	Custom report templates	It should offer customizable report templates (format and language)	
6	Language-independent comparison	Solution should allow analysis of any language and comparison of speakers speaking different languages	
7	PDF plots	Solution should Utilize PDF plots, histograms, and statistical representations for target and nontarget scores and opposing hypotheses (same speaker vs. not the same speaker)	
8	DET graph visualization	Solution should provide visualization of the Detection Error Tradeoff (DET) graph	
9	Tippett plots	Solution should enable Tippett plot graph visualization	
10	CLLR calculation	Solution should automatically calculates Log-Likelihood Ratio Cost (CLLR)	
11	Diarization	Solution should support diarization with manual input of the maximum number of speakers in a recording	
12	Portable software	Solution should be installed as a single zip file with no external dependencies, allowing installation on a portable pendrive	
13	Results saving	Solution should have option to save results to a specified work directory location outside of the installation directory	
14	Package size	Solution should be less than 300 MB in size for easy installation	
15	Operating system support	Solution should have Compatible with Linux and Windows	
16	Offline licensing options	Solution should offer both Hardware tied license and USB dongle license for offline licensing	
17	Customizable reports	Solution should enable customization of reports before saving or printing within the software	
18	Visualization features	Spectrogram, power panels, and waveform visualization of recordings	
19	Phoneme search	Solution should allow phoneme search and phoneme type search	

20	Identical phoneme sequence search	Solution should enables the search for identical sounding phoneme sequences, with user input for the length of identical phoneme sequence	
21	Audio editing capability	Solution should enables the removal of other speakers by replacing their speech with silence	
22	Support	SW vendor provides support within 8 business hours	
23	Recording quality estimator Includes an estimator for assessing recording quality, summarizing key audio	Solution should include an estimator for assessing recording quality, summarizing key audio aspects such as Signal to Noise Ratio, codec used, audio length, and speech length.	
24	Minimum speech setting	Solution should have configurable setting for minimum speech required for comparison	
25	Minimum SNR setting	Solution should have configurable setting for minimum Signal to Noise Ratio required for comparison	
26	Module version requirement	Solution should require the Speaker identification module no older than 1 year	
27	Knowledge base and support portal	Solution should offer a publicly available knowledge base portal, including a support portal.	

4.2 Hardware

S.No.	Workstation Specifications	Compliance (Yes/No)
1	Processor: Intel Core i7 or Higher	
2	Memory: RAM 32 GB	
3	Hard Disk: 1 TB or higher	
4	Operating System: Windows 10 or higher	
5	Screen 21 inch or higher	
6	Any software hardware required to run solution quoted by bidder	

5. Drone Forensics

S.No.	Specifications	Compliance (Yes/No)
1	**Various extraction methods for wide range of drone aircraft**	
2	- Extraction through the drone aircraft USB connection	
3	- Extraction through the network connection (WiFi)	
4	- Extraction through SD card	
5	- Chip-off Extraction (Requires memory Chip socket and reader)	
6	- drone App data should be extracted and exported to solution.	
7	- Provides an Extraction guide for each method	
8	**Timeline-based integrated flight data analysis**	
9	- Timeline-based flight parameter values (speed, altitude, value of each motor, etc.) can be viewed in graphic format	
10	- Drone's position and posture (Yaw, Roll, Pitch) information on the timeline	
11	- Integrated view of flight history and media data preview on the Timeline	
12	- Playback and reconstruct flight history on the map	
13	- Check the selected media in the Timeline chart	
14	**Deep analysis of flight data by AI and machine learning**	
15	- Learning of accidental or abnormal flight log data	
16	- Find out the collision, battery exhaustion, normal landing and abnormal flight position/time	
17	**Detail flight data view and selection**	
18	- Detailed values of the flight log in the table and visualization on the map	
19	- Classify meaningful flight log values such as altitude, ground speed, battery, and signal strength and display in different colours on the map	
20	- table view of GPS-based drone track, latitude, longitude and movement history	
21	- Sorting and filter flight data in time order	
22	**Multimedia gallery**	
23	- Select the multimedia (video, photo) file with the matching time information in the flight record	
24	- filter the multimedia file by such as the path, creation date, and size	
25	- Intuitive analysis through the preview feature	
26	**Bookmark**	
27	- Supports bookmark feature for flight time range, image and video	

28	**Notification**	
29	- Displays and saves important notifications during Extraction and analysis while using the product in the notification centre	
30	**Report generation**	
31	- Supports to export reports in PDF format based on the bookmarked contents	
32	- Supports to export each manufacturer's flight log glossary in csv format	
33	**Multimedia Export**	
34	- Supports to export the acquired original multimedia data (photo, video)	
35	**Supported drone aircraft list - aircraft - USB connection**	
36	• DJI (Phantom 4 series, Mavic Pro series, Inspire 2, Matrice 600), • Yuneec Typhoon H Plus, • ALLNEWTECH ANT-H5, • Sundori SDR-H-2021, SDR-M1, • EFT (EFT-E610, Flight Control Computer - USB connection, • DJI (A3, N3), • PixHawk (PixHawk4, The Cube, V5+, PX4_2.4.6, PixHawk New X7, PixHawk V5+, PixHwak2 Cube Orange, SD Card of Drone), • DJI (Phantom 3, 4 series, Mavic Pro series), • PixHawk (PixHwak4 series, PX4 2.4.6 series, Cube, V5+, X7), • Yuneec Typhoon H Plus, • All UAVs which use SD Card for their multimedia storage Chip-off, • DJI (Mavic 2 Pro, Mavic Air, Mavic Air 2, Spark, FPV, Matric 300), • Parrot (Bebop2, WiFi Network), • Parrot Bebop2	

6.1 OSINT & Darkweb Analysis

S.No.	Specifications	Compliance (Yes/No)
1	It Should be a professional bundle combining more than 1000 methods for Social Media, DarkNet, Blockchain, Internet Leakages, Corporate sources, messengers, and more resources. It easily allows one to discover the complete online presence, identify the person behind digital credentials, and map group structure and members affiliation easily and conveniently.	
2	PEOPLE SEARCH: Search using just a name or a photo of the target person, find people, profiles, events, companies, and posts by geolocation, find profiles in social networks, DarkNet and other resources by only nickname or alias	
3	SOCIAL NETWORKS: Allows you to find the subject's profiles in all social networks simultaneously: Facebook, Instagram, LinkedIn, Twitter, Youtube, Tinder, Snapchat, Tiktok, Whatsapp, Telegram, and more	
4	OBJECT DETECTION: Identify weapons, cars, masks, and faces in images, albums, and videos on Facebook, YouTube, Instagram, and many others	
5	PUBLIC DATABASES: Search the world's largest Yellow Papers and White Papers, company registries, public documents, and 10TB+ of Internet leaks database	
6	It should be protects your investigation and provides highly stable service.	
7	Data mining methods that collect data in real time as well as from historical data bases	
8	Some unique transforms: - Get mutual friends/visited places/groups/pages/likes/comments for two Facebook users with one click.	
9	- If the friends list of the 'target' person is private, you can still get all Facebook users, who made any kind of activity with the target – likes, comments, reposts, etc.	
10	With one click, you can check the 'target' person profiles in socials. You need only a name and a photo. Or look for the 'target' person in the photos on the other person's profile, as well as in the photos from the chosen geolocation	
11	Unique search in 30+ DarkNet forums and marketplaces without authorisation by Phrase, PGP Key, Alias, also, you can get analytics by Products and Locations (shipping from/to).	
12	IT should be with database – 9 billion records about people, companies, places and their connections. We collect them from internet leaks.	
13	Most of the data is obtained by parsing a variety of white and yellow pages, company registers, business directories, social networks and other open online sources.	
14	Increase investigation efficiency to get in one workplace powerful instruments, such as Pipl database, Bitcoinwhoswho, Securitytrails, Censys, Shodan, ZoomEye, WhoisXML and others.	
15	Advanced searching in: Facebook, Twitter, OK, Google.	

16	Available methods for searching by date:	
17	Facebook - Photos/Videos/Stories by type All/Liked/Tagged in/ Commented.	
18	Twitter - from Entity [Advanced Twitter search], tweet, hastag, keyword	
19	Instagram - search video by date, search 'Target' person's faces in location photos by date, etc	
20	Search for user profiles with the chosen alias in more than 500 sources with one transform	
21	Social media : Facebook, Instagram, LinkedIn, Twitter, TikTok, SnapChat, Skype, Xing, Foursquare, VK, OK, Tumblr, Gravatar, Flickr, Github, MyMail, MySpace, , Steam , Google ID, Youtube, Google ID and others 500+ sources for alias-profile matching	
22	Messengers : Telegram, WhatsApp, Skype, Discord	
23	Corporate : CompaniesHouse, Companies OC, Google Companies, OCCRP, Offshores, Vulners	
24	Social Network Database : 10+ TB with e-mails, aliases, names, phone numbers	

6.2 Hardware

S.No.	Workstation Specifications	Compliance (Yes/No)
1	Processor: Intel Core i7 or Higher	
2	Memory: RAM 32 GB	
3	Hard Disk: 1 TB or higher	
4	Operating System: Windows 10 or higher	
5	Screen 21 inch or higher	
6	Any software hardware required to run solution quoted by bidder	

7. Crypto Investigation Solution

S.No.	Specifications	Compliance (Yes/No)
1	Should allow even non-technical agents and analysts to easily identify and trace criminals who attempt to use Bitcoin on the internet to conceal their illicit activities.	
2	Solution should cover a wide range of blockchains including BTC, ETH, and others.	
3	Solution should be able to trace risky transaction activity across addresses and entities.	
4	Should identify risky attributes of crypto addresses, wallets, and related businesses participating in Bitcoin transactions—such as mixers, ransomware, and dark markets.	
5	Should help law enforcement follow digital money trails for illicit crime across multiple addresses and hops	
6	Platform should handle indirect exposure and multi-path tracing of connections between addresses and known entities.	
7	Blockchain search engine should allow a user to simply enter a cryptocurrency address or transaction ID into an intuitive search bar that can auto-complete long addresses.	
8	Provide high-quality attribution information	
9	Platform should rapidly aggregate and correlate a variety of indicators, and then provide users with risk assessments and actionable intelligence.	
10	Offer an interactive user interface should allow non-technical users to quickly perform deeper investigation and visualize cryptocurrency transaction flows. This capability should enable investigators to follow virtual money trails without having to become cryptocurrency or blockchain experts.	
11	Should profile hundreds of global exchanges, ATMs, mixers, money laundering systems, gambling services, and known criminal addresses. should then assigns risk levels to transactions, wallets and entities based on known associations with suspicious addresses	
12	Solution should cover a wide range of blockchains. Blockchains supported should include Bitcoin, Ethereum, Solana, Tron, Polygon, Avalanche, and Binance Smart Chain.	
13	Solution should be able to trace derivative assets, wrapped assets, stablecoins, and NFTs	
14	Solution should provide the source of risk attribution and associated confidence scores for all individual addresses	
15	Solution should support cross-chain tracing showing the flow of funds across all assets and all chains in a single graph	
16	Solution should be able to support address and cluster level tracing within the same graph	
17	Solution should be able to showcase programmatic money laundering with 1-click tracing capability showing transactions across multiple addresses and hops.	
18	Solution should integrate with Open Source intelligence sources, including Chainabuse and others.	

19	Solution should support over 150 Risk Categories to catch a wider set of illicit activity	
20	Solution should provide an intuitive and flexible User Interface that is easy to understand and use	
21	Solution should offer a flexible graphing platform allowing users a large range of customization options.	
22	Solution should offer Platform-independent Training and Certification, available for different user experience levels	

8. Forensic Imager

S.No.	Specifications	Compliance (Yes/No)
01	Capable to imaging/clone data from one to one, two to two or one to many destination media	
02	Capable to imaging/clone data at the speeds of 50GB/min or higher. Clone PCIe to PCIe at speeds of over 100GB/min	
03	Support multiple Imager Formats, copy, dd image,.dmg image, e01, ex01, supports MD5, SHA1, SHA256 and dual-hash (MD5+SHA-1) authentication	
04	Can use up to 10 sources and 11 destinations for imaging (with verify), hashing, or wiping for ultra efficient operation	
05	Multiple Imaging Ports:	
06	write-protected source ports include:	
07	1 SAS/SATA (SAS-3/12Gbps) that supports up to 4 drives with a single cable	
08	2 USB 3.2 Gen 2 (can be converted to SATA using an optional USB to SATA adapter)	
09	1 PCIe	
10	2 I/O ports for use with optional I/O cards including Thunderbolt 3/USB-C	
11	multiple destination ports include:	
12	1 SAS/SATA (SAS-3/12Gbps) that supports up to 4 drives with a single cable	
13	4 USB 3.2 Gen 2 (can be converted to SATA using an optional USB to SATA adapter)	
14	1 PCIe	
15	1 I/O ports for use with optional I/O cards including Thunderbolt 3/USB-C.	
16	Should have Two 10GbE network ports for network connectivity. The unit should include a USB 3.2 Gen 2 device port for drive preview and two USB 2.0 host ports	
17	Should allow imaging to an external storage device such as a NAS, using the 10GbE ports, USB 3.0 or via the SAS/SATA connection.	
18	Should be able to Simultaneously perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats. Image simultaneously from multiple sources to multiple destinations including a network repository. Supports imaging to one location while simultaneously hashing and/or wiping a second drive. Perform up to 5 tasks concurrently. Little or no speed degradation when imaging from two sources to two destinations	
19	Capable Web Browser/Remote Operation to allows to connect with device from a web browser	
20	Capable to cross copy support for IDE, SATA, e SATA, microSATA, SAS, ZIF and USB interface and combine-SATA etc.	

21	Should image CD/DVD/Blu-ray media by using a USB optical drive connected to the USB port on the device	
22	Capable to Detect and capture Host Protected Areas (HPA) and Device Configuration Overlay (DCO) hidden areas on the source (suspect) drive	
23	Should Capture network traffic, internet activity and VOIP.	
24	Capable to Generate Audit Trail Reporting/Log Files in XML, HTML or PDF format	
25	Should Secure sensitive evidence data with whole drive AES 256-bit encryption	
26	Allow to manipulate the DCO and HPA area of the destination drive so that the destination drive's total native capacity matches the source drive	
27	USB Host Ports and HDMI Port for connecting keyboard, Mouse and with Projector	
28	Forensic, Filter-Based File Copy, users can filter and then image by the file extension (such as.PDF,.xls, JPEG, .mov etc.).	
29	Capable to acquire data over a network	
30	Capable to generate the log of the processes	
31	Capable to boot/mount the suspect media virtually in a write protected environment for preview of live data.	
32	USB Host Ports and HDMI Port for connecting keyboard, Mouse and with Projector	

9. All in One Write Blocker

S.No.	Specifications	Compliance (Yes/No)
1	Must be very small, very light, extremely versatile, highly usable and easy to carry	
2	Should have Integrated Write Blocker with IDE, SATA, USB, SAS, FIREWIRE, PCIe interface	
3	Must have Retractable Ice Tray internal cooler for suspected drive	
4	Must have Forensic Card Reader for Compact Flash Card (CFC) - MicroDrive (MD) - Memory Stick Card (MSC), Memory Stick Pro (MS Pro) - Smart Media Card (SMC) - xD Card (xD), Secure Digital Card (SDC and SDHC) - MultiMedia Card (MMC)	
5	Must have 1x 4TB Enterprise HDD, SATA III in removable tray	
6	Must have Trayless Mobile Rack for 3.5" SATA HDDs	
8	Must have 2-Port USB Read/Write port Hub	
9	Must have 5x Anti-Static DriveBox for 3.5" HDD's (empty)	
10	Must include a cable set with all the necessary connector cables, adapters, a fine tool-kit and a sturdy but lightweight case (cabin luggage size) for easy transportation.	

10.1 CDR & IPDR Analysis Tool

S.No.	Specifications	Compliance (Yes/No)
1	**Data Acquisition**	
2	Data Normalization	
3	Ensures 100% file import	
4	Maintains file integrity	
5	Generates ETL logs	
6	Stores original file	
7	**Data Analysis**	
8	CDR, IMEI and TDR Analysis	
9	Number Tracing	
10	Pattern Analysis	
11	Behaviour Analysis	
12	Option to add Photos, Voice samples, Video files etc.	
13	Easy identification option (colour important numbers)	
14	**Robust Search Engine**	
15	CDR, IPDR, SDR, ILD search	
16	Fuzzy search	
17	Nested Search	
18	Geo Search	
19	Phonetic search	
20	Percentage match	
21	**Data Visualisation**	
22	Social Network Analysis based on these Centrality Measures - Degree - Betweenness - Closeness	
23	Forced Chart, Hierarchy Chart, Timeline Chart, Chain of Calls	
24	**Data Repository**	
25	Local or centralised configuration	
26	Entity data management	
27	Easy evidence tagging	
28	**Geo – Analysis**	
29	Crime Mapping	

30	Logical Geo – fences in maps	
31	Matching of Movements	
32	Plotting route on map	
33	Find nearest tower	
34	**IPDR Module**	
35	Pinpoint app to app internet calling in IPDR	
36	Identification of B-Party in app-to-app internet calling	
37	Common numbers	
38	Uncover suspect connections	
39	**SMS Query**	
40	Retrieval of SDR data with SMS	
41	Fetch data from centralised server	
42	**"Out of Box" Search**	
43	System wide search	
44	Multiple data sources	
45	External data search	
46	**Data Synchronisation**	
47	Sync files from android app	
48	Sync CDR, IMEI data from desktop app to android app	

10.2 Hardware

S.No.	Workstation Specifications	Compliance (Yes/No)
1	Processor: Intel Core i7 or Higher	
2	Memory: RAM 16 GB	
3	Hard Disk: 500 GB	
4	Operating System: Windows 10 or higher	
5	Database Software: MS SQL Server 2008 R2 or Higher Editions: Express Edition, Standard Edition or Higher	
6	.Net Framework 3.5/ .Net Framework 4.0 Service pack 1 or higher	
7	Microsoft Office 2010 or higher	
8	Screen 21 inch or higher	

11.1 Financial Data Analysis Tool

S.No.	Specifications	Compliance (Yes/No)
	Various File Formats Financial Data	
1	The system should accept (able to upload) Financial Data (Transaction Date Value Date, Description, Ref. No./ Cheque No. Debit, credit, Balance)) from Excel, Txt, CSV, MSSQL Server, MS-Access, PDF and HTML format and all other common formats. Able to define, modify and update import formats for data across Financial Institutes.	
	Financial Data Importing	
2	The system to ensure the automated acquisition and processes individual files or it should be done in batch mode.	
	Sorting/Filtering Financial Transactions	
3	The system should support for multiple sorting criteria for the required information on the available data.	
4	Comprehensive search should be provided on multiple criteria like • Transaction Date • Value Date • Description(ATM Withdrawal, To Transfer, RTGS, NEFT, Cash) Reference Number, Cheque No. • Debit • Credit • Balance	
5	The system should to allow user to categorize the data on various parameter like transaction type amount etc	
6	The system should allow user to apply multiple filters and get the desired results. NEFT transaction of more than particular amount from a individual account.	
	Identify High Value transactions	
7	The system able to identify high value / low value debit/credit transaction with conditions (>, <, =) specified Amount.	
8	The system able to identify high value/ low value debit/credit transaction between two entities with specified period of time.	
	Identify Mode of Transfer	
9	The system able to identify and list all transactions done in one account by different modes like NEFT,RTGS,Cheque,Cash	
10	The system able to identify and list all debit/credit transaction where transaction type is cash.(or any other mode like NEFT,RTGS,Cash)	
	Group Rotation of money/suspect money laundering Transactions	
11	The system should be able to identify the frequency of transaction between two accounts. The system should also be able to identify on the basis of mode of transfer or credit/debit transaction with (<,>) specified amount.	
12	The system should be able to identify group rotation of money among some accounts and also show other details like mode of transfer, transaction value, date etc	

13	The system able to identify key accounts where money exits or rotates in different accounts.	
	Key Word Search	
14	The system to enable the user to analyze 'text fields' of the transaction data.(i.e Transaction Description)	
	Data merging/ Demerging	
15	The system should allow user to analyze cumulative data of all the years by merging different files together.	
16	The system should allow user to merge transactions data of one or more individual spread over single or multiple entity further spread over single multiple entity branches.	
17	The system should allow user to apply various sorting and filtering criteria to merged/cumulative data.	
	Data Visualization	
18	The system should be a graphical interactive tool to analyze the Financial data by creating clusters or groups to depict possible routes of money flows.	
	Advance Search	
19	The system should allow user to perform customized search using logical and financial formulae.(And,Or Not).The system should allow user to cross manipulate among different result sets.	
	Case Visualizer	
20	The system should provide a facility to build the required case visually. Software should enable the IO to build up the case visually by selecting the entities identical to that of entities present in the case currently being investigated and it should also provide functionality to illustrate the communication between the entities whether the communication is two way or one-way and it should also enable the IO to customize the appearance of the required entities	

11.2 Hardware

S.No.	Workstation Specifications	Compliance (Yes/No)
1	Processor: Intel Core i7 or Higher	
2	Memory: RAM 16 GB	
3	Hard Disk: 500 GB	
4	Operating System: Windows 10 or higher	
5	Database Software: MS SQL Server 2008 R2 or Higher Editions: Express Edition, Standard Edition or Higher	
6	.Net Framework 3.5/ .Net Framework 4.0 Service pack 1 or higher	
7	Microsoft Office 2010 or higher	
8	Screen 21 inch or higher	

12 Password Cracking Solution

S.No.	Specifications	Compliance (Yes/No)
1	Password recovery cluster performance with up to 69,92 TeraFlops and 39936 Cuda Cores	
2	Chassis: - 4U / Full Tower Chassis Supports max. Motherboard, Sizes – E-ATX 15.2" x 13.2"/ ATX/Micro ATX	
3	Must have 8x3.5" SAS/SATA Backplane for Hot-Swappable Drives (Support SES2)	
4	Must have 11x Full-Height, Full-Length Expansion Slots Optimized for 4x Double Width GPU Solution	
5	Must have (2x) Rear Additional 80mm PWM Fans & (4x) Middle Lower 92mm PWM Fans	
6	Power supply: 2000W Redundant Titanium Level Certified High-Efficiency Power Supply	
3	CPU: 1x 8-Core Intel® Xeon® Silver Processor 4215 (11 MB Cache, 2,50 GHz)	
4	RAM: 4x 32GB DDR4-RAM - ECC REG	
5	System Drives: 1x 1000GB SSD, m.2 for OS	
6	Graphic cards: 4 x NVIDIA RTX A2000 12GB GDDR6 PCIe 4.0x16 (Quadro)	
	GPU memory 12GB 12 GB GDDR6 Memory interface 192-bit Memory bandwidth 288 GB/s NVIDIA Ampere architecture-based CUDA Cores 3,328 NVIDIA third-generation Tensor Cores 104 NVIDIA second-generation RT Cores 26 Single-precision performance 8.0 TFLOPS2 RT Core performance 15.6 TFLOPS2 Tensor performance 63.9 TFLOPS3	
7	Periphery: Keyboard / Mouse Kit	
8	Software: - Windows 10 Professional 64-bit. DualBoot with Windows & KaliLinux should be possible	
9	Solution must be Certified and tested with Passware Kit Forensic and ElcomSoft distributed Password Recovery.	
10	Should instantly recover many password types.	
11	Should instantly decrypt MS Word and Excel files for all versions (including Decryptum attack).	
12	Should reset passwords for Local and Domain Windows Administrators instantly.	
13	Should recover encryption keys for hard disks protected with BitLocker, including BitLockerToGo.	
14	Should decrypt TrueCrypt.	
15	Should recover from 8 different password attacks (and any combination of them) with an easy-to-use setup wizard and drag & drop attacks editor.	

16	Should use multiple-core CPUs and NVIDIA GPUs efficiently to speed up the password recovery process.	
17	Should provide detailed reports with MD5 hash values.	
18	Should be capable of recovering Mac User Login passwords and FileVault2 keys from computer	
19	Should support Distributed and Cloud Computing password recovery on both Windows and Linux platforms	
20	Should recover passwords for Windows users from a memory image or a standalone SAM file, including UPEK	
21	Should recover passwords for email, websites and network connections from standalone registry files in a very short time.	
22	Should have Search Index Examiner to retrieve electronic evidence from a Windows Desktop Search Database	
23	Should be able to decrypt passwords for Facebook, Google, and other websites from live memory images or hibernation files	
24	Should include Special password recovery attacks such as: Rainbow Tables, Decryptum, SureZip, ZipPlaintext	
25	Should support Password modifiers (case changes, reversed words,etc.)	
26	License term for the software must be for a period of 3 years with regular upgrades and updates.	

13 Implementation

S.No.	Requirement	Compliance (Yes/No)
1	Vendor have to do complete implementation of all the solutions.	
2	One time Implementation to be done Onsite.	
3	Open Source software provided by us has to be implemented by the vendor.	

Bill of Quantity

BOQ Compliance to be submitted along with technical bid. No partial Bidding Allowed.

Item Description	Technical Seps No.	License Type	Support	Total Qty	Quoted (Yes/No)
Computer Forensic	1.1	30 User Academic License	3 Years	1	
	1.2	Perpetual License	3 Years	10	
	1.3	Digital Investigation Platform 15 User License	3 Years	1	
	1.4	Hardware	3 Years	30	
Mobile Forensic	2.1	1 User License with Hardware	3 Years	3	
	2.2	1 User License	3 Years	3	
	2.3	1 User License	3 Years	1	
	2.4	1 User License	3 Years	1	
	2.5	High End Forensic Workstation	3 Years	5	
Video Analysis	3.1	1 User License	3 Years	1	
	3.2	1 User License	3 Years	1	
	3.3	High End Forensic Workstation	3 Years	1	
Audio Analysis	4.1	1 User License	3 Years	1	
	4.2	Hardware	3 Years	1	

Drone Forensics	5	1 User License	3 Years	1	
OSINT with Darknet Analysis	6.1	1 User License	3 Years	1	
	6.2	Hardware	3 Years	1	
Crypto Investigation	7	1 User License	3 Years	1	
Forensic Imager	8	Hardware	3 Years	1	
All in One Write Blocker	9	Hardware	3 Years	1	
CDR IPR Analysis Tool	10.1	1 User Academic License	3 Years	1	
Hardware	10.2	Hardware	3 Years	1	
Financial Data Analysis Investigation	11.1	1 User Academic License	3 Years	5	
Hardware	11.2	Hardware	3 Years	1	
Password Cracking Solution	12	Hardware & Software	3 Years	1	
Implementation	13	1 Job	One Time	1	

Place:
Date:

Signature of the Tenderer
Name & Address of the
Tenderer with Office Stamp

ANNEXURE-IV

OEM CERTIFICATION FORM

(In Original Letter Head of OEM)

Tender No: ..... Dated: .....

We are Original Equipment Manufacturers (OEM) of..... (Name of the company) Ms..... (Name of the vendor) is one of our Distributors/Dealers/Resellers/Partners (tick one) for the ..... and is participating in the above-mentioned tender by offering our product model.....(Name of the product with model number).

..... is authorized to bid, sell and provide service support warranty for our product
as mentioned above.

Name and Signature of the
Authorized signatory of OEM
along with
seal of the company with Date

Annexure V

NON-BLACKLISTING DECLARATION

Date: XXXX

Subject: Non-Blacklisting declaration in connection with tender RFF No: XXXXXX for procurement of "XXXXXXXXXXXXXXXXXXXXXXXXXXX"

This is to notify you that our Firm/Company/Organization <*provide Name of the Firm/Company/Organization*> intends to submit a proposal in response to the invitation for procurement of "XXXXXXXXXXXXXXXXXXXXXXXXXX" In accordance with the above we declare that:

a. We are not involved in any major litigation that may have an impact of affecting or compromising the delivery of services as required under this assignment.

b. We are not blacklisted by any Central/ State Government/ agency of Central/ State Government of India or any other country in the world/ Public Sector Undertaking/ any Regulatory Authorities in India or any other country in the world for any kind of fraudulent activities in last 3 years.

Place:
Date:

Signature of the Tenderer
Name & Address of the Tenderer with Office Stamp

Annexure - VI

TENDER CHECKLIST – Mandatory to be filled in and upload in the portal along with specification Document.

(1) Completed and **Signed Form of Tender**. The Form of Tender document shall be signed by a person legally authorized. ☐

(2) Completed Technical Compliance Statement. ☐

(3) OEM/Bidder Undertaking of similar contracts completed/Product supplied. ☐

(4) Manufacturer Authorization Form from OEM is mandatory if Indian agent/Indian office of OEM is participating in this tender on behalf of OEM. (Ref. tender document pg.no. 2, Point no.2) (Annexure IV) ☐

(5) EMD Submitted (If applicable) ☐

(6) Land border certification (Annexure II) ☐

(7)Non-Blacklisting Declaration (Annexure V) ☐

(8) Acceptance of General Terms & Conditions under Technical Specification ☐

The above documents should be provided for a contractor's bid to be valid. Bidders are asked to supply and tick off the required information. Failure to provide any of the stated documents may result in the bid being considered non-compliant and rejected.

Signature of the Bidder

FINANCIAL BID (PROFORMA) - BILL OF QUANTITIES (BOQ)

Item Name: Cyber Innovation Centre.

Item Description	Tech Spec. No.	License Type	Support/ Warranty	Qty	Unit Rate	Amount
Computer Forensic	1.1	30 User Academic License	3 Years	1		
	1.2	Perpetual License	3 Years	10		
	1.3	Digital Investigation Platform 15 User License	3 Years	1		
	1.4	Hardware	3 Years	30		
Mobile Forensic	2.1	1 User License with Hardware	3 Years	3		
	2.2	1 User License	3 Years	3		
	2.3	1 User License	3 Years	1		
	2.4	1 User License	3 Years	1		
	2.5	High End Forensic Workstation	3 Years	5		
Video Analysis	3.1	1 User License	3 Years	1		
	3.2	1 User License	3 Years	1		
	3.3	High End Forensic Workstation	3 Years	1		
Audio Analysis	4.1	1 User License	3 Years	1		
	4.2	Hardware	3 Years	1		
Drone Forensics	5	1 User License	3 Years	1		
OSINT with Darknet Analysis	6.1	1 User License	3 Years	1		
	6.2	Hardware	3 Years	1		
Crypto Investigation	7	1 User License	3 Years	1		

Forensic Imager	8	Hardware	3 Years	1		
All in One Write Blocker	9	Hardware	3 Years	1		
CDR IPR Analysis Tool	10.1	1 User Academic License	3 Years	1		
Hardware	10.2	Hardware	3 Years	1		
Financial Data Analysis Investigation	11.1	1 User Academic License	3 Years	5		
Hardware	11.2	Hardware	3 Years	1		
Password Cracking Solution	12	Hardware & Software	3 Years	1		
Implementation	13	1 Job	One Time	1		
					Total Basic Amount	
					GST	
					Grand Total	

Total Amount Rupees in words

_____

Note:-

1. Determination of L-1 will be done based on total of basic prices (not including taxes) of all the items/requirements as mentioned above. GST to be indicated and will be based on the rates notified by the government.
2. Price bid as per this format to be submitted along with the detailed quote of the bidder organization in the financial bid cover.
3. Technical Bid Should NOT Contain Price Bid/Financial Bid details (or) Indication. If the price Details are indicated, mentioned inside the Technical bid, then bid will be disqualified and neither the Technical Bid nor the Price Bid/Financial Bid will be considered.

I/We the bidder accept all the terms and conditions as per tender including all technical & commercial conditions.

Place:
Date:

Signature of the Tenderer
Name & Address of the
Tenderer with Office Stamp